SIGA
Level Zero OT Resilience

# Electrical signals do not lie.

## The Importance of Level-0 Visibility.

A paradigm shift has taken place in the detection of cyber-threats to machinery and equipment in your operational and ICS environments.

Just as it is important to ensure network monitoring for the protection of Industrial Control Systems (ICS) in Operational Technology (OT) environments, it's essential to understand the importance of monitoring and detecting field and process oriented anomalies at Level 0, the sensors and actuators at the equipment and machinery levels—to be able to defend the OT system holistically.

The Purdue Model represents an organization's network divided into 5 levels: Level 5 is the internet DMZ. Level 4 is the organization's corporate network. Level 3 is the manufacturing zone or main control center that communicates with HMI control points at Level 2. These Level2 HMIs interact with Level 1 controllers and Level-0 field devices.

From a cyber perspective, Level 1 to Level 5 consist of traditional Information Technology (IT) cyber solutions, comprised of servers, workstations, switches, routers and firewalls. However, at Level 0, the environment is significantly different. Controllers (PLCs) dictate the physical space, communicating with machinery via current and voltage signals. That's why cybersecurity at Level 0 must be treated very differently.

Monitoring the electric signals transmitted directly from the critical assets is an exceptionally viable and reliable method of detecting malicious cyber-attacks on operational machinery and equipment. Unlike Intrusion Detection Solutions at the network levels—which are often "blinded" to the actual process—monitoring and diagnosing the un-filtered and un-hackable electric signals directly from Level 0 can deliver bulletproof protection to mission-critical operational assets.

Many cyber-attacks, such as Stuxnet, Irongate and the most recent cyber-attacks on Israeli water facilities, highlight the vulnerability of global OT infrastructures. Monitoring Level 0 will ensure operational resiliency even when cyber-attacks are successful in manipulating the logic of ICS controllers, or when malware that blinds operator dashboards. The significance of Level-0 monitoring has already been validated and reflected in recent regulatory directives for critical infrastructure and by leading experts and thought leaders worldwide.

In late April 2020, a Stuxnet-like attack on Israel's water facilities highlighted the necessity of Level-0 monitoring. The apparent goal was to raise the level of chlorine in the water supply by changing the logic of the PLC without raising any alarms. According to cybersecurity experts "… they were trying to manipulate the chlorine levels and at the same time send operators a signal that the chlorine levels were fine". These cyber-attacks highlight the vulnerability of global water & energy infrastructure.

## OT VS. IT Security

Control systems in commercial, industrial and critical infrastructures employ a combination of commercial off-the-shelf human-machine interfaces with communication networks, along with field devices such as process sensors, actuators, and field-level networks drives. Traditionally, cyber security in OT environments has been a top-down approach, achieved by first building digital walls around the digital assets, followed by identifying malware and network anomalies in the IP networks (network anomaly detection), to ensure that data has not been compromised. The IT approach has been expanded to address control systems by monitoring Operational Technology (OT) control system Ethernet networks. This network-monitoring approach is essential but not sufficient for cyber secure control systems and preventing severe damage to OT equipment and machinery.

This is because network monitoring will never be able to fully cover the real assets of the OT architecture: the physical equipment and processes, aka, Level-0 devices. Network cyber security anomaly detection systems assume that process sensors provide secure, authenticated input, however, there is no cyber security or authentication functionality in these devices or device networks. In fact, legacy control system devices have no cyber security or authentication options, nor do they identify which control system devices (e.g., pumps, valves, motors, relays, etc.) are vulnerable to network attacks. Consequently, the IT/OT approach cannot support reliability, resiliency or safety considerations, nor can it provide cyber security to the systems that comprise the control systems – an intractable problem.

## Who's Responsible?

Control system protection should initially be based on the engineering priorities of safety and reliability, then cyber security (if a cyber incident can affect reliability or safety). Legacy process sensors, (e.g., pressure, level, flow, temperature, voltage, current, etc.) are mechanical and/or electrical devices that have cyber and non-cyber failure modes, but no cyber security or authentication functionality. Examples where sensors contributed to catastrophic failures include the Three Mile Island core melt, the Texas City refinery explosion, and the Buncefield tank farm explosion in the UK. Large equipment such as generators, motors, pumps and relays have "do not operate" zones that can cause catastrophic damage. Threats such as the Aurora vulnerability use cyber vulnerabilities to cause equipment to operate in "do not operate" zones, leading to catastrophic failures with no cyber forensics. Studies show that the Aurora vulnerability can bring the grid down for 9-18 months by damaging critical equipment.

Monitoring the electrical characteristics of the process sensors in real time is all about process anomaly detection rather than network anomaly detection. Process anomalies can occur for any reason—including cyber threats. If the sensors— which are ground truth—do not agree with the network, the network is the suspect. Making cyber security an engineering problem can make an intractable network problem tractable, prevent long term equipment damage, improve safety and reliability, and help identify impacts from supply chain threats. Sensor monitoring can also help address the cultural abyss that continues to exist between the engineering and security organizations. Control systems cannot be secured without bridging this cultural gap.

## What is the Difference?

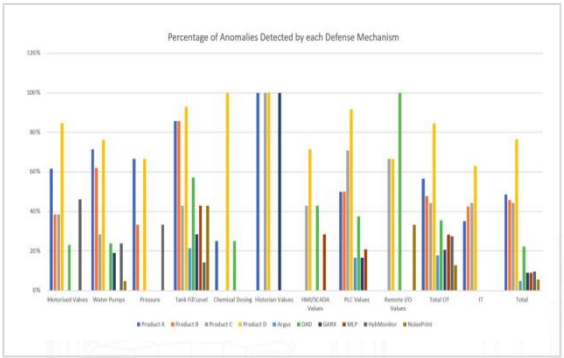
Control system protection should initially be based on the engineering priorities of safety and reliability, then cyber security (if a cyber incident can affect reliability or safety). Legacy process sensors, (e.g., pressure, level, flow, temperature, voltage, current, etc.) are mechanical and/or electrical devices that have cyber and non-cyber failure modes, but no cyber security or authentication functionality. Examples where sensors contributed to catastrophic failures include the Three Mile Island core melt, the Texas City refinery explosion, and the Buncefield tank farm explosion in the UK. Large equipment such as generators, motors, pumps and relays have "do not operate" zones that can cause catastrophic damage. Threats such as the Aurora vulnerability use cyber vulnerabilities to cause equipment to operate in "do not operate" zones, leading to catastrophic failures with no cyber forensics. Studies show that the Aurora vulnerability can bring the grid down for 9-18 months by damaging critical equipment.

## It all starts at level 0

There is a distinct difference between how OT engineers view control system cyber security compared to control system engineers. To control engineers, it is about the security of the network, not the actual impact to systems. When control engineers find malware or network anomalies, they cannot directly relate those anomalies to specific field equipment such as pumps, valves, motors, relays, etc. As an OT engineer, if you cannot tell me what specific equipment can be affected and how, what does the disclosure do for me? For the OT engineers, the focus is the process. Is the process working as designed and is there degradation of the equipment regardless of whether it is malicious or unintentional? Most control system incidents won't be cyber-related (or even identifiable as being cyber) but it is still critical to know the state of the process. For OT to be of value to the engineers, network cyber security must help with these issues. The question is: What reliability and safety requirements can be impacted by lack of cyber security of process sensors, actuators, and drives? If you can't trust your measurements, you're in trouble. Sensors, actuators, and drives are engineering systems; not network devices. They must meet design and operational requirements for processes to be safe and reliable. Cyber security is just one "threat" to meeting the design and operational requirements of the sensors.

## The Critical Infrastructure Security Showdown (CISS)

August 2019, Singapore. Real-time field testing of OT Cybersecurity detection tools. A full report was recently published, and the results show that the cyber Intrusion Detection System (IDS) that monitored Level 0 received highest ranking score for detection of cyber-attack anomalies related to the OT process. The results explicitly demonstrate, beyond any doubt, that monitoring the electrical signals at Level 0 is a crucial element for any cybersecurity protection platform in industrial environments.



There have been many incidents where inaccurate sensors have caused catastrophic failures. Both analog and digital sensors have, been compromised. There has been at least one incident where a sensor was maliciously hacked, and the system was not able to perform its function.

## Actionable Insights from Level 0

Monitoring the sensors and actuators at Level 0 represents a paradigm shift in how early warning OT process anomaly detection systems operate: combining cyber security and operational methodologies to provide unique detection of any major process event. A process anomaly detection system that monitors critical assets using electrical signal-based advanced analytics, artificial intelligence and machine learning must be considered as a complementary and synergetic cyber detection layer in any end-to-end cyber Intrusion Detection System in OT environments. Electrical signals from the operational network cannot be hacked or manipulated. They provide a wealth of information for operational reliability, process optimization and cyber-security. Monitoring Level 0 is the first line of misbehaviour or anomaly detection, ensuring continued operational optimization at all times.

Focusing on electric signals—before they are converted into data packets and filtered by the PLC—is probably the most effective technique for accurately identifying an operation anomaly, regardless of cause. It can bring the highest possible level of visibility into process equipment and sensor functioning, thereby:

- reducing cost and improving performance by limiting downtime and minimizing risk of damage.
- providing resilience to Windows-based HMIs.
- maximizing safety, reliability, and security.

Monitoring electrical signals at Level 0 can be done completely out-of-band, detached from the OT network and independently of the ICS/SCADA system, making it the most secure and reliable anomaly detection solution.

Evolving government regulatory frameworks validating the importance of regulatory compliance to deploy unidirectional monitoring of electrical signals at sensors/ actuators levels

| Control ID | Title | The Control | Complementary explanation | Control Implementation Example | Control Depth* |
|---|---|---|---|---|---|
| 12.32 | Information Security Monitoring | The organization will have independent monitoring capability in the operating network and/or IT network. | This monitoring examines a change in the physical space, which is an indication that is independent of the organization's architecture and constitutes an anomaly, which requires an examination of the operating personnel for the exception. | This can be realized, for example, with the ability to read values (analog and digital) to measure changes from sensors and actuators (level 0) in a completely disconnected configuration that is independent of the operating network (out of band) and unaffected. These changes can be detected by measuring electricity, pressure, temperature, etc. | 4 |

Cyber Israel
Prime Minister Office
National Cyber Directorate

Author: SIGA OT Solutions

## About SIGA OT Solutions

SIGA OT Solutions (https://sigasec.com/) develops and markets unique OT & cyber security, protocol agnostic solutions based on raw electrical conditioning monitoring. Siga technology provides 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, has satisfied customers in the United States, Europe, Singapore, Japan, and Israel.

SIGA holds approved U.S. Patents with additional patents pending and is certified with the ISO/IEC 27001 information security standard. Siga was Named a “Cool Vendor” in Gartner’s “Cool Vendors in Industrial IoT and OT Security” for 2018, awarded the European Union's "Seal of Excellence” and is a member of the EU's Energy Shield consortium.