Transforming Brownfields into Industry 4.0, Smart and Efficient Operational Environments

SigaInsight, an Autonomous, IIoT Solution for Operational ICS Environments, Offering Anomaly and Process Inefficiencies Detection, and Advanced Industrial Analytics on Mission-Critical Automated Equipment, Machinery & Processes.

The Transition to Industry 4.0

The rise of new digital industrial technology, known as Industry 4.0, is transforming the way we gather and analyze data across machines, enabling faster, more flexible, and more efficient processes to produce higher-quality goods at reduced costs. This manufacturing revolution will increase productivity, shift economics and foster industrial growth. In this transition, the convergence of IT & OT and the accelerated “internet connectivity”, companies face formidable challenges in the adoption and implementation of new technologies.

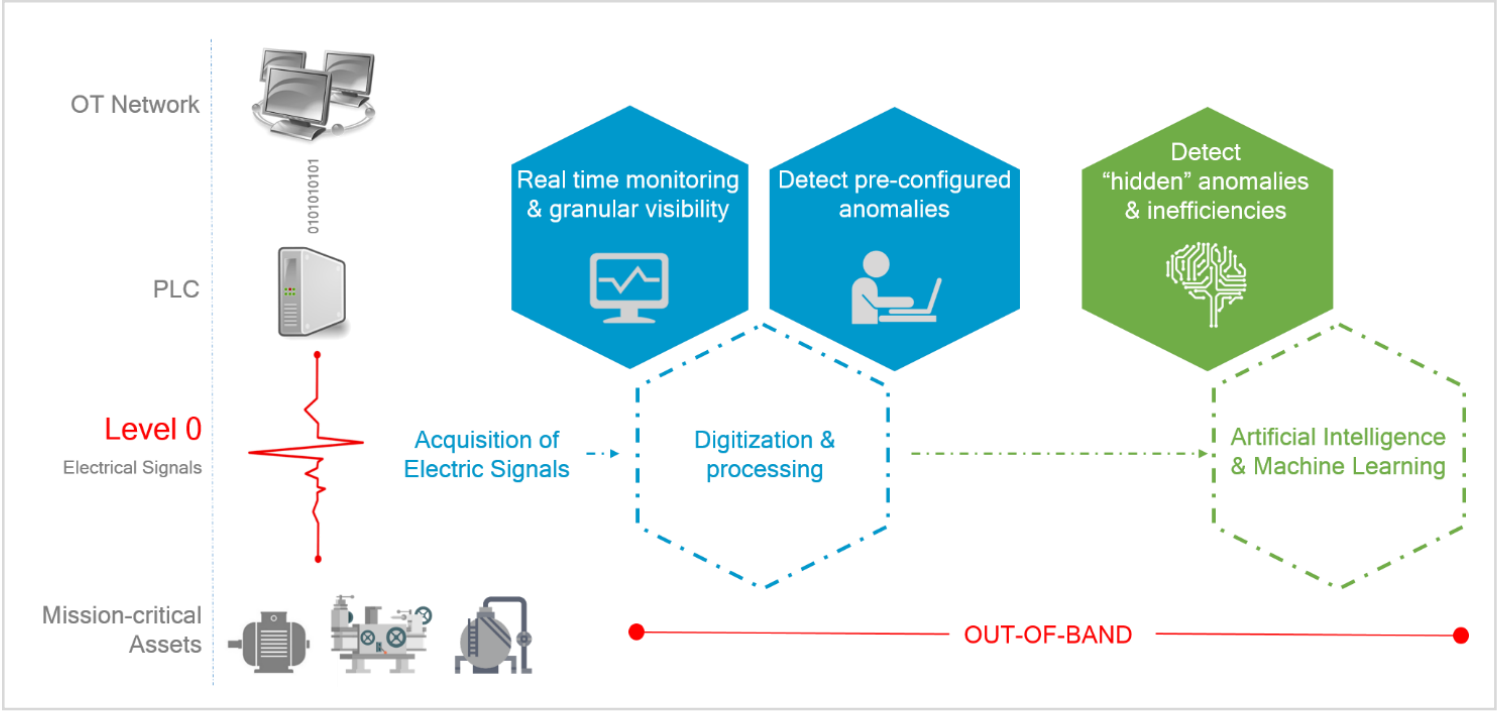
In most industries, automated machinery and operational processes play mission-critical roles. These mission-critical OT assets, primarily in brownfield operational environments, are exposed to costly operational malfunctions, inefficiencies, delays, misconfigurations & failures, resulting in financial losses due to downtime & inefficiencies, regulatory breaches, loss of customer trust & reputational damage, law suits & management liability, high remedial costs and dangerous consequences to human health. In many industrial sectors and critical infrastructure environments, companies are seeking to adopt new industrial analytics technologies that can be easily integrated into their complex, and often legacy oriented, operational environments, to minimize exposure to cybersecurity risks, to ensure safety and all in affordable and sufficiently flexible ways. Unfortunately, most IIoT technologies that are available today unable to offer neither seamless implementation, cybersecurity, nor sufficient and measurable results.

SIGA offers a Paradigm Shift in Industrial Analytics OT / ICS environments

By activating Independent machine learning engines on rich and unfiltered electrical signals at Level 0, we deliver autonomous inspection & industrial analytics solutions, offering inaccessible insights, operational resilience and un-paralleled situational awareness of industrial processes and automated machinery. Electrical Signals at Level 0 of the Purdue Model are the most reliable source of data for OT environments. This source of data is rich & unfiltered, un-hackable, and often un-available to operators.

The SigaInsight enhances reliability and optimization of industrial assets by monitoring raw electrical signals (level 0 realtime monitoring) – as opposed to data packets in the OT networks monitored by all others solution providers. SigaInsight brings new and unmatched operational reliability and efficiency into physical processes, to provide real-time anomaly detection and to support intelligent, real-time, business-critical decision making. SigaInsight delivers unique and granular visibility into physical processes - supporting more informed decision making. 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.

SigaInsight Innovative Topology for Industrial Analytics



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.

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 SigaInsight 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

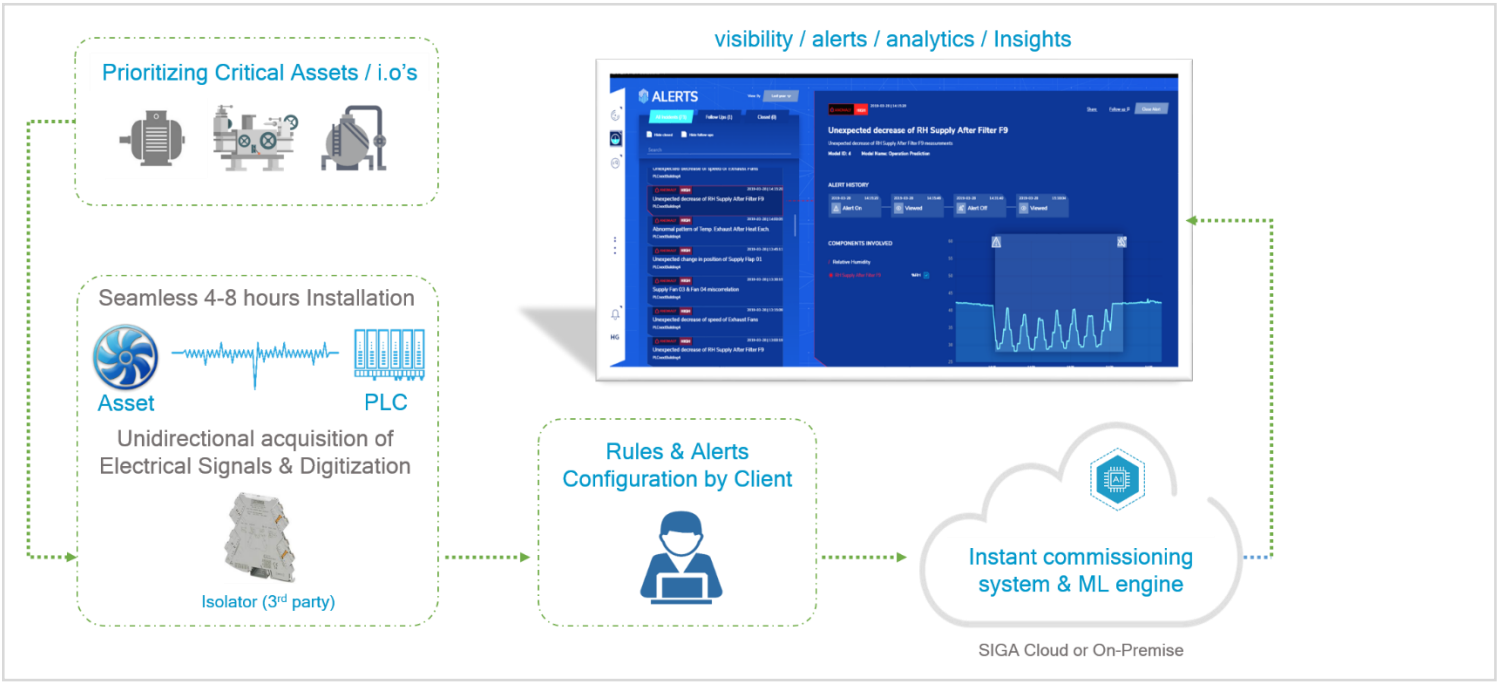
Isolated Transmitters: A standard automation control component, Utilization of non-invasive Isolated Transmitters to mirror selected electrical signals (current/ voltage) utilized by the assets without affecting the ICS system or the signals themselves. The result is an identical signal that can be processed 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.

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. 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.



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.

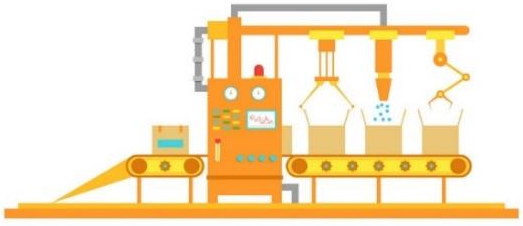
Our Value Proposition

SigaInsight offers operational teams an Autonomous Inspection, Monitoring and Analytical Solution for operational optimization and situational awareness. By monitoring the richest and most reliable source of operational data, and by activating powerful machine learning tools, SigaInsight delivers the following benefits:

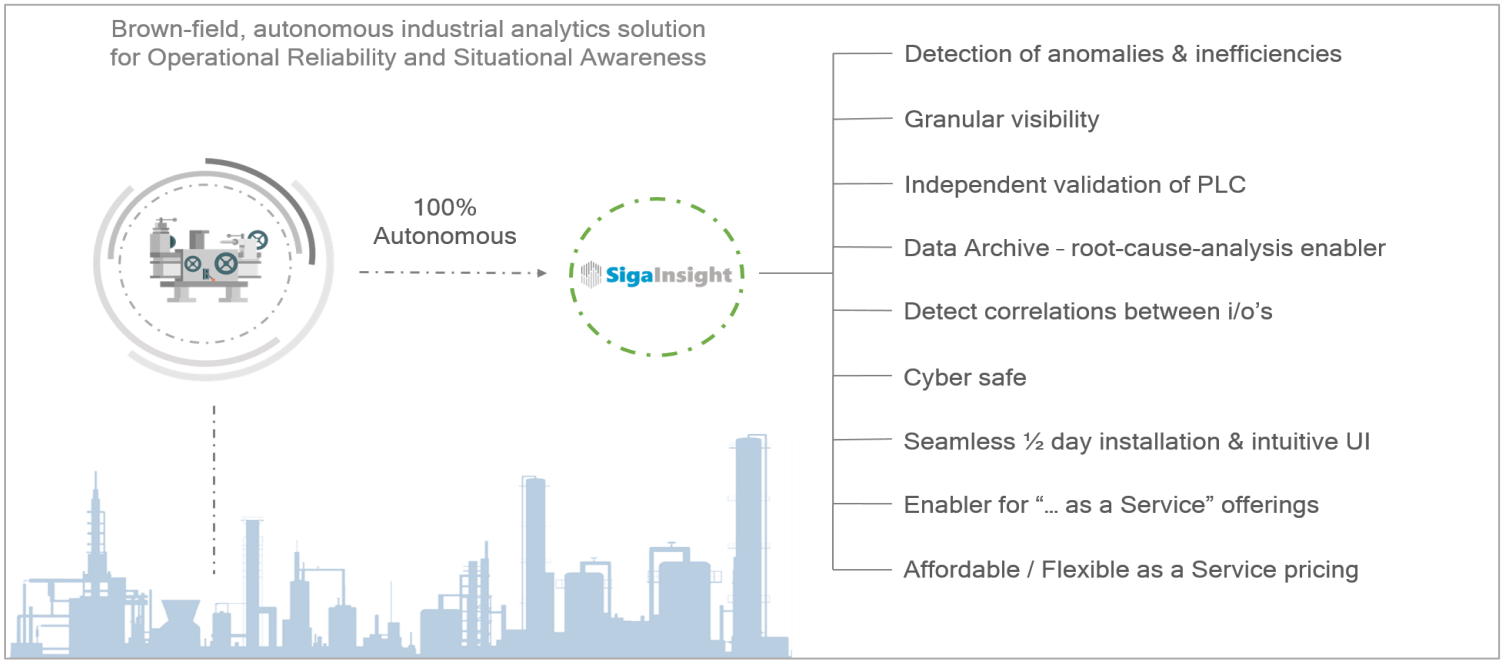
- Constant detection of pre-configured and “hidden” anomalies and inefficiencies, often at their initial evolvement stage.
- Granular process visibility – unparalleled resolution.
- Independent validation of PLC output.
- Situational awareness of critical operations – 24/7 anywhere.
- Out of Band: unidirectional secure data export – 0 exposure to cybersecurity threats.
- Detection of simple and complex correlations between different machines or i/o’s.
- Independent data archiving – enabler for root cause analysis and fast recovery of operational processes.
- Enabler for continuous operation even when the ICS/SCADA system is compromised or shut down
- Seamless ½ day installation, simple integration & intuitive and friendly UI.
- Enabler for “… as a Service” remote service offerings.
- Affordable solution / Flexible as a Service pricing

An enabler to maximize uptime, optimize yield, improve asset health and eliminate bottlenecks in any industrial environment.

Critical Infrastructure



Manufacturing Facilities



About Siga

SIGA OT Solutions ltd is a young and dynamic company, led by synergetic and highly experienced managers, R&D, commercial and operational teams. SIGA developed a unique OT & Cyber Security, protocol agnostic solutions based on raw electrical signals of level 0 – sensors and actuators monitoring, with a range of solutions at commercial stage, and with over 30 installations worldwide.

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.