SIGA
OT Solutions

Building Management Systems (BMS) Application Brief

SIGA Solutions are 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

Critical Asset Management Protection

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 security by establishing a defensive barrier between a trusted internal network and an untrusted external network by monitoring the network level, PLCs remain vulnerable and eventually can be compromised with 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, analyzed and identified the code of Siemens protocol, created a fake alternative engineering station, commanded the controller at will, turned the controller on and off, downloaded rogue command logic, changed the operation and source codes, all while succeeding to create a situation in which the engineer operating the controller did not recognize their "hostile intervention."

Physical destruction is often the goal when a process safety systems or protective relays of a building management system (BMS) is targeted. 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 disruption, chaos, and potential loss of human life. Purdue Level 0 anomaly detection is a critical defense component to thwart such attacks.

SIGA OT Solutions (SIGA) develops and markets unique, independent, and out-of-band OT cyber security and process optimization & operational reliability by monitoring electrical signals from Level 0 (between PLC and device actuators and sensors) providing independent verification and validation from the device level. SIGA applies advanced analytics & unsupervised machine learning for anomaly detection, process optimization and failure prediction.

Era of Technology:

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.

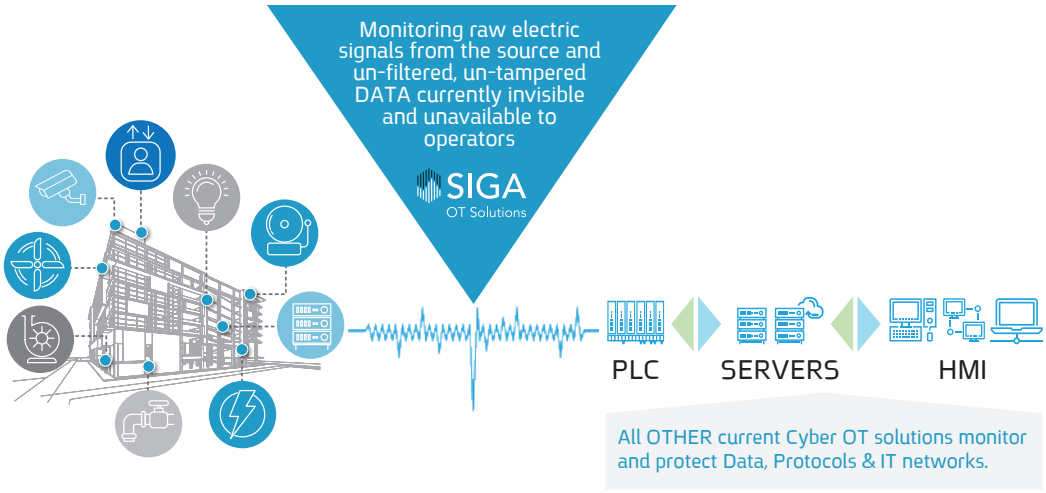
An incapacitated elevator, a gas leak in the heating system or a complete unanticipated building lockdown are simple examples of the catastrophic effects of a critical infrastructure hack or malfunction. Unfortunately, these are not hypothetical scenarios, and present new challenges to prevent damage and even the loss of human lives.

Maintaining real-time situational awareness and operational reliability and the ability to independently detect any operations anomaly give operators the chance to visualize the most authentic, real-time, real-life situation of the infrastructure and ensure critical asset management, operational reliability, process optimization and protect human life.

Critical information is often invisible, undetected or lost in interpretation.

Operators are too often unaware that:

- Systems might not be working to spec
- Equipment / process is nearing failure
- Critical processes are out of sync
- Sensors malfunction
- Cyber-attacks are in progress
- Time & resources are wasted
- People's health and safety are at risk!



The best available solution is monitoring and securing Level 0 (Process) layer of the Purdue reference model, which is where real damage can be caused to owners and operators of any real estate property, by equipment malfunction or cyber attack. It is agnostic of the protocols and electrical equipment being used as it monitors and analyzes the electrical signals, rather than data packet communications. Thus, it can be connected to monitor and analyze any end device equipment or sensor connected to a PLC or an RTU irrespective of the manufacturer and version.

The Solution:

Real-time continuous monitoring of unfiltered & untampered electric signals, directly from the source in any ICS/OT system, equipment or process in residential, commercial or industrial properties.

We empower operators with timely alerts and actionable insights.

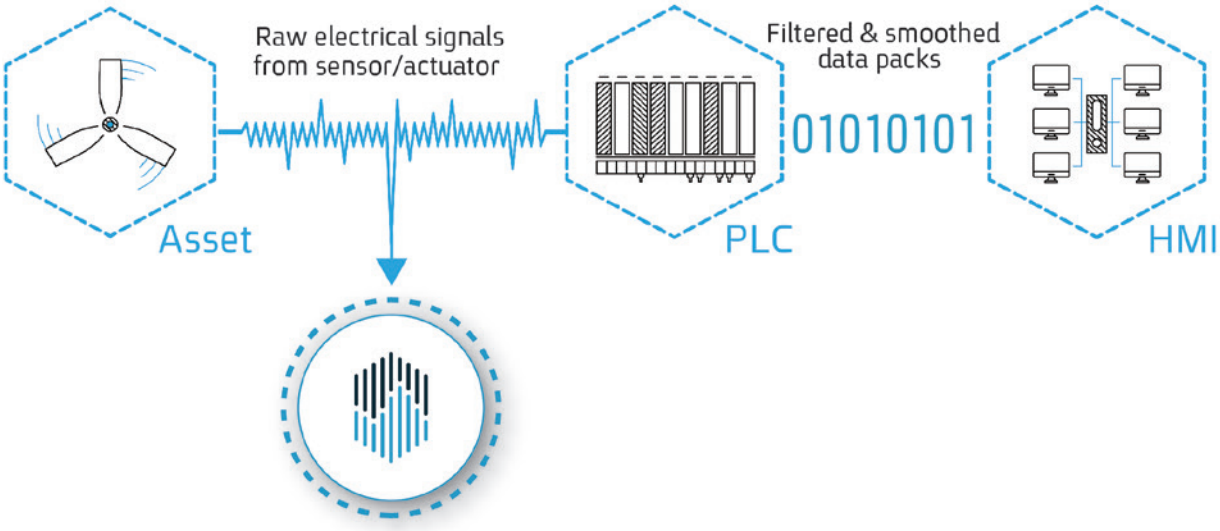
A single source of unfiltered, intelligently analyzed and actionable data, enabling task-specific, business-critical modules that eliminate risk and generate

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.



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 can be processed in the SigaPlatform™, 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.

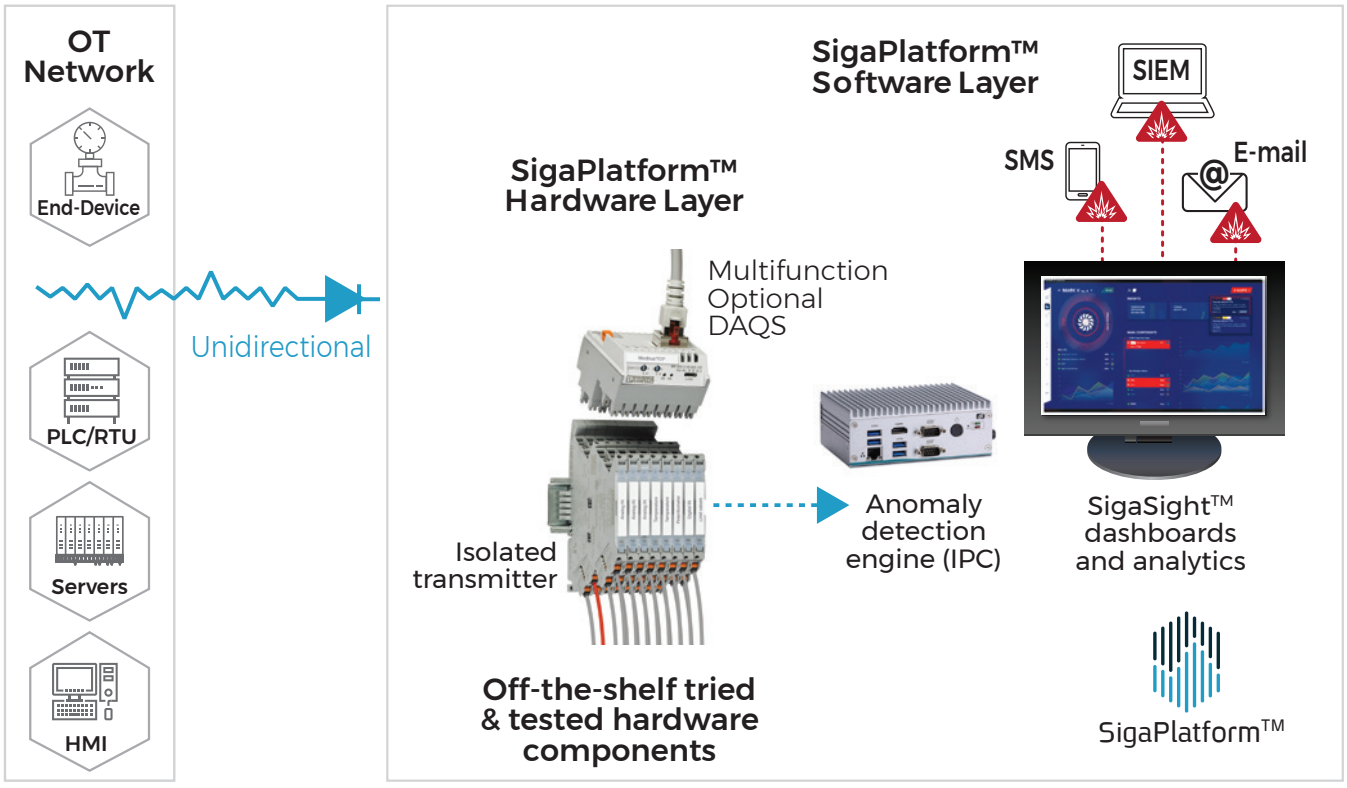
Industrial Computer: A compact rigid computer that is the host of the Anomaly Detection Engine (see Software Layer Components section below). This computer has a powerful processor and is suitable for operating in industrial conditions including high temperatures, dirt and heavy equipment vibrations.

The Software Layer:

Source Visualization: Is the core offering of the SigaPlatform™ which allows users to continuously monitor their sensors and operational process' health, with data that is normally unavailable in 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 can analyze trends and prepare reports of their equipment and process performance. In addition, the system logs all major events for future review.

The SigaPlatform™ Architecture:

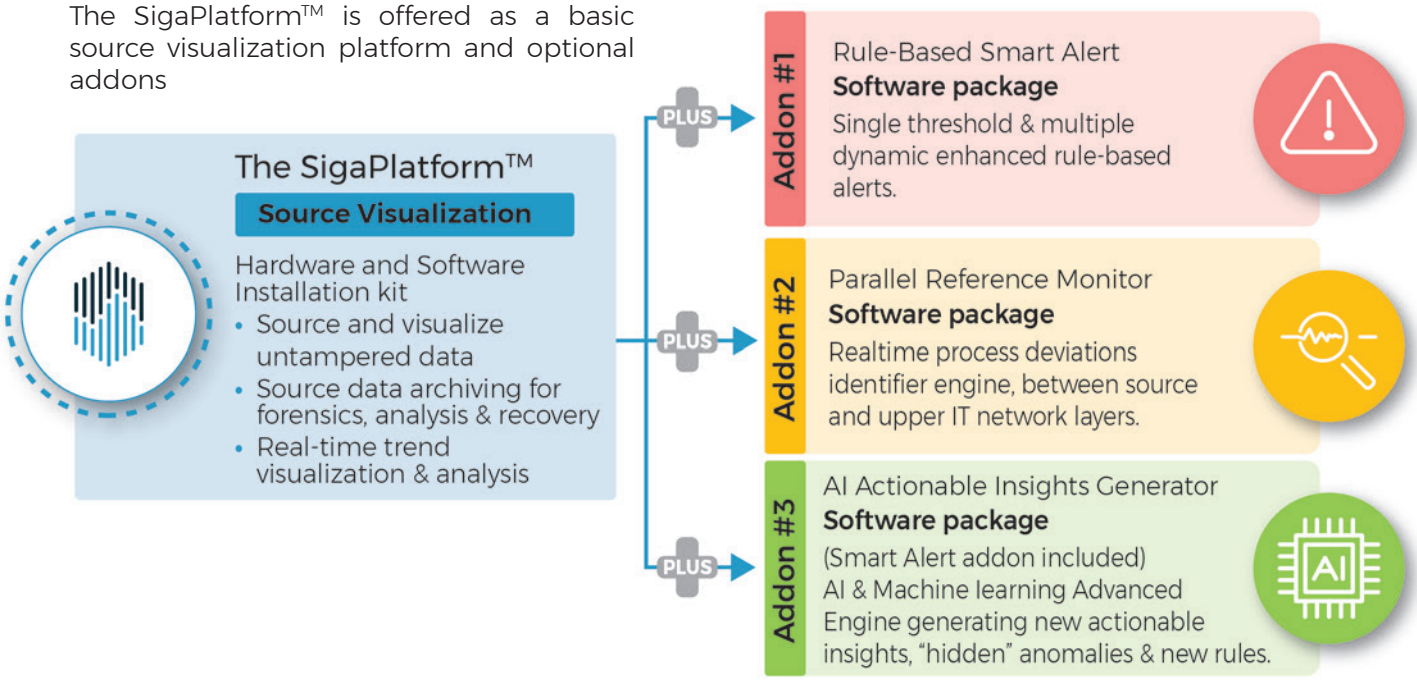
Out-of-Band: Totally Separated, Isolated Network



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

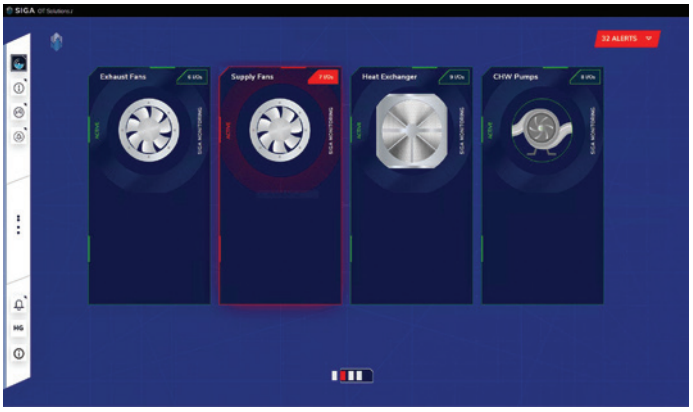
Product Offering:

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



Machine Learning Engine:

The main ML engine's task is to detect anomalies and potential danger in the operational process which are not part of the expected fault cases and not included in pre-defined operational alarms or are unidentified for any reason (operational or cyber). This engine combines proprietary and advanced predictive analysis algorithms that employ machine learning to analyze all incoming signals and identify potential process related anomalies. Any possible threat is forwarded to the SigaSight™ dashboard where it is displayed to an operator or security professional who can investigate, shut-down the asset, flag the warning or determine as "not relevant".



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 identification of the source of the anomaly.

Built-in ICS Cybersecurity Solution:

The SigaPlatform™ 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 SigaPlatfrom™ a 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.

The SigaPlatform™ creates value to both operational needs and cyber security needs both under the same platform.

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

Installation 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. The SigaPlatform™ is connected to process sensors, located in the building ducts, and continuously monitors electrical signals obtained from chiller frequency, heat pumps, operating commands, etc.

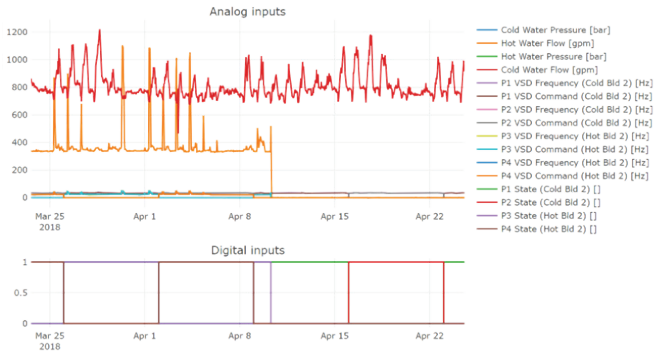
The SigaPlatform™ employs unsupervised machine learning to establish the normal operation processes, enabling advanced identification of operational faults in early stages. The platform provides alerts and reports to the operations manager in order to prevent system downtime, ensure operational efficiency, timely maintenance, safety and cyber protection.

A normal process is one in which both chillers and heat pumps operate simultaneously. SigaPlatform™ has the ability to distinguish between a normal process and any process deviation, providing process optimization and power conservation by maintaining ideal operating requirements.

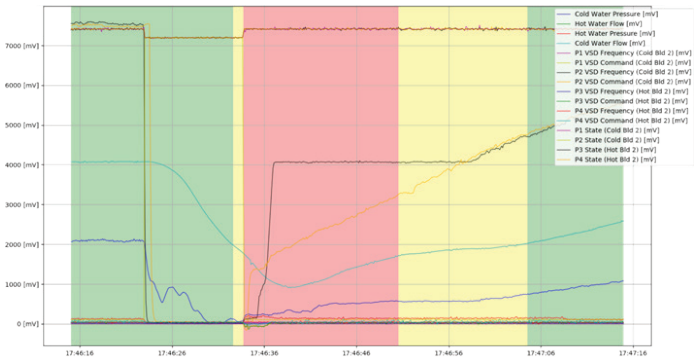
Malfunction/shutdown of pumps may result from voltage fluctuations in the electrical grid, malfunctioning PLC or mechanical malfunction. SigaPlatform™ detects the fault(s) at the onset and provides real-time alerts immediately upon identification of any deterioration in the process. The system sends an accurate detailed SMS/screen notification (in addition to any required logs) describing the specific alert.

SigaPlatform™ 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.

Normal pattern of Cold/ Hot Water Pumps



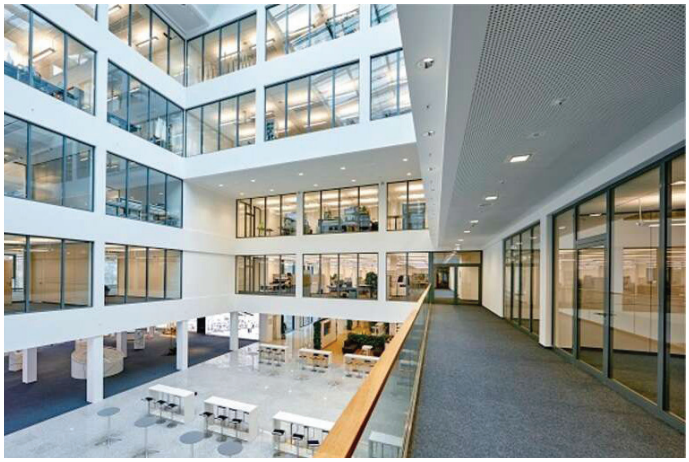
Anomaly Detection in Pump 2 (Cold Water)

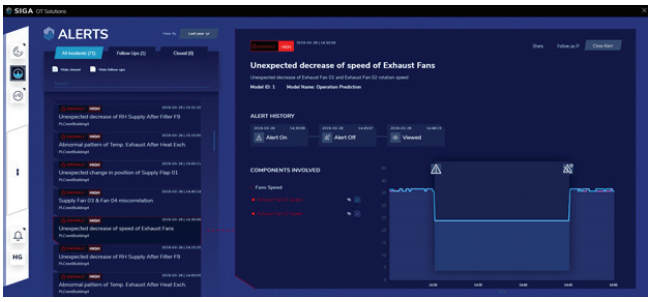


Use Case 2: Installation at Building 4, Phoenix Contact, Germany

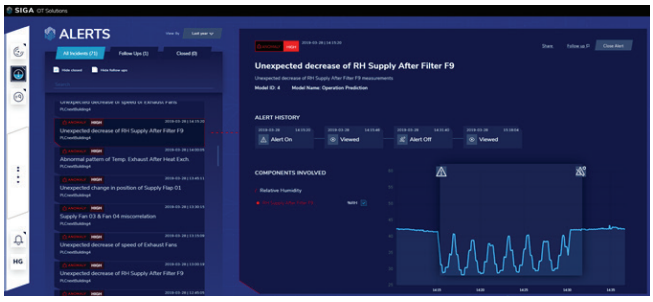
The SigaPlatform™ is installed in an HVAC system of building 4 in Bad Pyrmont, Germany, monitoring the air treatment system, including the fresh air inlet to the building in terms of IAQ, temperature and humidity. The system contains an energy-saving air rotary heat exchanger for energy saving purposes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

SIGA is continuously monitoring these IOs, and presenting full visualization of the data and alerts when any anomaly is detected by using 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.

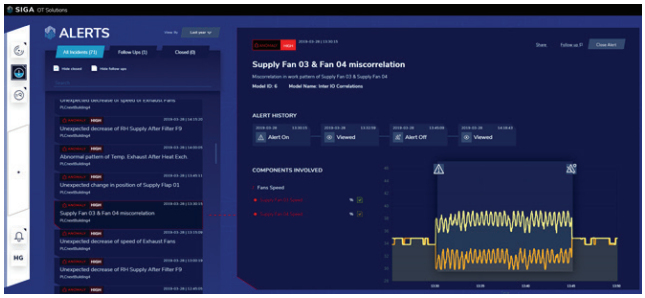




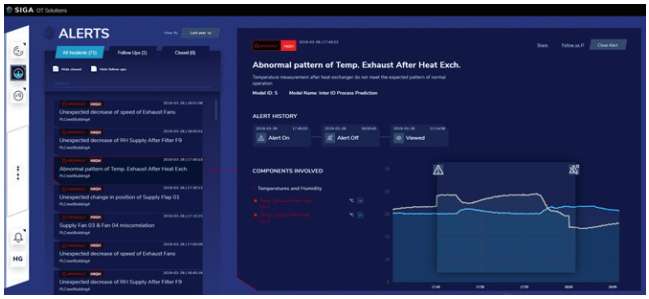
Unexpected speed of exhaust fans



Unexpected decrease of RH



Fan 3 & Fan 4 - Miscorrelation



Abnormal exhaust-temp pattern

- Power Loss on Exhaust Fans 01 & 02
- A Problem with Supply Damper 01
- Relative Humidity Problems in Supply Air
- Problem with the Rotary Heat Exchanger
- Mis-synchronization of Supply Fans 03 & 04
- Problem with HVAC Start-up Sequence

All scenarios detected in real-time, 0 false alerts, highest resolution of visualization and full traceability.

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/IEC 27001:2013 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.

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 robust 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.

Easy Implementation:

- 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.
- SigaPlatform™ works with all SCADA equipment and is protocol agnostic.
- Each installation can immediately and securely export the information in any format to any platform.

Select Customers & Collaborations:

New York Power Authority · Phoenix Contact · Schneider Electric · Siemens · Toshiba · ICL Industrial Products · Energean Oil & Gas · CyberGym · ST Engineering · Oak Ridge National Laboratory

Unique Benefits:

Data From The Source For Operational Insights	Monitors Unhackable Electric Signals	Advanced Analytics Machine Learning	Fast, Easy Installation and Commissioning	Predictive Failure for Zero Downtime