SIGA Multi-Level OT Cyber Process Resilience

A Cyber Breach is Inevitable -

Layered Cyber-Physical Security is a key for Critical OT Security

A Cyber Breach is Inevitable – Why a Layered Cyber-Physical Security Approach is Critical for OT Security

The threats of cyberattacks on Industrial Control Systems (ICS) are real.

In the last year, the frequency and intensity of cyberattacks on **Operational Technology (OT) systems** have surged, with ransomware activity increasing by more than **87%**. [i] The risks are well documented, ranging from physical harm, financial loss, and regulatory or legal consequences.

We have reached the point of no return. Prevention alone is no longer sufficient. The working assumption in the cybersecurity community is that successful breaches are inevitable, shifting the focus to early detection, containment, and recovery.

This article explores how a combination of Process-Oriented Cybersecurity and Network-Based Intrusion Detection & Threat Intelligence, delivered by SIGA Security and Dragos, respectively, forms a multi-layered cyber-physical defense. By integrating real-time process anomaly detection with network-level threat visibility, organizations establish a more complete security posture, ensuring that both process manipulation and network intrusions are detected and mitigated before they cause widespread operational disruption.

A Layered Approach to OT Cybersecurity: Addressing the Gaps in Cyber-Physical Defense

Operational Technology (OT) environments are under increasing attack, yet many industrial organizations still rely on security models that were designed for IT networks instead of ICSs. The assumption that cybersecurity can be managed solely through network monitoring, firewalls, and access controls leaves critical blind spots in OT security.

OT cyber threats are often hybrid in nature, combining network intrusions with physical process manipulation. For instance, attackers may use legitimate credentials or compromised access points to issue commands that appear valid within the system, bypassing conventional security tools. Traditional defenses such as network-based firewalls or endpoint detection solution are unlikely to identify this type of attack because the compromised system is still functioning as programmed.

This is where a layered approach to OT cybersecurity comes in.

Instead of relying on single points of detection, cyberteams integrate multiple security disciplines to ensure both network-based threats and cyber-physical process anomalies are addressed.

A multi-layered cyber-physical security strategy is comprised of two elements:

Process-Oriented Cybersecurity: directly monitoring the physical process itself to detect operational anomalies that indicate manipulation, spoofing, or sensor compromise.

Network-Based Intrusion Detection & Threat Intelligence: monitoring for unauthorized access, lateral movement, and adversary activity across OT networks.

By combining these two approaches, we gain full-spectrum visibility, ensuring that both digital intrusions and physical process disruptions are identified, investigated, and mitigated before significant damages occur.

Use Case: Protecting Water Treatment Facilities from a Cyber-Physical Attack

To understand how process-oriented security and intrusion detection work together to defend industrial operations, consider the example of a municipal water treatment facility.

Water treatment facilities rely on **automated control systems** to regulate chemical dosing, filtration, and distribution. Cyber threats targeting these systems can **manipulate setpoints, disable alarms, or alter chemical balances**, leading to serious public health risks.

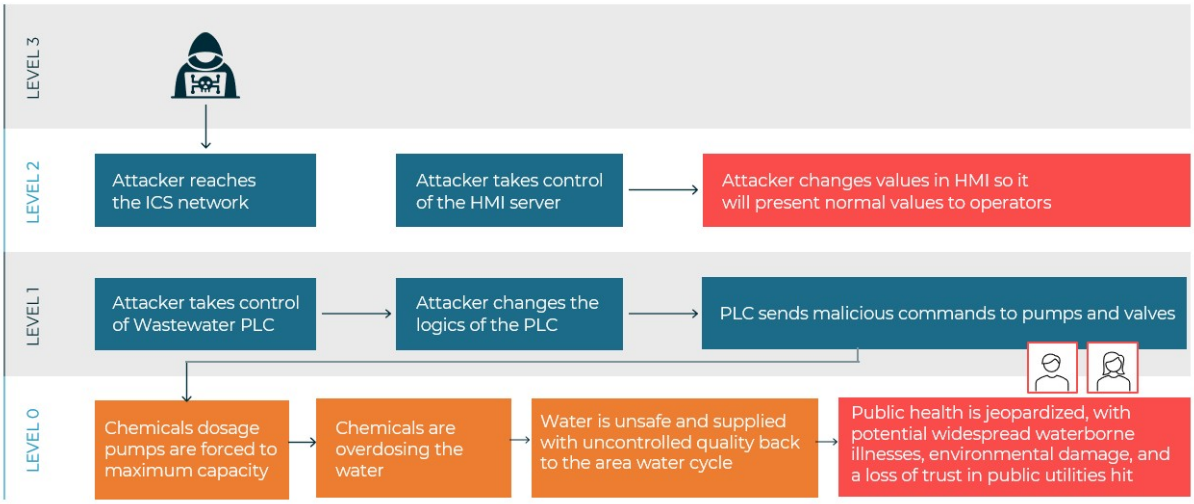
The challenge is that **network security (SYSTEMS?) detects unauthorized access and system modifications** but does not confirm if the process itself is compromised. Meanwhile, **process-oriented monitoring detects deviations in physical conditions** but does not trace them back to specific cyber intrusions. (IS THIS TRUE?) **Only when these two layers work together can security teams fully understand and mitigate cyber-physical threats.**

The Attack: Manipulating Chemical Dosing in a Water Facility

An attacker exploits a remote access vulnerability to gain control of the SCADA system at a municipal water treatment facility. Once inside, they remotely modify the PLC's chemical dosing setpoints, increasing sodium hydroxide to unsafe levels.

To evade detection, they alter the HMI's display values, making it appear as though water treatment is functioning normally. This attack goes unnoticed until contaminated water reaches the public.

Water Utility Attack Scenarios



How Intrusion Detection and Process-Oriented Security Work Together

A cyberattack on an industrial process does not always follow a clear sequence. Network intrusion detection and process-oriented monitoring identify different aspects of an attack, often simultaneously.

Intrusion detection flags unauthorized access to the system, identifying a remote session into the engineering workstation and unapproved PLC modifications. It detects anomalous command sequences that alter chemical dosing levels.

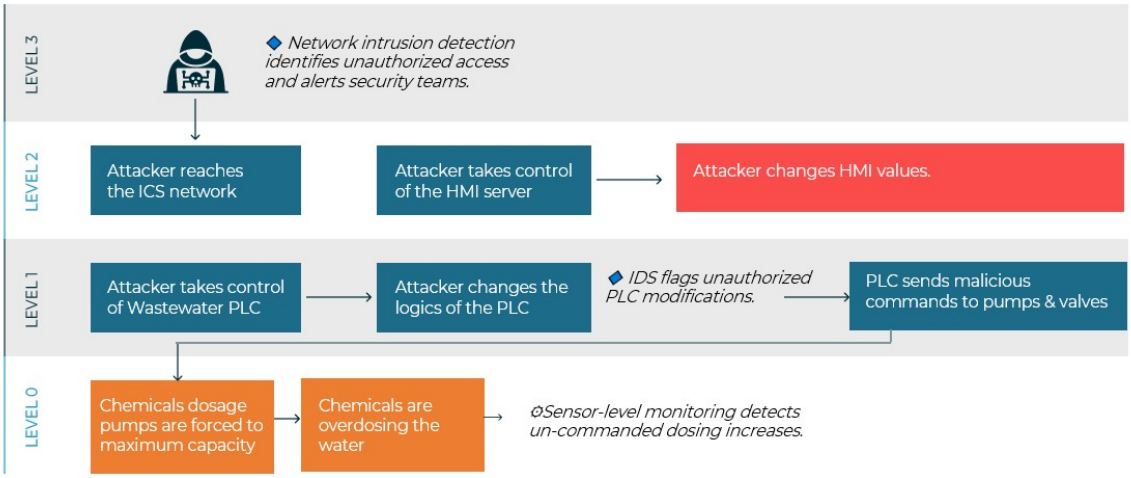
At the same time, process-oriented security monitors raw sensor data, identifying discrepancies between real-time chemical levels and the values reported in the SCADA system. Despite the HMI displaying normal operations, sensors reveal that sodium hydroxide levels are rising beyond safe thresholds.

These two layers of detection work together, validating the attack from both a cyber and physical perspective. Network security identifies the source of manipulation, while process monitoring confirms its real-world impact. By correlating both, security

teams can take decisive action to isolate the compromised system and prevent unsafe water from entering circulation.

With both network-based security alerts and process-level anomalies aligning, the response plan becomes clear. The security team isolates the compromised workstation, cutting off the attacker's ability to issue further commands. Meanwhile, process-level monitoring alerts water facility operators, who manually intervene to adjust chemical dosing levels before unsafe water enters public circulation.

By cross-verifying network intrusions with real-time process deviations, security teams gain high-confidence detection, ensuring that a rapid and coordinated incident response prevents the attack from escalating into a public health crisis.



Why a Layered Approach is Essential

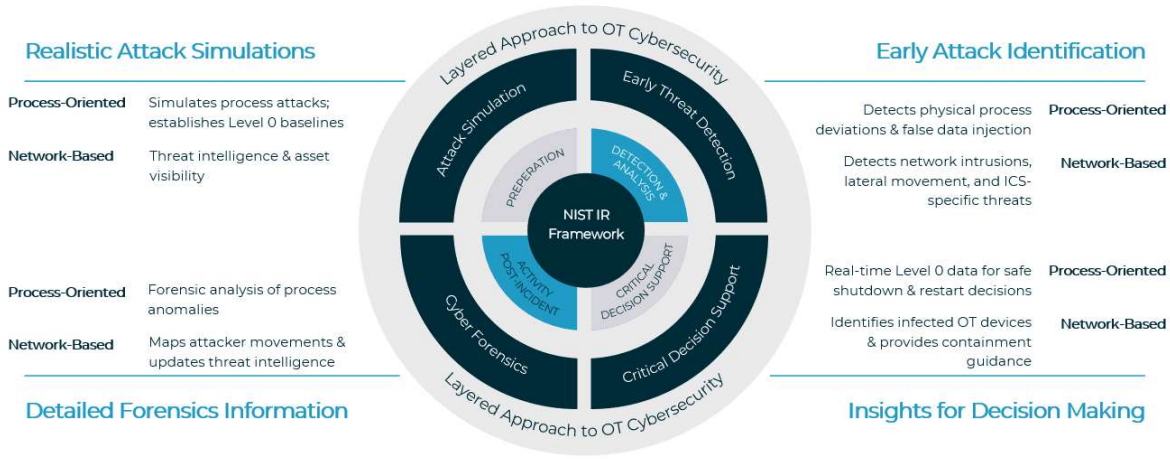
This scenario highlights why both network-based intrusion detection and process-level security are critical to protecting industrial operations.

Intrusion Detection Systems recognize unauthorized access and suspicious control system modifications, but they do not provide visibility into whether those changes have successfully altered the process itself. **Process-Oriented OT Cybersecurity** detects the physical effects of manipulation, but it does not trace those anomalies back to a specific cyber intrusion.

Only by integrating both approaches can security teams see the full picture, ensuring that threats are not just detected but also mitigated before they cause real-world damage.

Layered Approach to Incident Response: Aligning Process Oriented and Network Based OT Cybersecurity

Effectively managing OT cybersecurity incidents requires aligning process-oriented and network-based cybersecurity strategies with a strong incident response framework. The NIST Incident Response Framework provides a structure for this alignment. By examining each phase of the NIST framework, we can detail the contributions of process-oriented and network-based approaches, and how their combined use creates a more complete defense



1. Preparation Phase (Before an Attack)

Before an attack, proactive security measures are essential to improve an organization's readiness. Process-oriented security plays a crucial role in preparing OT teams. Process attack simulation trains operators with simulated process-based cyberattacks, ensuring they can recognize anomalies. It also establishes normal process baselines, enabling early detection of deviations. Network-based security contributes by mapping all OT devices, reducing blind spots in the network, and by providing ICS threat intelligence to keep security teams aware of emerging threats. In the preparation phase, process-oriented security ensures OT operators are trained to recognize process anomalies, while network-based security provides cybersecurity teams with intelligence on known attack tactics. This combined approach improves the organization's preparedness.

2. Detection & Analysis Phase (Identifying an Ongoing Attack)

Identifying a cyberattack as it occurs and analyzing it are the focus of this phase. During this phase, process-oriented security detects real-time process deviations, such as abnormal chlorine or pH levels in water treatment plants, and cross-verifies Level 0 sensor data with SCADA system reports to detect false data injection attacks. Network-based security detects unauthorized PLC modifications, network intrusions, and lateral movement between devices, and flags abnormal command sequences that suggest malicious intent. Process-oriented security validates whether network-based attacks are impacting physical operations, while network-based security detects adversary tactics that might not be immediately visible in process anomalies. The combined information from both security approaches provides a clearer understanding of the attack.

3. Critical Decision Support & Containment

Limiting the impact of the cyberattack is the goal of this phase. Process-oriented security provides real-time Level 0 sensor data, ensuring operators know the actual state of the system, and guides shutdown or containment decisions by confirming process integrity. Network-based security identifies which OT assets are compromised, allowing for containment of affected systems, and ensures attackers are removed from the environment before operations resume. Process-oriented security helps process engineers verify whether containment efforts restore safe operating conditions, while network-based security ensures no attacker presence remains in the OT network.

4. Post-Incident Activity

Recovery, investigation, and preventing future incidents are the focus of this phase. Process-oriented security provides forensic analysis of process deviations, showing how the attack affected real-world operations, and ensures future anomaly detection models are improved based on past incidents. Network-based security reconstructs the attack path, identifying vulnerabilities and attacker techniques, and integrates new attack patterns into ICS threat intelligence databases to prevent similar incidents. Process-oriented security aids physical process resilience by providing forensic information on the attack's effects, while network-based security strengthens cyber defenses against future threats by analyzing the attack.

Summary and Conclusion

Cyberattacks on Operational Technology are an increasing risk, and traditional IT security is not enough to protect these systems. OT cyber threats often combine

network intrusions with physical process manipulation, making them hard to detect and very damaging. A layered approach, using both process-oriented cybersecurity and network-based intrusion detection, is needed for full protection.

Process-oriented OT cybersecurity provides visibility into the physical process, finding anomalies and manipulations that network security might miss.

Network-based security gives crucial threat intelligence and detects malicious activity on the OT network. By combining these security approaches within the NIST Incident Response Framework, organizations improve their ability to prepare for, detect, contain, and recover from cyberattacks. In short, a layered defense enables faster detection, better containment, and safer recovery, creating a more resilient operational environment.

[i] https://www.dragos.com/resources/press-release/dragos-reports-ot-ics-cyber-threats-escalate-amid-geopolitical-conflicts-and-increasing-ransomware-attacks/