SIGA OT Solutions

Submitted to:

UNITED STATES OF AMERICA
DEPARTMENT OF ENERGY
Office of Electricity

Notice of Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure

Electrical signals don't lie.

Highlighting the Importance of Level-0 Visibility for securing critical infrastructure.

The importance of Level-0 monitoring cannot be overlooked. It's an integral part of network monitoring of Industrial Control Systems (ICS) in Operational Technology (OT) environments. Detecting field and process-oriented anomalies at Level 0 in the sensors and actuators at the equipment and machinery levels enable holistic defense of the OT system.

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 Level-2 HMIs interact with Level 1 controllers and Level-0 field devices.

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

Monitoring the electric signals transmitted directly from the critical assets is a 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. Monitoring at Level 0 ensures operational resiliency—even when cyber-attacks are successful in manipulating the logic of ICS controllers, or when malware 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.

OT Vs. IT Security

Control systems in commercial, industrial and critical infrastructures employ a combination of commercial off-the-shelf human-machine interfaces and communication networks with field devices such as process sensors, actuators, and field-level network drives. Traditionally, cyber security in OT environments has taken a top-down approach—achieved by first building digital walls around the digital assets and then 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 OT control system Ethernet networks. This network-monitoring approach is essential, but not sufficient for securing 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, no cyber security or authentication functionality exists 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.

Cyber-physical devices

Control system protection should be based on the engineering priorities of safety and reliability from the outset because cyber incidents can impact reliability and safety. Legacy process sensors, (e.g., pressure, level, flow, temperature, voltage, current, etc.), are mechanical/electrical devices that have cyber and non-cyber failure modes, but are without 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.

Engineering vs. Control

To control engineers, cyber security is all about the security of the network, not the actual impact on 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. If an OT engineer, cannot identify which equipment can be affected and how—what's the value of the disclosure?

For OT engineers, the focus is on the process. Is the process working as designed and is there degradation of the equipment (regardless of whether it's malicious or unintentional)? Most control system incidents aren't cyber-related (or even identifiable as such) 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 the 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.

Starting from 0

Currently, process sensors, actuators, and drives do not have cyber security requirements. Even if they did, it wouldn't solve the problem that a compromised PLC (or any other net entity) generates in false or masked information, regardless of authentication or other security measures. These devices have a variety of cyber weaknesses: the sensors themselves, the sensor networks, and the serial-to-Ethernet convertors (gateways). Existing process sensors may not be capable of incorporating even minimal cyber security protections. If the sensors are compromised, (i.e., the sensor values/settings are "incorrect" due to unintentional or malicious reasons), before the gateways convert the data to Ethernet packets, the PLC and HMIs would not be aware that the sensor values/settings had been compromised. There are many ways to electronically compromise sensors with impacts ranging from range from a denial-of-service to effectively removing safety systems by manipulating sensor setpoints. There are no cyber security process sensor forensics present before they become Ethernet packets, so it would not be evident if a sensor were compromised due to unintentional or malicious reasons. To an engineer, it's irrelevant.

There have been many incidents where inaccurate sensors have caused catastrophic failures, whereby 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

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 anomaly detection, ensuring continued operational optimization.

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 the 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 the risk of damage;
- providing resilience to Windows-based HMIs; and
- 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.

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 successful installations 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 EnergyShield consortium.