Response to National Institute of Standards and Technology (NIST)

Request for comments on "Updating the NIST Cybersecurity Framework – Journey To CSF 2.0"

March 17, 2023

Response From: SIGA - Level Zero OT Resilience

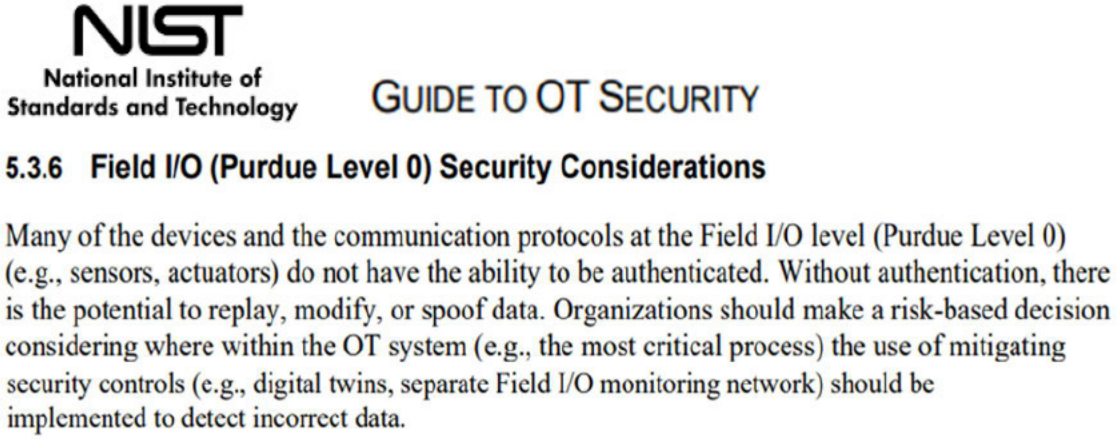
https://sigasec.com/ [redacted], [redacted]

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 enables holistic defense of the OT system.

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 network levels which could be "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.

NIST 800-37 outlines the Risk Management Framework (RFM) which includes 7 steps. In our reply we'd like to relate to step **3.7 MONITOR,** in the attempt of demonstrating how capitalizing on Level 0 can facilitate and significantly improve monitoring and categorizing risks in an OT/ICS environment, to act upon them quickly and effectively. As opposed to network monitoring, which keeps track of data packets, Level 0 monitoring, refers to the continuous tracking of electrical signals stemming directly from the critical assets, the machines carrying out production processes across industries (Oil & Gas, Water, Electricity, Data Centers, Building Management Systems (BMS), Defense, Transportation, etc. By monitoring electrical signals, operators can gain ultimate situational awareness, as the electrical signals represent the machinery's pulse, a source of rich and unfiltered data, which reliably indicates the real state of the machine.

Additionally, in the **NIST 800-82r3** Special Publication guidelines for OT security, Level 0 was implemented as part of the security considerations, as mentioned below -



NIST National Institute of Standards and Technology

GUIDE TO OT SECURITY

5.3.6 Field I/O (Purdue Level 0) Security Considerations

Many of the devices and the communication protocols at the Field I/O level (Purdue Level 0) (e.g., sensors, actuators) do not have the ability to be authenticated. Without authentication, there is the potential to replay, modify, or spoof data. Organizations should make a risk-based decision considering where within the OT system (e.g., the most critical process) the use of mitigating security controls (e.g., digital twins, separate Field I/O monitoring network) should be implemented to detect incorrect data.

Level 0 – monitoring the critical assets directly from the source

We consider Level 0 to be both a detection tool as well as a curative cyber measure. It acts as a distinctive detection tool, as the ongoing monitoring of the electrical signals can tell us a lot about the state of the machinery, giving operators a distinct perspective to detect any kind of anomaly, including the most minimal one, **even when a control network is compromised**, to prevent more extensive cyber assaults. Level 0 can also serve as a curative method, because no matter how sophisticated or innovative hackers are, they simply cannot “fool” the laws of physics, namely, a PLC using data packets, can potentially be spoofed, but the electrical signals can’t. Therefore, even if a cyber-attack is already under way, Level 0 monitoring is ultimately the only way to recover, providing operators with unparalleled insights as to the state of their machinery, to ensure a safe activation of the production processes, while minimizing the number of downtimes due to a cyberattack.

Level 0 monitoring can be classified as an Attack-Detection system, an essential tool for combating cyber-attacks, and a pioneering method to further reinforce RMF, by permitting cutting-edge monitoring of mission-critical assets in real-time.

We also maintain that Level 0 is an essential cornerstone for implementing Zero-Trust Architecture (ZTA), as outlined in **NIST 1800-35E**. Network protocols, although an efficient method for transferring data, is a shaky method to opt for. Ransomware attacks, HMI spoofing, or any other cyber-attacks take advantage of the many vulnerabilities network protocols suffer from, to insert and execute their malicious code. Therefore, implementing ZTA presents a serious challenge, because no matter the quality or quantity of patches and actualizations, the susceptible nature of network protocols prevents us from reaching a trusted solution that can overcome the risk this method faces. In other words, acknowledging that any programable tool can eventually be hacked leaves us with a critical gap to bridge in our quest of reaching ZTA.

We see Level 0 as a potential method driving towards implementing a more reliable ZTA. The data available at Level 0 is simply unsusceptible, as it simply “mirrors” the state of the machinery, any kind of change, even the slightest is immediately reflected in the flow and quality of the electrical signals. Level 0 could potentially serve as the “polygraph” of the data packets transferred in through higher level of the Purdue Model, by performing constant comparison between the two, to detect any kind of anomaly in real-time. Level 0 assures the employment of network protocols, by continuously monitoring and comparing the values appearing in Level 0 to those appearing in the upper levels (Level 1, 2, etc.).

As we have demonstrated above, Level 0 represents key importance for achieving ZTA and further improving monitoring, which is why we believe Level 0 should form part of CSF 2.0.

Author: SIGA OT Solutions

About SIGA OT Solutions

SIGA OT (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.