

# Building Management Systems (BMS) Application Brief

















Cyber-attacks against building management systems (BMS) or building automation systems (BAS) are becoming more frequent and sophisticated, requiring stronger, more comprehensive defenses than ever before. Although network firewalls and security systems offer increased network security, PLCs remain vulnerable and eventually can be compromised bearing potential catastrophic consequences.

In August 2019, a team of “ethical hackers” presented the successful hacking of the Siemens Simatic S7 Controller at the renowned U.S. “Black Hat” conference. They gained full control of the advanced Siemens S7 Simatic System, and by analyzing its protocols they created a fake alternative engineering station, which commanded the controller at will. This fake engineering station turned the controller on and off, downloaded rogue command logic, and changed the operation and source codes. The hackers even managed to mask themselves so that the controller won’t recognize them as a “hostile intervention”.

These types of attacks may not be detectable from network monitoring as the network vulnerabilities and malware may not immediately or directly result in impact on actual control system equipment and processes. Network security has real vulnerabilities if it cannot capture real-time impacts on physical assets and processes during an incident, leaving a gap in the understanding and resolution of the event. The new generation of cyber-attacks, many of which appear to be sponsored by nation-states with almost unlimited resources, are sophisticated multistage attacks designed to gain control over OT systems and cause disruptions, chaos, and potential loss of human life. Level 0 monitoring is the key to making BMS systems ever-more cyber resilient.

SIGA OT Solutions (SIGA) develops and markets unique, independent, and out-of-band OT cyber security solution for critical assets by monitoring electrical signals from Level 0 (between PLC and device’s actuators and sensors). SIGA applies advanced analytics & unsupervised machine learning for anomaly detection to promote organizations’ cyber resiliency.

## SIGA Solution is ideal for:

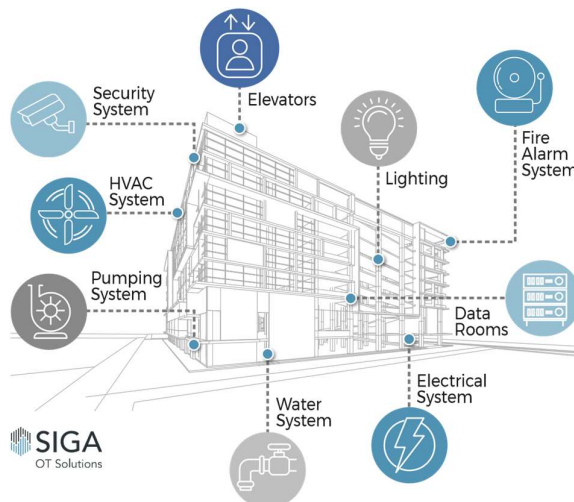
-  Commercial / Residential Buildings
-  Industrial / Manufacturing Buildings
-  Government Buildings
-  Military Installations
-  Emergency Management Centers (OEMs)
-  Command and Emergency Response Centers
-  Fire and Police Departments
-  Traffic Operations Centers
-  Container and Marine Terminals
-  Airport Control Centers
-  Tunnels and Bridges Control Centers
-  Data Centers
-  CERT and CSIRT
-  Exhibition, Conference Centers and Museums
-  Hotels
-  Hospitals, Healthcare Centers and Assisted Living

## Elevate your BMS/BAS cyber resilience to Level 0

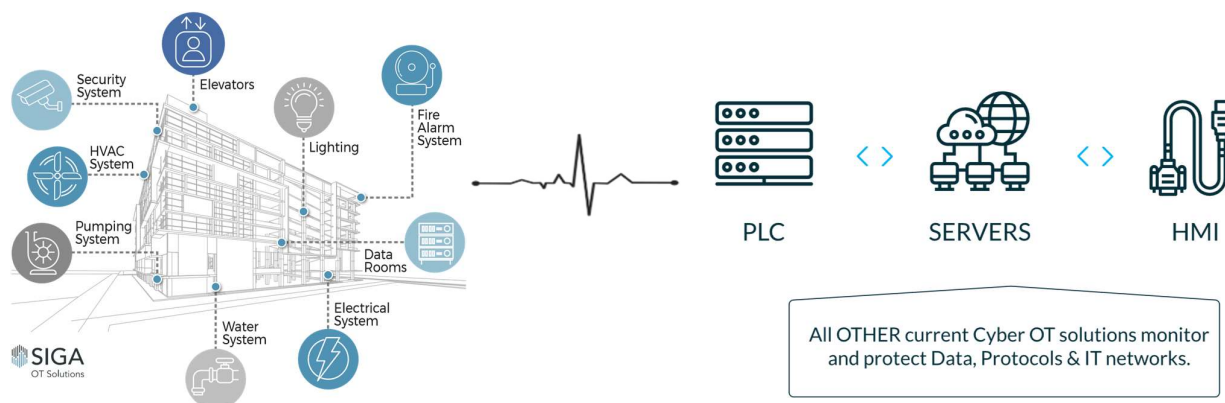
In this era of "smart" buildings, connectivity and technology are being incorporated at an unprecedented scale. The use of security access cards and apps replace manual tasks, like turning a key or lowering the blinds. This technological progress presents new vulnerabilities and risks to property managers and owners as well as to the BMS/BAS industry and the communities they serve.

Broken elevators, a gas leak in the heating system or an unanticipated building lockdown are simple examples of the catastrophic effects of a critical infrastructure hack or malfunction. Unfortunately, these are not hypothetical scenarios, and these present new challenges the industry must face with.

Maintaining real-time situational awareness and operational reliability is essential for minimizing the consequences of such attacks. The ability to independently detect any operational anomalies ensures the operators can visualize the most authentic and up-to-date data to act upon cyberattacks quickly and efficiently.



## Monitoring raw electrical signals to deliver inaccessible operational insights



Monitoring and securing Level 0 (Process layer), which is where real damage can be caused to owners and operators of any real estate property is key to gaining cyber resilience. Electrical signals ensure operators can really feel the pulse of their machinery to detect cyber-attacks and malfunctions instantaneously and resolve them as quickly as possible to prevent their costly aftermath.

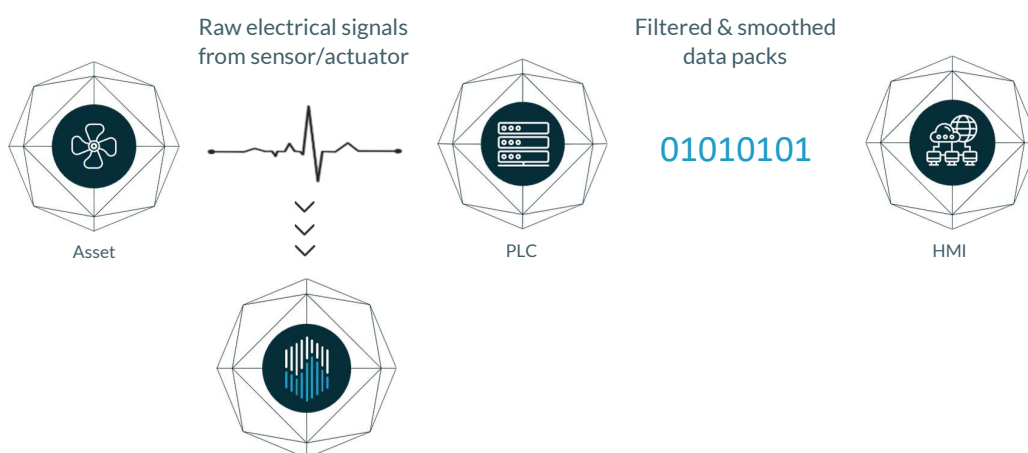
## SIGA is got you covered

Real-time continuous monitoring of unfiltered & untampered electrical signals, directly from the source in any ICS/OT system, equipment, or process in residential, commercial or industrial properties. SIGA empowers operators with timely alerts and actionable insights to act upon cyber attacks and/or malfunctions quickly and efficiently. We deliver a single source of unfiltered, intelligently analyzed, and actionable data, enabling task-specific, business critical modules that eliminate risk and ensure the integrity of your most critical operational processes.

## 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.

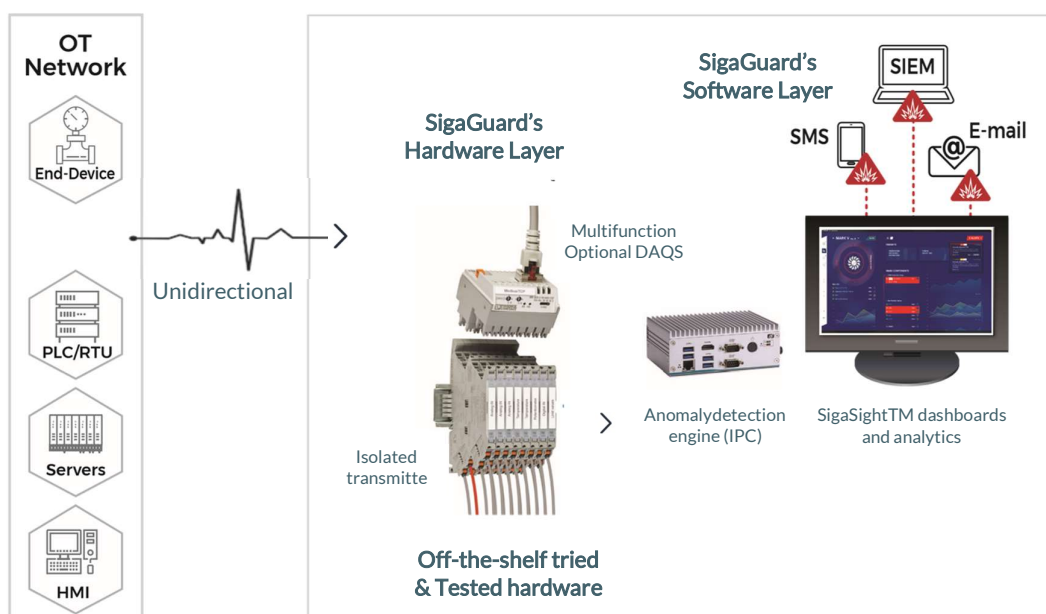
**Industrial Computer:** A compact rigid computer that is the host of the Anomaly Detection Engine (see Software Layer Components section below). This computer has a powerful processor and is suitable for operating in industrial conditions including high temperatures, dirt, and heavy equipment vibrations.

## SIGA's Software Layer:

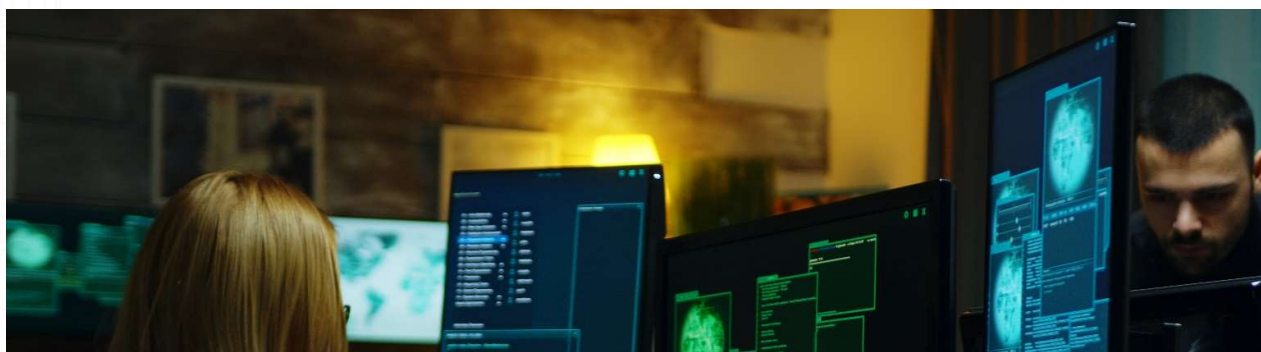
**Source Visualization:** SigaGuard ensures users can continuously monitor their sensors and operational process' health, with data that is normally unavailable in conventional network-based systems. The information is displayed on a user-friendly and intuitive GUI dashboard. By default, the dashboard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



### 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.

## 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**

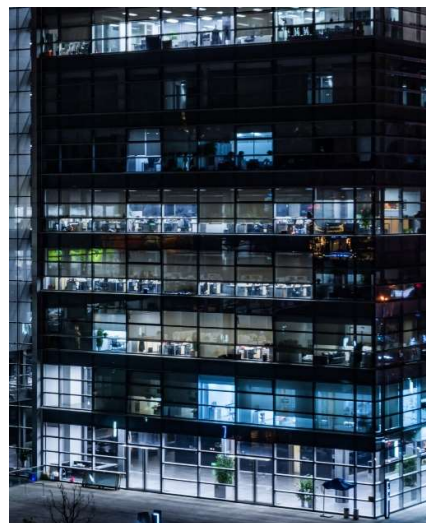
## Use Case 1: Cybersecurity Protection for Commercial Office Building and Government CERT

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.

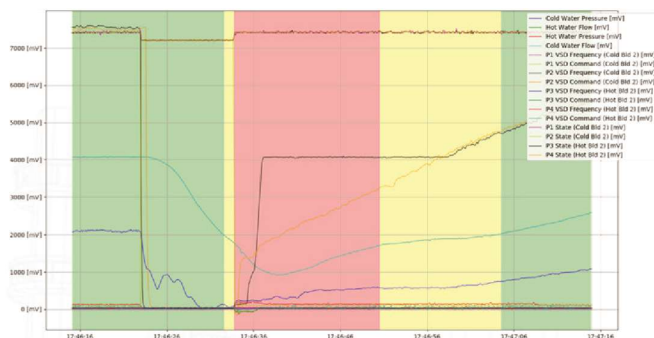
SigaGuard employs unsupervised machine learning to learn the normal operational processes, enabling advanced identification of operational faults in early stages. The platform provides alerts and reports to the operation managers in order to promote cyber resilience, prevent system downtime, ensure operational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

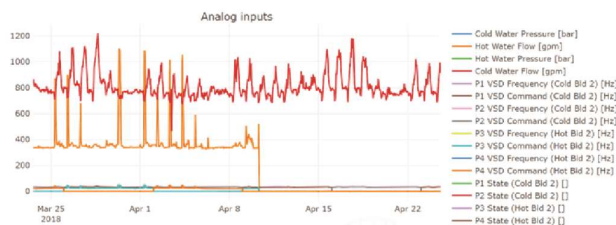
SigaGuard saves countless “human-hours” by producing automatic & continuous operational reports on demand, providing real-time data on each process, or pinpointing critical end-points for monitoring as a separate and independent system. Real-time fault detection is invaluable to critical asset management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



Anomaly Detection in Pump 2 (Cold Water)



Normal pattern of Cold/Hot Water Pumps

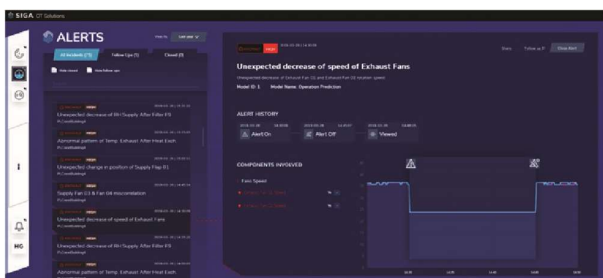


## Use Case 2: Installation at Building 4, Phoenix Contact, Germany

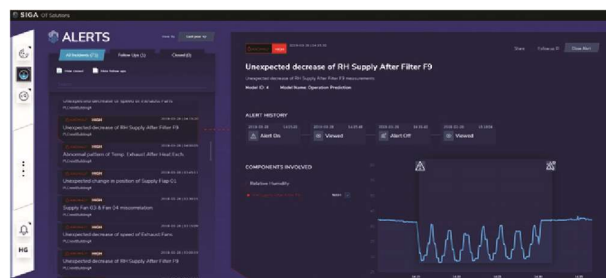
SigaGuard is installed in an HVAC system of building 4 in Bad Pyrmont, Germany, monitoring the air treatment system, including the fresh air inlet to the building in terms of IAQ, temperature and humidity. The system contains an energy-saving air rotary heat exchanger for energy saving purposes in the heating/chilling process of the fresh air.

SIGA is continuously monitoring these IOs, and presents full visualization of the data and alerts when any anomaly is detected by using SigaGuard's cutting-edge machine learning models. 6 different operations' malfunctions were simulated in the HVAC system of building 4 by facility management in order to test different anomalies that might occur in this HVAC system. All 6 faults were detected by SIGA's detection tool, allowing operators to act-upon the issue quickly and efficiently.

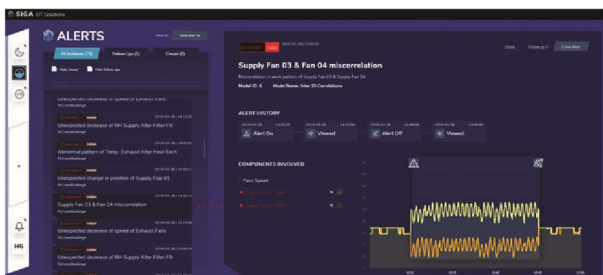
### Unexpected speed of exhaust fans



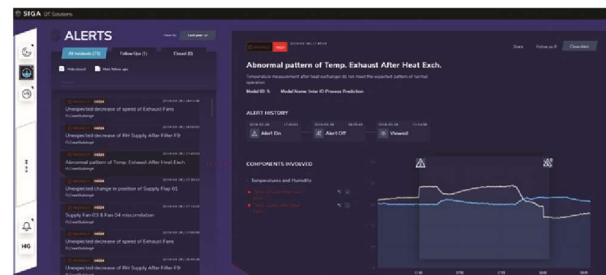
### Unexpected decrease of RH



### Fan 3 & Fan 4 - Miscalibration



### Abnormal exhaust-temp pattern



## 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 Enhanced monitoring and deeper operational perception to operators of critical assets.

## Why SIGA:

SIGA enables operators of critical infrastructure to visualize what was previously undetectable. By monitoring electric signals directly from Level - 0, SIGA delivers OT cybersecurity resilience offering a cutting-edge solution that detects anomalies straight from the physical layer (Level - 0) in real-time to protect your most critical assets.

SigaGuard's unique positioning (Level - 0) can be used as a complementary solution to other OT solutions. And SIGA's unmatched visibility ensures a quick and safe recovery from downtime, thereby reducing any interruptions to a minimum. SIGA's cutting-edge abilities are implemented in your organization seamlessly:

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

## Selected Customers & Collaborations:



## Unique Benefits:

