SIGA ML²

The Case for Process-Oriented OT Cybersecurity

Water Utility Cyber Attack Scenarios

Contents

Introduction **2**

Process Oriented OT Cyber Security Defined **2**

Multi-Level (Purdue Model Levels 0-4) 2

Machine Learning 3

Alignment to NIST Incident Response Processes **4**

Phase 1: Preparation 4

Real World Examples of Water Utility Cyber Attack Scenarios **6**

Drill-Down into Chemical Dosage Attack Scenario 7

Manipulation of Wastewater PLC 7

Preventing Water Utility Attacks with Process-Oriented OT Cyber Security 9

Conclusion **11**

About SIGA **12**

Introduction

Water and wastewater treatment facilities are essential to maintaining public health and environmental safety. In many countries, including the United States and those in the European Union, these systems are classified as Critical National Infrastructure (CNI), highlighting their crucial role in delivering clean water and managing sanitation services.

Despite advancements in IT cybersecurity, many of the Operational Technology (OT) systems that control water and wastewater processes remain vulnerable to cyber threats. These gaps expose water utilities to attacks that can disrupt operations, lead to contamination, and endanger public safety.

In this document, we explore real-world examples of cyberattacks on water and wastewater systems to demonstrate how Process-Oriented OT Cybersecurity can provide stronger protection. By focusing on safeguarding the physical processes within these facilities, we employ a multi-level strategy across the Purdue model, addressing vulnerabilities from Level 0 (where chemical dosing and pumps are controlled) up to the higher supervisory controls.

Recognizing that breaches are inevitable, this approach emphasizes the importance of robust incident response strategies to reduce service disruptions, prevent contamination, and maintain public trust in water and wastewater services

Process Oriented OT Cyber Security Defined

At a high level, Process-Oriented OT Cybersecurity is a framework for identifying potential cyber disruptions or manipulating industrial processes. This approach is based on two core components: a Multi-Level (Purdue Model) strategy and the use of advanced Machine Learning techniques.

Multi-Level (Purdue Model Levels 0-4)

Unlike traditional cybersecurity methods that offer only a partial view of an ICS, Process-Oriented OT Cybersecurity covers Levels 0-4. This comprehensive view is essential because higher levels of the ICS (Levels 1-4) are more susceptible to manipulation during cyberattacks. For instance, in a false data injection attack where the HMI or PLC is blinded, only an unfiltered view of Level 0 can reveal the true nature of the attack. Level 0 data—directly from physical processes—offers a reliable

baseline against which to verify higher-level information, especially when that data may be compromised.

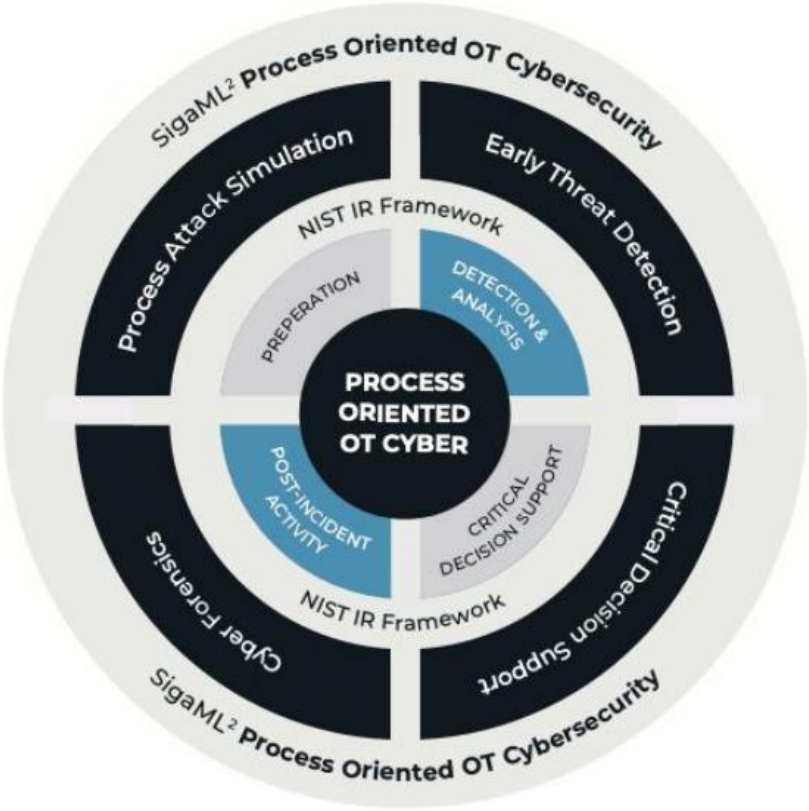
Machine Learning

Suspicious behavior within the ICS is indicative of a potential or ongoing attack. This is critical information can be derived from advanced Machine Learning models, which are applied to vast datasets to detect anomalous patterns both **within** and **between** different levels of the ICS. Unsupervised ML models are used to learn the expected or predicted behavior of an asset or process and then identify deviations from the expected data patterns that are indicative of a potential cyber incident.

Alignment to NIST Incident Response Processes

The **NIST Incident Response (IR) Framework** is a structured approach to handling cybersecurity incidents. It's detailed in NIST Special Publication 800-61, "Computer Security Incident Handling Guide."

Process Oriented OT Cybersecurity provides critical support during each four key phases of the NISR IR framework:



Phase 1: Preparation

The goal is to ensure readiness for handling incidents efficiently by setting up and training an incident response team (IRT), establishing policies, and preparing tools. Injecting simulated anomalies helps train Cyber and Operations teams and develop IR playbooks, all without disrupting ongoing operations.

Phase 2: Detection and Analysis

Involves identifying potential incidents through monitoring and alerts, followed by analyzing their scope and impact. Level 1-4 data is verified using a subset of Level 0 data for real-time attack detection. AI models and the MITRE database classify events as operational or OT cyber breaches, identifying False-Data Injection attacks. This provides IR teams with insights for effective containment.

Phase 3: Containment, Eradication, and Recovery

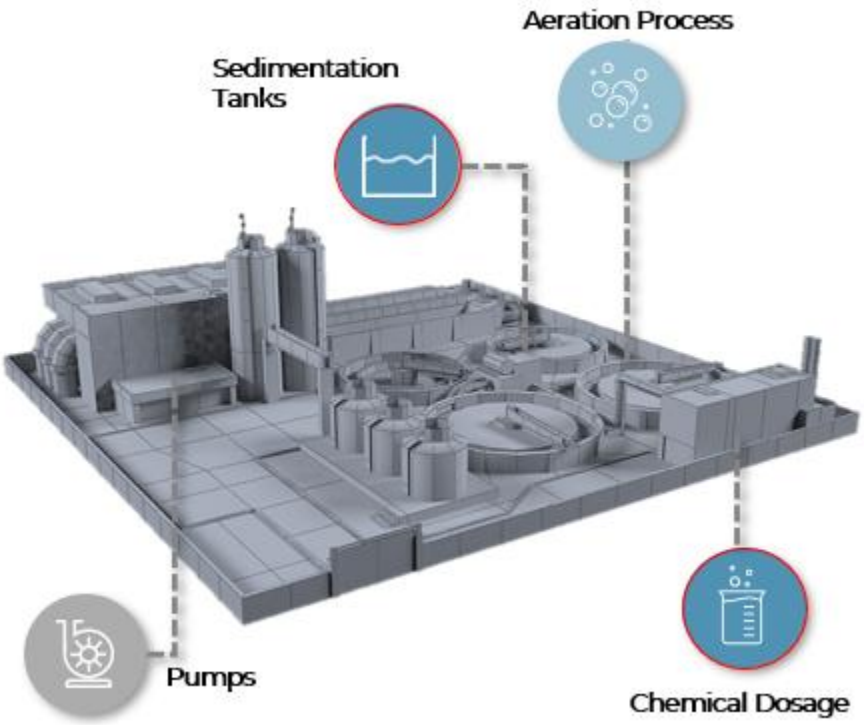
Aims to limit damage, eliminate threats, and restore operations. A real-time decision support system assists in making critical containment choices. Multi-level data offers real-time assessments of physical assets, helping identify attack vectors and aiding in the eradication process.

Phase 4: Post-Incident Activity

Focuses on analyzing the response to understand the incident and evaluate response effectiveness. This phase includes "lessons learned" sessions and updates to the incident response plan to improve future performance and security strategies.

Real World Examples of Water Utility Cyber Attack Scenarios

The following are two examples of potential OT cyberattacks targeting water utilities, illustrating the severity of consequences these attacks can cause:



Example 1: Interference with Sedimentation Tanks

Manipulating the pumps to stop or operate at reduced capacity

Consequence: Untreated sewage accumulates in the system, leading to pipe bursts or the release of raw sewage into local waterways.

Impact: Severe environmental and ecosystem contamination and public health crises due to exposure to untreated waste, and damaged infrastructure.

For more information on how attackers were able to manipulate a Water System PLC, please refer to the Muleshoe, Texas Water Utility Attack of 2024.

Example 2: Targeting Chemical Dosage Process

Altering the chemical dosing process, changing of disinfectants levels

Consequence: Excess or insufficient chemical dosing leads to unsafe water supply

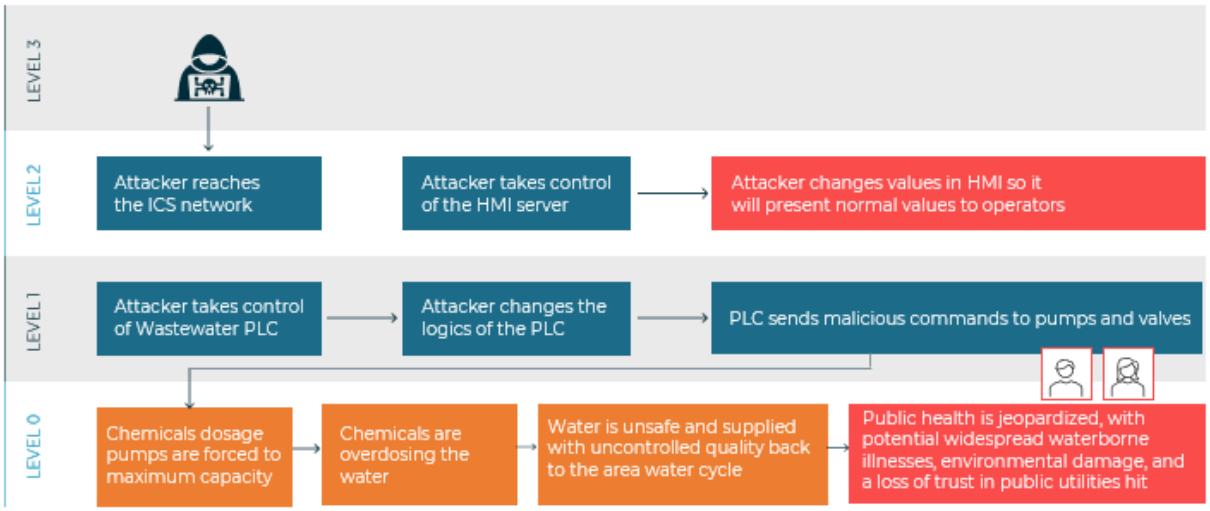
Impact: Public health is jeopardized, with potential widespread waterborne illnesses and environmental damage

Drill-Down into Chemical Dosage Attack Scenario

This scenario outlines a cyberattack on chemical dosage, leading to unsafe water and the potential of widespread waterborne illness and environmental damage. It demonstrates the role of Process-Oriented Cyber OT in Incident Response.

Manipulation of Wastewater PLC

The attacker alters the PLC logic controlling pumps and valves, forcing them to operate at maximum capacity, which results in a dangerous chemical overdose in the water treatment process. This targeted cyberattack disrupts normal operations, and the diagram below shows the attack progression across different ICS Levels, demonstrating how the attacker escalates from network penetration to physical damage in the system.



Level 2: HMI

The attackers gain unauthorized access to the ICS network through a vulnerability or compromised credentials. They then take control of the Human-Machine Interface (HMI) server, a key system used by operators to monitor and control the wastewater treatment process in real-time.

Level 1: PLC

After gaining control of the ICS network and the HMI, the attackers move to take control of the Wastewater PLC, a critical device responsible for executing the physical commands that control pumps and valves in the wastewater treatment process.

Level 0: Chemical Dosage Pumps

The effects of the altered PLC logic become apparent at Level 0, where the physical machinery and pumps are now functioning based on the attacker's commands. The chemical dosage pumps, which regulate the amount of chemicals added to the water to make it safe for public consumption, are forced to run at maximum capacity.

As a result, the water is flooded with excessive chemicals, which leads to the release of unsafe water back into the public water supply system. Operators, unaware of the issue due to the manipulated HMI values, fail to intervene in time. The dangerous water, now contaminated with an overdose of chemicals, enters the broader water cycle, posing severe risks to public health, including potential waterborne diseases and environmental damage. The longer the attack goes unnoticed, the greater the damage to the community's trust in the public utility infrastructure.

Preventing Water Utility Attacks with Process-Oriented OT Cyber Security

To illustrate how a Process-Oriented Cyber OT approach could have mitigated the attack, we align it with each NIST Incident Response (IR) Framework phase.

Preparation: Focuses on readiness to handle incidents. Simulating realistic attack scenarios trains teams to detect and respond effectively.

- **Simulated Anomalies:** Simulating scenarios like chiller pumps at low speeds or altered HMI displays exposes attack symptoms, preparing teams for real incidents.
- **Training Teams:** Training helps teams recognize symptoms like unexpected equipment behavior or discrepancies between process data and HMI displays, enabling early detection.
- **Incident Response Playbooks:** Creating detailed playbooks outlines steps to isolate compromised PLCs, verify HMI data, and mitigate the cooling system's impact.
- **Safe Simulations:** Repeated training with simulations ensures teams can respond effectively without disrupting actual operations.

Detection and Analysis: Identifying incidents quickly through real-time data verification and AI analysis.

- **Verification Using Level 0 Data:** Real-time comparisons between Level 0 and Levels 1-4 data detect discrepancies, like altered HMI values not matching actual pump speeds.
- **AI-Driven Event Classification:** AI models classify anomalies to distinguish between operational issues and cyber breaches, identifying patterns like reduced pump speed as attack indicators.
- **Detection of False-Data Injection:** Comparing real-world data with HMI displays detects false-data injections, flagging attacks even when HMI shows normal conditions.
- **Real-Time Detection:** Continuous monitoring catches anomalies immediately, providing operators with critical time to respond before overheating causes server shutdowns.

Containment, Eradication, and Recovery: Limiting damage, removing the threat, and restoring normal operations.

- **Real-Time Decision Support:** Multi-level visibility enables precise containment decisions. For example, accurate data on chiller pump status helps decide whether to isolate compromised systems.
- **Collaboration Between Teams:** Shared data allows Cyber and Operations teams to jointly decide on containment actions, balancing security and operational continuity.
- **Informed Recovery Decisions:** Real-time assessments of physical assets guide recovery decisions even when SCADA is compromised, ensuring safe operations during the recovery process.

Post-Incident Activity

Involves reviewing incidents and improving future responses based on insights from both physical and cyber operations.

- **Data-Driven Incident Review:** Analyzing data from all levels helps identify what worked and what needs improvement in detection and response.
- **Lessons Learned:** Reviewing discrepancies between Level 0 and HMI data highlights areas for enhancing detection, while decision-making analysis informs better containment strategies.
- **Updating Response Plans:** Insights lead to updated response plans with new strategies and improved communication protocols.
- **Improving Security Strategy:** Implementing additional safeguards and refining AI models strengthens defenses against future threats.

Conclusion

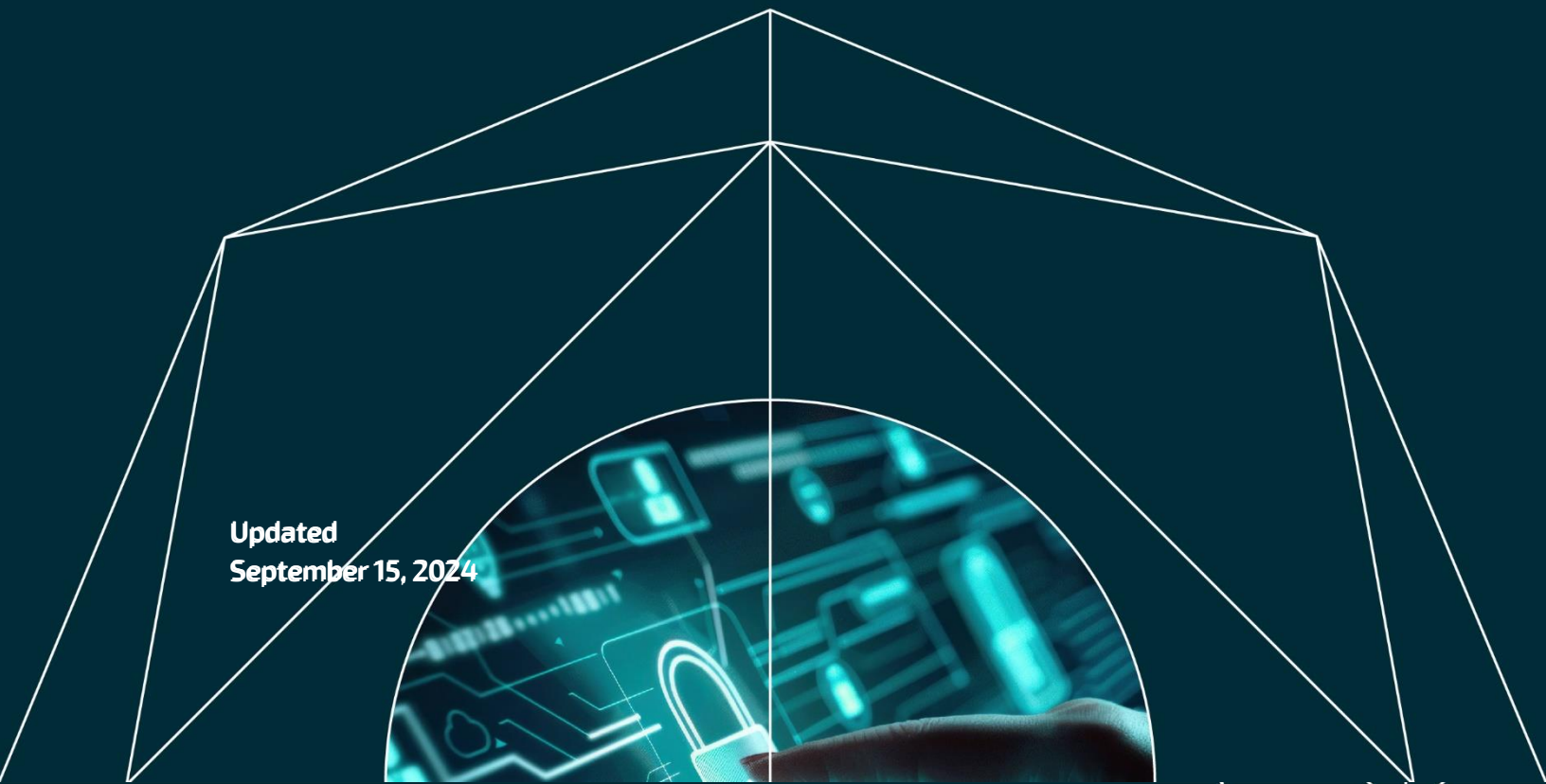
This document highlights the need for a shift to Process-Oriented OT Cybersecurity in response to rising cyberattacks on Water Utilities and critical infrastructure. By using Machine Learning and a Multi-Level strategy, this approach enhances the NIST Incident Response framework across all phases: preparation, detection, containment, and post-incident activity. Simulated attacks, team training, and AI analysis enable more precise threat detection and response. Integrating this method is crucial for bolstering resilience against evolving cyber threats in OT environments.

About SIGA

SIGA's provides a Process-Oriented OT Cybersecurity for real-time decision-making capabilities for managing all Incident Response phases of an OT cyberattack – including Detection, Containment and Cyber Forensics. Unlike other solutions, SIGA detects all expressions of a cyber-attack based on its unfiltered view of all Levels of Cyber OT, including Level Zero visibility.

Founded in 2014, SIGA has global customers in multiple sectors including Oil & Gas, Power Utilities, Data Centers and Water.

For more information visit:
www.sigasec.com



Updated
September 15, 2024