The Case for Process-Oriented OT Cybersecurity

Power Utility Cyber Attack Scenarios

Contents

Introduction

Power utilities are critical to the global economy and are considered Critical National Infrastructure (CNI) in many parts of the world. Despite significant investments in IT cybersecurity, the Operational Technology (OT) systems that control power generation plants, transmission grids, and distribution networks remain vulnerable to cyber threats. This vulnerability exposes the entire power supply chain to risks of attacks that could lead to operational outages, grid instability, and financial losses.

In this document, we examine real-world cyberattacks on power utilities to illustrate how Process-Oriented OT Cybersecurity can provide enhanced protection. Our multi-level strategy secures physical processes across the Purdue model, from Level 0 (where turbines and transformers are controlled) to the higher supervisory controls, helping to prevent catastrophic blackouts and other incidents.

Recognizing that cyber breaches are inevitable, we emphasize the importance of robust incident response measures to minimize downtime, prevent widespread outages, and safeguard the long-term reliability of power utility infrastructures.

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.

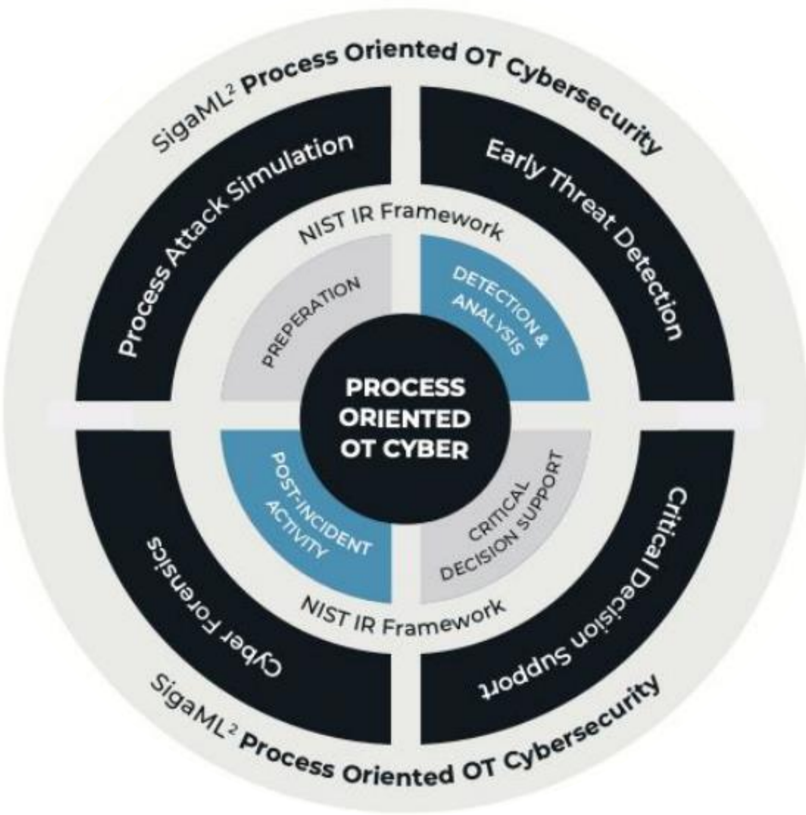
Machine Learning

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

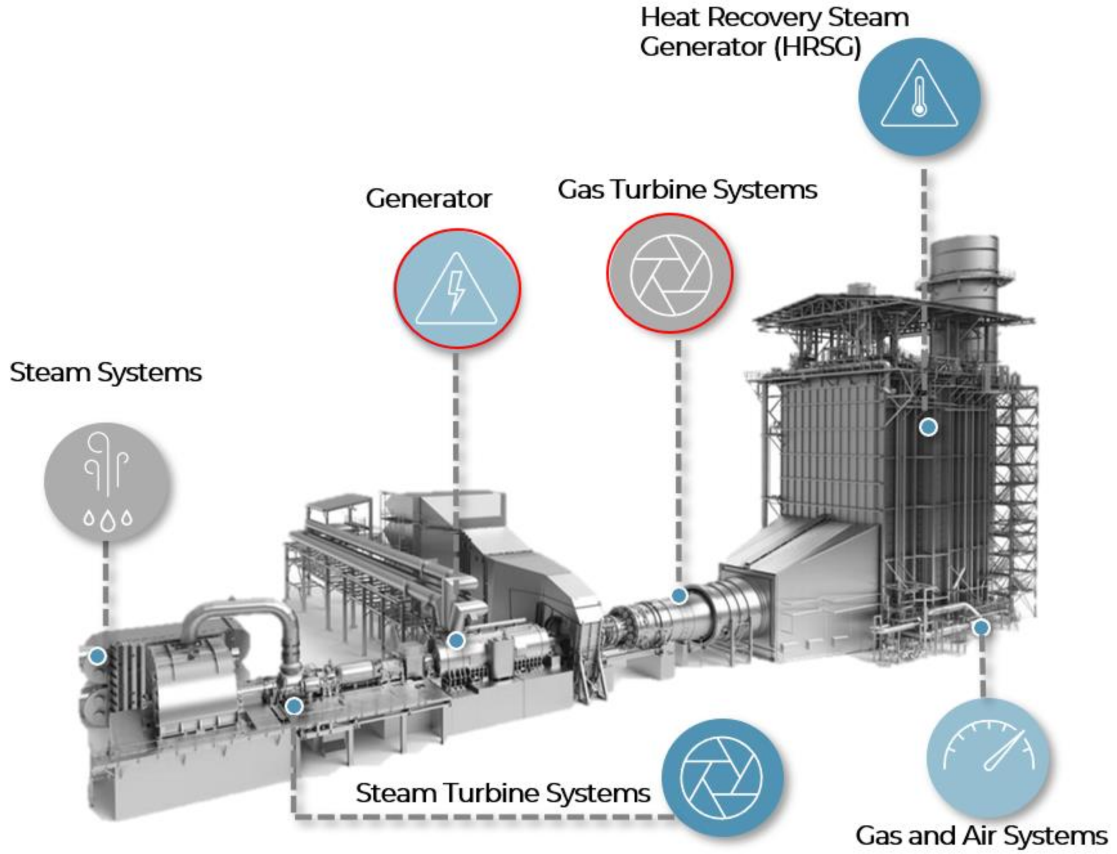
Aims to limit damage, eliminate threats, and restore operations. A real-time decision support system assists in making critical containment choices. Multi-level data offers real-time assessments of physical assets, helping identify attack vectors and aiding in the eradication process.

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 Power Utility Cyber Attack Scenarios

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



Example 1: Targeting the Generator

Deliberate interference with generator excitation system.

Consequence: Disorders in reactive power causing the system to shut down

Impact: Power outage, no power is supplied to the grid.

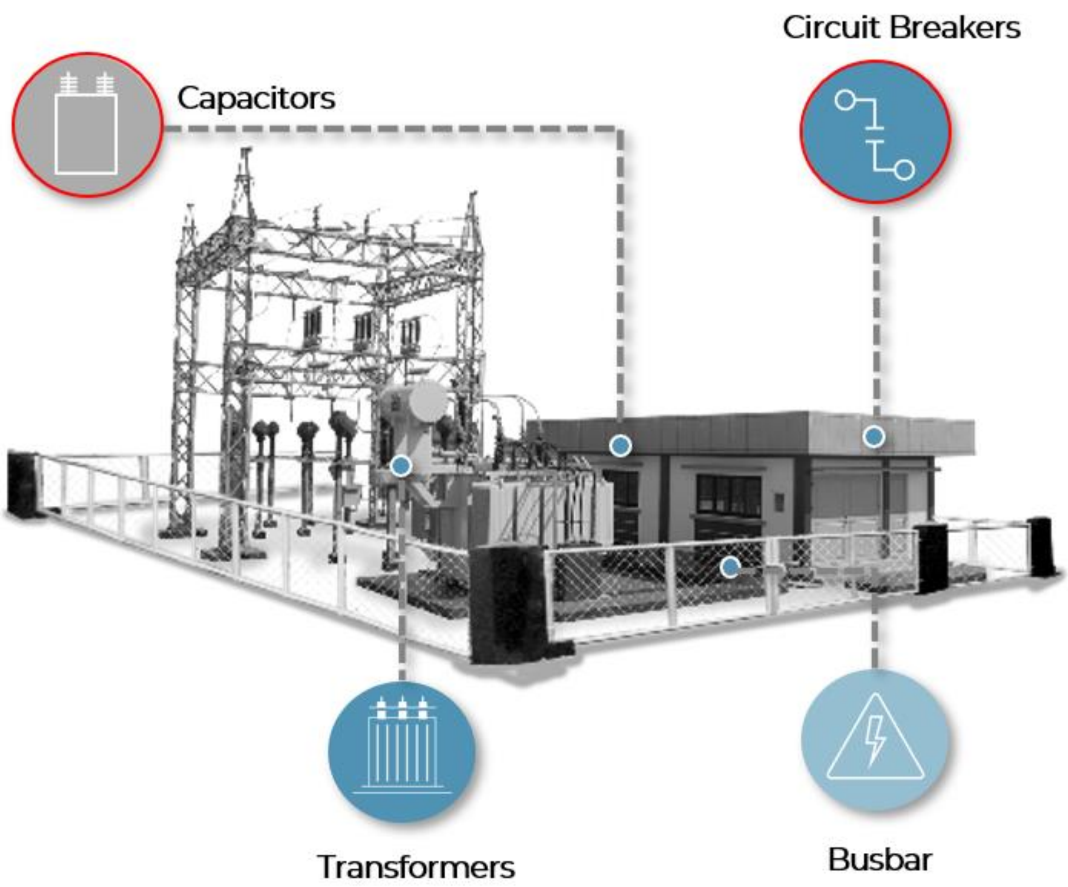
Example 2: Manipulation of the Gas Turbine Systems

Targeting the gas turbine process.

Consequence: Gas overflows, causing an explosion in combustion process.

Impact: Gas turbine suffers severe damage resulting in a power outage.

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



Example 1: Targeting Capacitors

Tampering the capacitors operation sequence

Consequence: Main busbar current and voltage are becoming unstable, causing low quality power supply to the grid

Impact: Unstable power supply to the grid, resulting in power outages.

Example 2: Targeting Circuit Breakers

Targeting the circuit breakers protection devices

Consequence: Circuit breakers are tripped, causing supply lines to be disconnected.

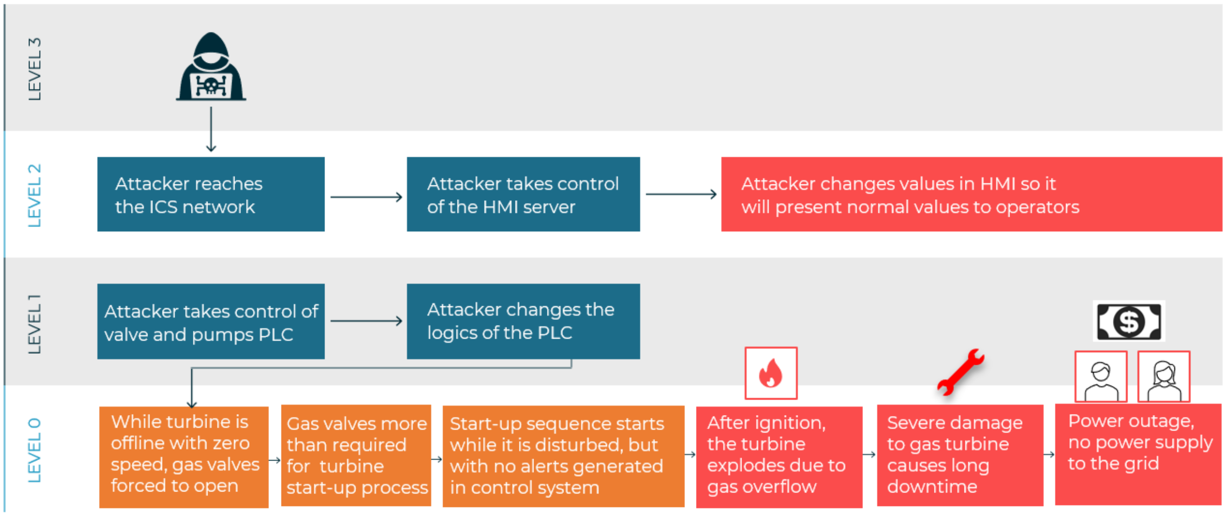
Impact: Power outage in the grid, resulting in a large-scaled blackout.

Drill-Down into Gas Turbine Attack Scenario

This scenario outlines a cyberattack on a gas turbine system, resulting in the incorrect actuation of critical equipment such as valves and pumps. This leads to unsafe conditions, potential operational disasters, and extended downtime for the affected infrastructure. It demonstrates the critical importance of Process-Oriented Cyber OT in incident response and prevention.

Manipulation of the ICS Network

The attacker alters the PLC logic controlling key elements of the gas turbine system, such as valves and pumps. This forces them to operate outside of safe parameters, either opening or closing improperly during crucial stages of the turbine start-up process. The targeted cyberattack leads to severe operational disruptions, and the diagram below illustrates the attack's progression across different ICS levels, showing how the attacker moves from network penetration to causing catastrophic physical and operational damage.



Level 2: HMI

The attackers gain unauthorized access to the ICS network through vulnerabilities or stolen credentials. From there, they seize control of the HMI server, a critical system used by operators to monitor and control the turbine operations in real time. The attackers manipulate the HMI to display normal operational values, concealing their malicious actions from operators, while dangerous conditions are developing.

Level 1: PLC

Following the compromise of both the ICS network and the HMI, the attackers then gain control of the PLCs responsible for managing the turbine's valves and pumps. These PLCs execute the commands that govern critical turbine operations, including gas flow control and start-up sequences.

Level 0: Turbine Operations

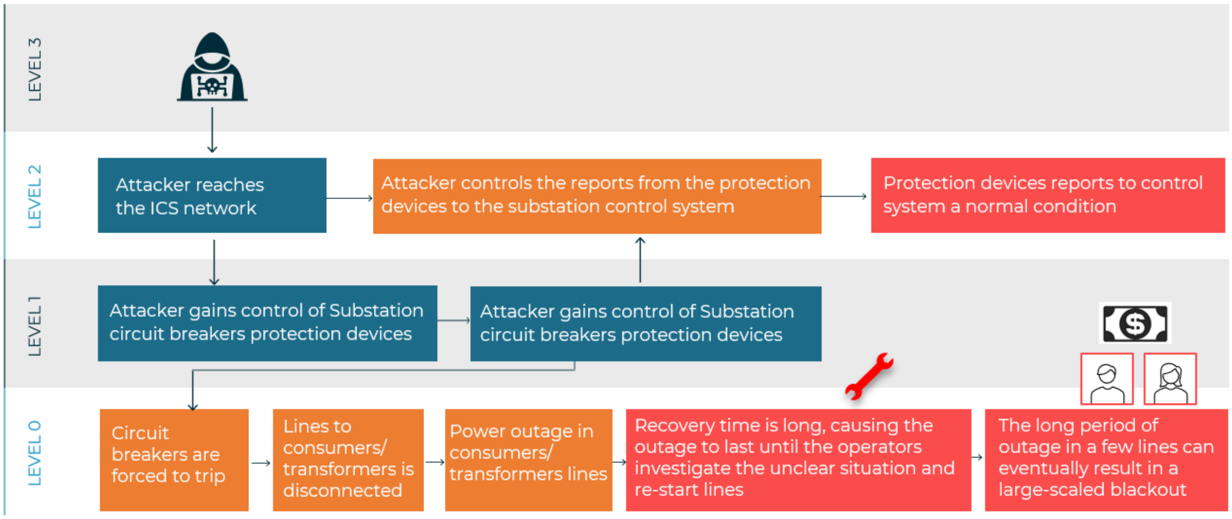
At Level 0, the consequences of the manipulated PLC logic come into full effect. The turbine's valves and pumps respond incorrectly to the attacker's commands—gas valves are forced open while the turbine is offline, allowing gas to flood the system. As the start-up sequence begins under these compromised conditions, the turbine suffers a gas overflow, which leads to a catastrophic explosion. The damage to the turbine results in severe operational downtime, and power is no longer supplied to the grid. The malfunction not only disrupts power generation but also has financial, reputational, and potentially environmental consequences due to prolonged recovery times and the damage caused.

Drill-Down into Substation Attack Scenario

This scenario outlines a cyberattack on a substation's electrical protection system, leading to the incorrect tripping of circuit breakers and a large-scale power outage. The incident reveals the critical role that Process-Oriented Cyber OT security plays in incident response and recovery for power infrastructure.

Manipulation of the ICS Network

The attacker gains access to the ICS network and manipulates the logic within the substation's protection devices. This results in the incorrect tripping of circuit breakers, disconnecting power lines to transformers and consumers. The attack progression is illustrated below, showing how the attacker escalates from network penetration to a large-scale blackout.



Level 2: HMI

The attackers gain unauthorized access to the ICS network, exploiting vulnerabilities or using compromised credentials. They take control of the protection devices' reports sent to the substation's control system, ensuring that the system continues to display normal conditions to the operators. This prevents the detection of the malfunctioning breakers while the attack unfolds.

Level 1: Protection Devices and Circuit Breakers

Once they have control of the ICS network and the HMI, the attackers move on to compromise the substation's protection devices and circuit breakers. They force the breakers to trip unnecessarily, cutting power to vital transmission lines and disrupting power delivery to both transformers and consumers.

Level 0: Physical Impact

At Level 0, the effects of the altered protection logic become visible. Circuit breakers are forced to trip, resulting in the disconnection of power lines. The outage affects a wide area, causing disruptions for consumers and businesses alike. Due to the altered reports at higher levels, the operators are unaware of the true cause of the outage, leading to long recovery times. This delayed response extends the outage, and in some cases, may escalate into a large-scale blackout that could affect multiple areas, creating both financial losses and reputational damage for the affected utility.

Preventing Power 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 Power Utilities. 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