SIGA
OT Solutions

Data Centers: Cyber & Operational Resilience Solutions Overview

One single minute of Data Center downtime costs $8,000. *
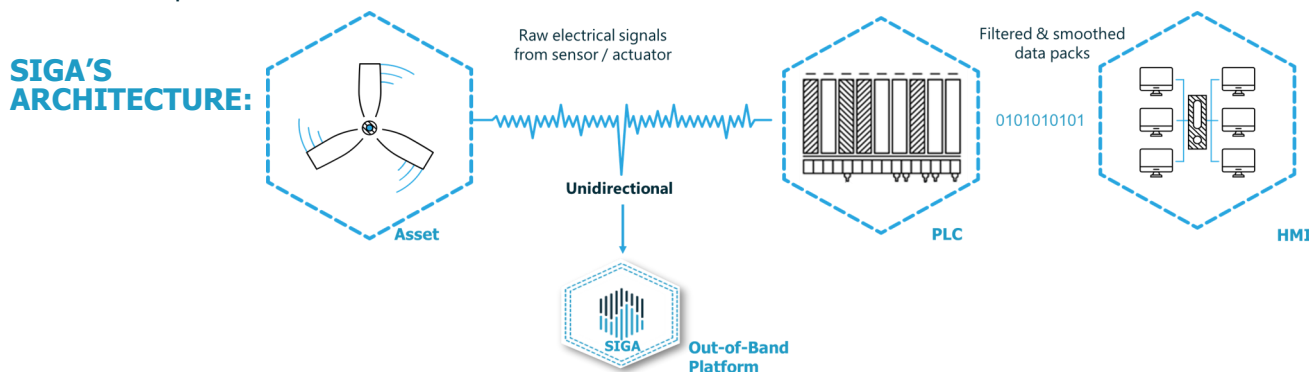
While securing the data-network is crucial, the system remains vulnerable despite the layers of protection installed, and the *operators wouldn't even know it* — as demonstrated at the Stuxnet (2010), Irongate (2016) and Black Hat (2019) events, where PLCs were hacked and compromised without detection or operator awareness of such compromise.

This vulnerability can be solved by monitoring the most reliable source of information, the physical source – the raw (un-hackable) electrical signals at level 0 – sensors and actuators.
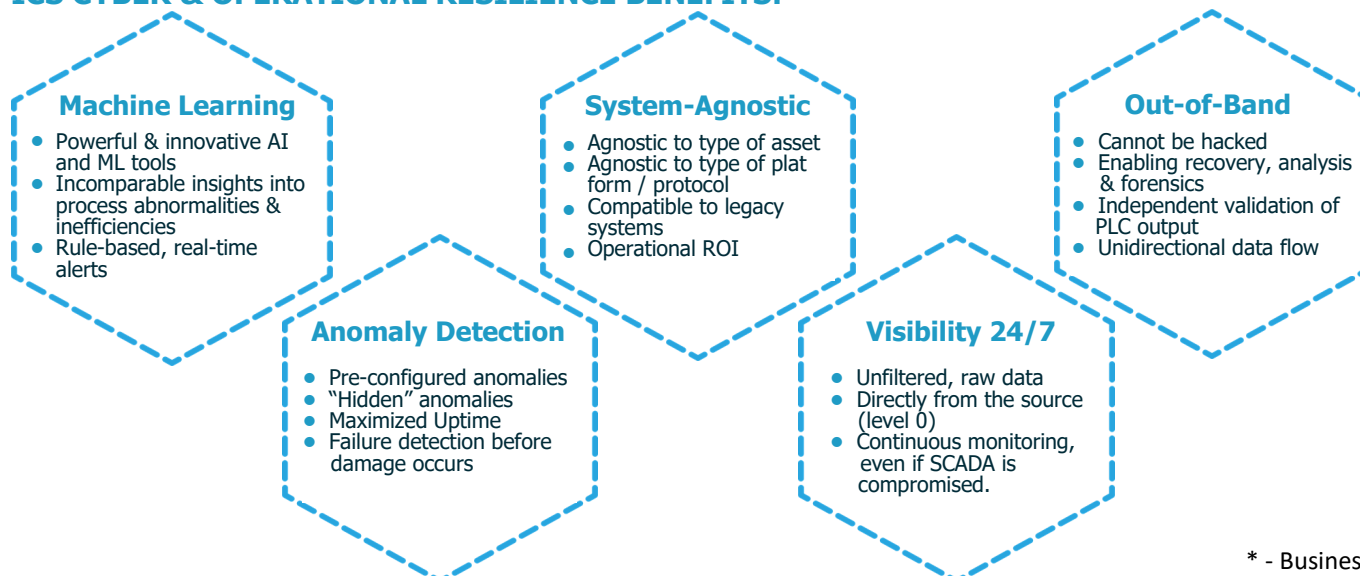
NIST (National Institute of Standards and Technology) Report 8228 states that it cannot issue a cybersecurity standard for IoT systems and devices due to the lack of interoperability between the network platforms and IoT devices.

Level 0 monitoring is an essential component for Cyber Security & maximizing uptime.

The SigaPlatform™ safeguards data center assets by using an out-of-band network to monitor raw, untampered electrical signals. These signals are analyzed by SIGA's unsupervised machine learning software to provide operators **real-time alerts on anomalies caused by cybersecurity intervention** or operational failure indicators to maximize uptime.

SIGA'S ARCHITECTURE:

Raw electrical signals from sensor / actuator

Unidirectional

Asset

Filtered & smoothed data packs

0101010101

PLC

HMI

SIGA Out-of-Band Platform

ICS CYBER & OPERATIONAL RESILIENCE BENEFITS:

Machine Learning
- Powerful & innovative AI and ML tools
- Incomparable insights into process abnormalities & inefficiencies
- Rule-based, real-time alerts

System-Agnostic
- Agnostic to type of asset
- Agnostic to type of platform / protocol
- Compatible to legacy systems
- Operational ROI

Out-of-Band
- Cannot be hacked
- Enabling recovery, analysis & forensics
- Independent validation of PLC output
- Unidirectional data flow

Anomaly Detection
- Pre-configured anomalies
- "Hidden" anomalies
- Maximized Uptime
- Failure detection before damage occurs

Visibility 24/7
- Unfiltered, raw data
- Directly from the source (level 0)
- Continuous monitoring, even if SCADA is compromised.

* - Business Insider