SIGA ML²

The Case for Process-Oriented OT Cybersecurity

Oil and Gas Cyber Attack Scenarios

Contents

Introduction

Oil and gas operations are critical to the global **economy and in many parts of the world considered** Critical National Infrastructure (CNI)**.** Despite significant investments in IT cybersecurity, the Operational Technology (OT) systems that control oil and gas facilities, such as rigs, pipelines, and refineries, remain exposed to cyber threats. This vulnerability puts the entire supply chain at risk of attacks that could cause operational disruptions, environmental damage, and financial losses.

In this document, we examine real-world cyberattacks on oil and gas operations to illustrate how Process-Oriented OT Cybersecurity can offer enhanced protection. Our multi-level strategy focuses on securing physical processes across the Purdue model, from Level 0 (where valves and pumps are controlled) to the higher supervisory controls, helping to prevent catastrophic incidents.

Recognizing that cyber breaches are inevitable, we highlight the importance of having robust incident response measures in place to minimize operational downtime, prevent environmental disasters, and protect the long-term reliability of oil and gas 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

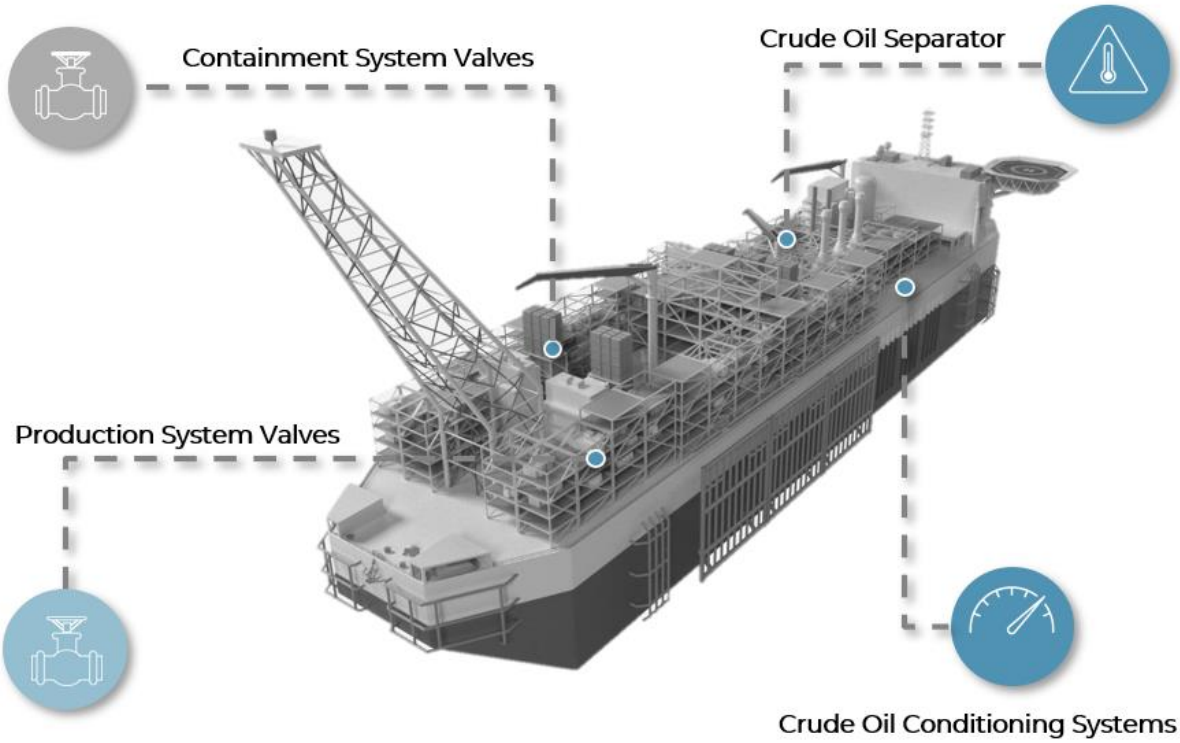
Aims to limit damage, eliminate threats, and restore operations. A real-time decision support system assists in making critical containment choices. Multi-level data offers real-time assessments of physical assets, helping identify attack vectors and aiding in the eradication process.

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 Oil & Gas Cyber Attack Scenarios

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



Example 1: Targeting Crude Oil Separator

Targeting a valve actuator to stop or misdirect flow through valve.

Consequence

- **Process Impact:** Process throughput interrupted; inefficient processing yields out-of-spec hydrocarbon output.
- **Environmental Impact:** Severe environmental and ecosystem contamination and public health crises due to exposure to untreated waste.
- **Infrastructure Damage:** Significant damage to facilities and infrastructure.

Impact

Substantial Financial and Environmental Consequences:

- **Upstream:**
  - Duration: 0.5 to 2.0 days to identify the problem, mitigate it, test it to ensure control has been re-established, and restart systems.
  - Daily Cost: 180,000 Barrels/Day = $10M/Day (based on ~$55/barrel).
- **Downstream:**
  - Downstream operations impacted, resulting in idle facilities and vessels.
  - Daily Cost: Idle shuttle vessels ~$30-50K/Day/Vessel.
- **Environmental Costs:**
  - Severe contamination cleanup and restoration efforts required.
  - Potential legal and reputational damage.

Example 2: Manipulation of the Crude Oil Conditioning Systems

Altering valve actuator to misdirect flow through valve.

Consequence: Loss of process containment allowing hydrocarbon and/or contaminant release.

Impact: Immediate safety hazard for workforce and vessel; potential ongoing environmental, financial, and reputational damage:

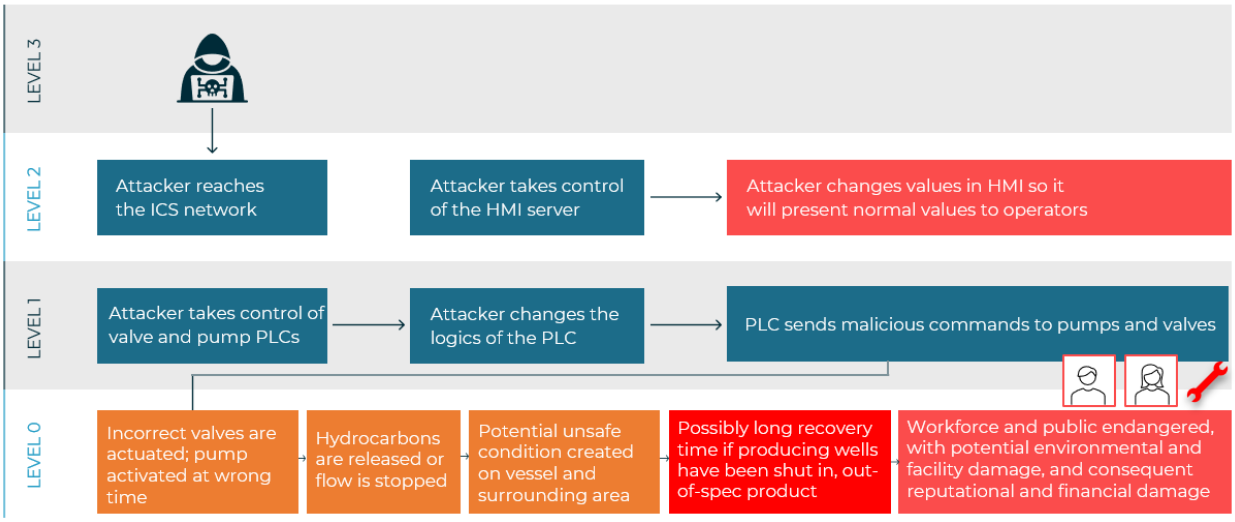
- **Safety damage** (Loss of lives etc.)- Multi Millions $
- **Environmental & Regulatory impact** – contaminants spill like in Deep Water Horizon disaster (Est. $3B)
- **Risk of loss of license-to-operate**
- **Change in future design and FPSO costs** for years ahead

Drill-Down into Crude Oil Separator Attack Scenario

This scenario outlines a cyberattack on a crude oil separation process, resulting in the incorrect actuation of valves and pumps. This could lead to unsafe conditions on production vessels, potential environmental contamination, and long recovery times for oil and gas operations. It demonstrates the critical role of Process-Oriented Cyber OT in Incident Response.

Manipulation of the ICS Network

The attacker alters the PLC logic controlling valves and pumps, forcing them to operate incorrectly, which results in either the release or stoppage of hydrocarbons in the oil separation 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 causing both operational and environmental damage.



Level 2: HMI

The attackers gain unauthorized access to the ICS network through a vulnerability or compromised credentials. They then take control of the HMI server; a critical system used by operators to monitor and control the oil separation process in real-time. The attackers manipulate the HMI to present normal operational values to the operators, concealing the ongoing malicious activities.

Level 1: PLC

After compromising the ICS network and HMI, the attackers proceed to take control of the PLCs that manage critical devices such as valves and pumps within the oil separation process. These PLCs execute the commands that control the physical flow of hydrocarbons.

Level 0: Pumps and Valves

The effects of the altered PLC logic become apparent at Level 0, where the physical pumps and valves respond to the attacker's malicious commands. Valves may actuate incorrectly, and pumps could activate at the wrong times, leading to the unintended release or cessation of hydrocarbon flow. These malfunctions create unsafe conditions on the production vessel or surrounding areas, potentially resulting in environmental damage and long recovery times. If producing wells are shut in and out-of-spec products are generated, the incident could also harm the workforce and public, leading to reputational and financial damage for the organization.

Preventing Oil & Gas 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 Oil & Gas 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