SIGA Multi-Level OT Cyber Process Resilience

A Process Oriented Approach to OT/ICS Cyber Incident Response

Introduction

Operational Technology (OT) and Industrial Control Systems (ICS) are the backbone of critical infrastructure, from energy utilities to water treatment facilities. While these systems were historically isolated from external networks, the convergence of IT and OT has introduced unparalleled efficiencies—but also unprecedented risks.

As these networks grow interconnected, cyberattacks targeting OT systems are escalating in frequency and severity.

This article examines Process-Oriented OT Cybersecurity, a new Cyber OT category that focuses on the physical processes driving critical infrastructure. By leveraging real-time monitoring, it enhances the existing Incident Response framework with improved detection, faster containment, and more effective post-incident analysis.

A Historical Perspective on OT/ICS Cybersecurity

Historically, OT environments were designed for reliability and safety rather than security. Systems operated in isolation, often on proprietary networks, which reduced their exposure to cyber threats. However, as organizations sought to optimize operations and integrate real-time data insights, the adoption of IT technologies within OT environments became inevitable. This shift introduced vulnerabilities that adversaries quickly exploited.

The introduction of standardized protocols like Modbus and OPC UA, while improving interoperability, further expanded the attack surface. Unlike IT systems, which benefit from regular updates and patches, OT devices often run legacy software, leaving them susceptible to exploitation. As attackers grow more sophisticated, the need for proactive OT cybersecurity strategies becomes increasingly urgent.

The Expanding OT Attack Surface

The attack surface for OT systems has broadened significantly as organizations integrate IT networks with their operational environments. While this integration enables real-time data exchange and streamlined operations, it also exposes OT systems to the same vulnerabilities plaguing traditional IT networks.

According to recent studies, nearly 70% of industrial organizations have experienced a cyberattack in the past year. Alarmingly, one of four incidents led to operational

shutdowns, disrupting not only business continuity but also essential public services. The ramifications of these attacks extend beyond financial losses, potentially endangering human lives in sectors such as energy, water, and healthcare.

Drill-Down into Specific and Dangerous OT Cyber Attacks

These challenges represent critical vulnerabilities that organizations must address to protect their operational environments and maintain resilience in the face of evolving threats

1. Ransomware: Continuous Visibility to the Process While SCADA is Blind
   Ransomware attacks often encrypt or lock critical systems, rendering traditional monitoring tools such as SCADA (Supervisory Control and Data Acquisition) systems ineffective.

2. False Data Injection (Stuxnet): Immediate Identification of False Data through Multi-Level Comparison
   False data injection attacks, like the infamous Stuxnet, manipulate process data to deceive operators and control systems. These attacks can cause subtle and cumulative damage to physical assets, such as turbines or centrifuges, while appearing normal to SCADA systems.

3. Changing Process Values Within Threshold (Aurora): Detection of Subtle Attacks via High-Resolution Monitoring
   The Aurora vulnerability is a type of cyberattack targeting industrial control systems, specifically the synchronization between electrical equipment, such as generators, and the power grid. By sending carefully timed commands, attackers can create out-of-phase conditions, causing equipment to experience severe mechanical stress and, ultimately, catastrophic failure.

   This type of attack exploits weaknesses in monitoring systems like SCADA, which may overlook rapid but small process deviations that fall within acceptable operating thresholds.

Incident Response: The NIST Framework in Focus

The US-based National Institute of Standards and Technology (NIST) Incident Response (IR) Framework provides a structured methodology to manage cyber incidents. Its four phases—Preparation, Detection & Analysis, Containment & Eradication, and Post-Incident Activity—provide a roadmap for organizations to systematically address threats.

Below, I outline how each phase applies specifically to OT environments, ensuring that operational and cybersecurity priorities are aligned:

1. Preparation: This phase focuses on establishing the foundational capabilities needed to respond to potential incidents effectively. Organizations lay the groundwork for their response strategies and ensure readiness to tackle potential threats. Key actions include:

- Conducting risk assessments to identify and prioritize critical assets.
- Developing and regularly test incident response plans to address various attack scenarios.
- Implementing comprehensive training programs for personnel, focusing on incident detection, response protocols, and communication strategies.

2. Detection & Analysis: The goal of this phase is to identify potential incidents, confirm their occurrence, and assess the scope of the impact. This step involves

monitoring and analyzing system activities to uncover suspicious behaviors. Key actions include:

- Using monitoring tools to detect anomalies and unusual activities that might indicate a security event.
- Analyzing logs, alerts, and other diagnostic data to confirm the nature of the incident.
- Performing a root-cause analysis to determine the origin and impact of the incident, differentiating between false alarms and actual threats.

3. Containment & Eradication: Once an incident is confirmed, the focus shifts to containing the threat to prevent it from spreading and eliminating the root cause to avoid recurrence. Key actions include:

- Implementing containment measures, such as isolating affected systems or network segments.
- Removing malicious code, compromised accounts, or other sources of the incident from the environment.
- Ensuring systems are cleaned and patched to prevent similar attacks in the future.

4. Post-Incident Activity: The final phase involves reviewing the incident to identify lessons learned, refine the response plan, and improve organizational readiness for future threats. Key actions include:

- Conducting a thorough post-mortem analysis to document the incident timeline, actions taken, and outcomes.
- Updating incident response policies and procedures based on the findings.
- Sharing insights with relevant stakeholders to foster collaboration and enhance overall cybersecurity resilience.

In addition to these challenges, the three most significant types of cyberattacks on OT environments—Ransomware, False Data Injection, and Changing Process Values Within Threshold (Aurora)—introduce unique complications during incident response:

Ransomware

Ransomware attacks encrypt critical data, disrupting IT and OT systems. In OT environments, SCADA systems often depend on IT infrastructure, and ransomware can render them ineffective. This delays detection, containment, and recovery efforts, increasing downtime and operational risks.

False Data Injection (Stuxnet)

False data injection manipulates SCADA data to deceive operators, causing damage while appearing normal. Detection is complicated as legitimate system logs often appear unaffected. This delays containment and eradication, extending operational disruptions.

Changing Process Values Within Threshold (Aurora)

Aurora attacks exploit subtle process deviations that remain within normal thresholds, making them nearly undetectable with traditional SCADA systems. Misdiagnoses delay containment, and the absence of high-resolution data hampers root-cause analysis, leaving systems vulnerable to repeat attacks.

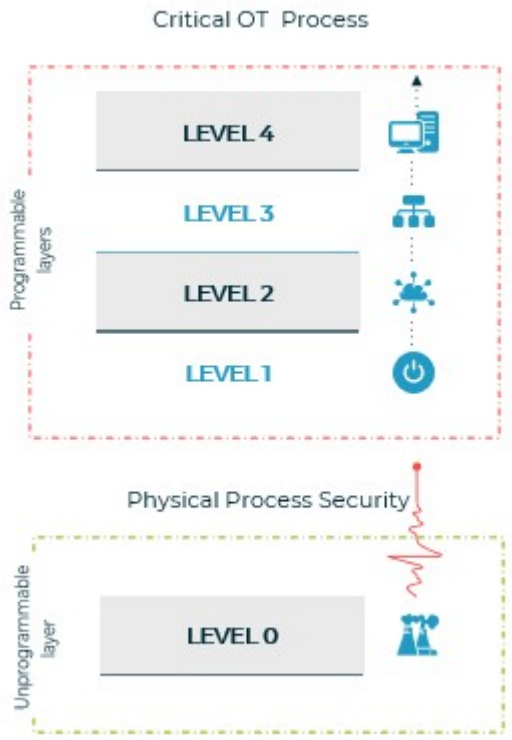
Addressing these challenges requires rethinking IR frameworks to account for the unique demands of OT systems. Process-Oriented approaches bridge these gaps by offering tailored solutions that enhance detection, containment, and recovery for these complex scenarios.

Process-Oriented OT Cybersecurity: A Paradigm Shift

Traditional OT cybersecurity solutions often focus on programmable layers of the Purdue Model (Levels 1-4), such as controllers, networked systems, and IT assets. While these layers are critical, they often overlook the unprogrammable layer, **Level 0**, where physical processes like temperature, pressure, flow rates, and mechanical movements occur. **Process-Oriented cybersecurity** addresses this gap by focusing on **direct monitoring and protection of physical processes**, which form the foundation of critical OT operations.

As depicted in the image below, the programmable layers (Levels 1-4) rely on digital logic and network communications to manage and control operations. These layers are vulnerable to common cyber threats, such as ransomware and data manipulation. Level 0, by contrast, represents the physical layer where processes are executed. It includes **sensors**, which measure environmental variables, and **actuators**, which perform tasks like opening valves or regulating machinery. While critical to operations, these components are often unprogrammable and lack standard

cybersecurity measures like encryption or authentication, making them particularly susceptible to threats such as false data injection or threshold manipulation (e.g., Aurora).



Process-oriented OT cybersecurity integrates **real-time monitoring** of Level 0 data to identify threats that may not be visible at the higher levels. By continuously analyzing operational parameters and comparing them to baseline conditions, this approach enables organizations to detect anomalies indicative of malicious activity. For example:

- **Ransomware**: Maintains operational visibility even when programmable layers like SCADA are compromised.
- **False Data Injection**: Cross-references Level 0 feedback with higher-level instructions to uncover discrepancies and identify malicious manipulation.
- **Aurora Attacks**: Monitors high-resolution data to detect subtle deviations in process thresholds before mechanical damage occurs.

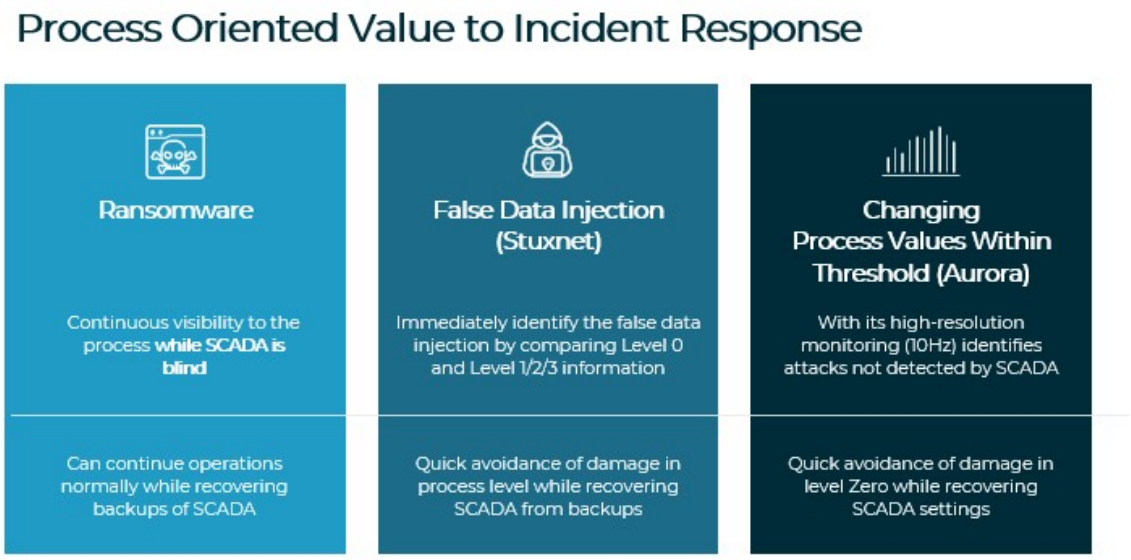
By bridging the gap between the physical process layer (Level 0) and programmable layers (Levels 1-4), process-oriented OT cybersecurity ensures comprehensive protection of both operational integrity and critical infrastructure.

Enhancing the Four Phases of NIST Incident Response

1. **Preparation:** Process-Oriented OT cybersecurity improves organizational readiness by incorporating real-time physical process monitoring into IR planning. Tailored simulations, such as mock ransomware or data manipulation scenarios, enable teams to test and refine their response strategies. This approach ensures that organizations can continue monitoring and managing critical operations even if SCADA systems are compromised.

2. **Detection & Analysis:** Including real-time Level 0 data significantly improves the accuracy of anomaly detection. By comparing Level 0 data with higher-level information (Levels 1/2/3), cyber teams can quickly uncover discrepancies indicative of malicious activity, as seen in false data injection attacks. For example, operators can detect manipulated process data by identifying differences between physical process readings and expected outcomes, enabling faster identification and analysis of threats.

3. **Containment & Eradication:** Process-Oriented OT cybersecurity enables precision containment, isolating affected systems without disrupting broader operations. This approach minimizes collateral impact while facilitating targeted eradication of threats. For instance, high-resolution monitoring allows teams to localize and isolate compromised systems efficiently, ensuring that physical operations continue while mitigation efforts focus on the root cause.
4. **Post-Incident Activity:** Process-level insights greatly enhance post-incident reviews by providing detailed data for root-cause analysis. In the case of an Aurora attack, high-resolution monitoring data can recreate the exact sequence of events, pinpointing how subtle process deviations caused mechanical stress or damage. These insights enable organizations to refine response strategies, adjust operational thresholds, and enhance future detection capabilities, ensuring long-term resilience.



Recognizing the Importance of Process-Oriented OT Cybersecurity

NIST has acknowledged the critical role of Process-Oriented cybersecurity in its publication **NIST SP 800-82r3 (2023)**. This foundational guide provides tailored security measures for OT systems, including ICS and SCADA, emphasizing the protection of physical processes from both internal and external threats. Key recommendations include implementing OT-specific risk management frameworks, real-time monitoring, anomaly detection, and layered defense strategies.

Section 5.3.6 highlights the vulnerabilities at the Field I/O level (Purdue Level 0), where devices like sensors and actuators often lack authentication. This lack of security leaves critical processes exposed to risks such as replay, modification, or spoofing attacks. NIST emphasizes the need for robust controls and continuous monitoring to detect and address these threats effectively.

This recognition by NIST underscores the growing importance of Process-Oriented OT cybersecurity as an essential strategy for protecting critical infrastructure sectors, including energy, water, transportation, and healthcare.

Conclusion

As OT cyberattacks grow more sophisticated, a Process-Oriented approach provides the necessary enhancements to the NIST IR Framework for tackling these unique challenges. By focusing on real-time operational data, this paradigm bridges critical gaps in detection, containment, and recovery, offering resilience in an increasingly volatile threat landscape. For industries dependent on OT systems, adopting these advanced strategies is essential for both compliance and long-term operational security.