CASE STUDY
SECURING OPERATIONAL TECHNOLOGY
AT AN OIL AND GAS STORAGE STATION

Safeguarding Industry 4.0

Securing the future of tomorrow

Securing Operational Technology at an Oil and Gas Storage Station

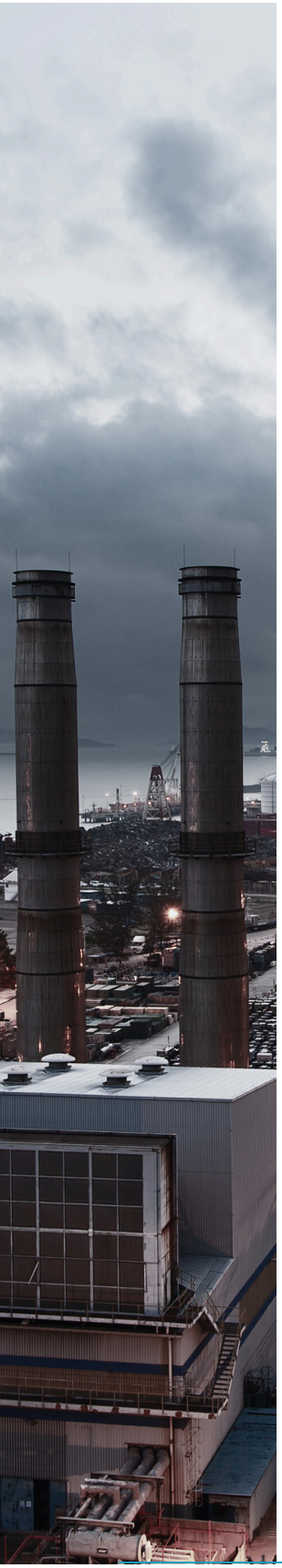
Overview

A major Oil and gas storage station plant based in Abu Dhabi approached DTS Solution to conduct a comprehensive risk assessment and develop an OT security reference architecture aimed at securing their Operational Technology (OT) systems.

As one of the key facilities in the oil and gas supply chain, the storage station faces increasing cyber threats, particularly as industrial control systems (ICS) become more interconnected with enterprise IT networks and external systems. The risk of cyberattacks, which could lead to operational downtime, safety hazards, or environmental disasters, is a significant concern. Additionally, the station must comply with industry regulations and cybersecurity standards specific to critical infrastructure, such as DoE, OTCC, NIST 800-82 and IEC 62443.

The client's goal was to develop a robust cybersecurity architecture that would ensure secure communication between its OT systems, monitor potential cyber threats, and mitigate risks related to both internal and external threats. CS4 - CS4 - DTS Solution was tasked with designing and implementing a tailored solution that would protect the station's critical assets and ensure the station's continued safe operation.

Challenges



Legacy Control Systems

The oil and gas storage station relied on outdated Distributed Control Systems (DCS) and Programmable Logic Controllers (PLCs) ,tank gauge system, custody metering skid, safety instrumented system, and fire and gas detection system that were no longer supported by the manufacturer. These legacy systems lacked modern cybersecurity protocols, increasing vulnerability to cyberattacks targeting critical processes, such as tank monitoring, fuel dispensing systems, and pressure control systems.

Vulnerability in Tank Monitoring and Safety Systems

The station's tank monitoring systems and safety shutdown systems were directly connected to the SCADA network, with minimal network segmentation. This lack of isolation made the systems vulnerable to potential cyber intrusions that could manipulate operational data, such as tank levels and pressure readings, leading to overflows, equipment damage, or even catastrophic failure.

High Risk of Insider Threats and Third-Party Vendor Access

The station regularly worked with third-party contractors and vendors for maintenance and support of its systems. These third parties had remote access to critical OT systems like PLC controllers of safety critical system such as safety instrumented system (SIS) and fire and gas detection systems, and SCADA for centralized remote monitoring and controlling, creating significant security risks if their access credentials were compromised or if contractors inadvertently introduced malware into the network.

Lack of Visibility into OT Environment

The client struggled with limited visibility into the status of its OT systems. The existing monitoring tools were inadequate for detecting anomalies in real-time, such as unauthorized changes to PLC configurations or process parameter manipulation. This made it difficult to quickly respond to potential cyberattacks or equipment failures.

Non-compliance with Cybersecurity Standards

The storage station was not fully compliant with key industry regulations (DoE, OTCC) and cybersecurity standards (NIST 800-82 and IEC 62443). This non-compliance exposed the plant to potential legal penalties, reputational damage, and the risk of regulatory audits, which would have negatively impacted their ability to maintain operations safely and securely.

Integration Challenges with IT Systems

With the growing integration of IT and OT systems, the oil and gas storage station faced difficulties securing the communication pathways between critical control systems and enterprise systems. The lack of a secure data exchange strategy meant that sensitive data, including operational metrics and safety-critical information, was at risk of being intercepted or altered during transmission.

Process Control Inventory

- SCADA System (Supervisory Control and Data Acquisition)
- PLC Systems (Programmable Logic Controllers)
- Tank Management Systems
- Pipeline Monitoring Systems
- Emergency Shutdown Systems
- Distributed Control Systems (DCS)
- Energy Management Systems (EMS)
- Fire and Gas Detection Systems
- Flow Meters and Pressure Sensors
- Vapor Recovery Systems
- Intrusion Detection and Physical Security Systems
- Data Historian Systems
- Remote Monitoring and Telemetry Systems
- Energy Storage System
- Environmental Monitoring Systems (for gas leak detection)
- Alarm Management Systems
- Backup Power and UPS Systems
- Communication Networks (Industrial Ethernet, Modbus, etc.)
- Niterogen Generation Packages

Cybersecurity Risks in the Oil and Gas Storage and Distribution Station.

1. Automated Tank Management Systems

RISK - Cyberattacks targeting tank monitoring systems can manipulate tank levels and flow measurements, leading to overflows, incorrect product distribution, and environmental contamination. Tampering with data could also delay the detection of leaks or hazards, increasing the risk of catastrophic failure.

2. Pipeline and Leak Detection Monitoring Systems

RISK - Unauthorized access to pipeline monitoring systems can allow attackers to alter critical data on pressure levels, flow rates, or valve operations. This could result in pipeline ruptures, leakage, or disruption to the supply chain, causing environmental damage and financial loss.

3. Emergency Shutdown Systems

RISK - If Emergency shutdown systems are compromised, it could prevent automated shutdowns in the event of an emergency, allowing dangerous conditions to persist. Attackers may disable or manipulate these systems, causing explosions, fires, or toxic gas leaks that threaten both human safety and the environment.

4. Fire and Gas Detection Systems

RISK - Tampering with fire and gas detection systems could delay or prevent early warning of hazardous conditions, such as gas leaks or fires, leading to significant operational, safety, and environmental risks. Attackers could disable alarms or manipulate sensors to conceal dangers.

5. Custody metering skids

RISK - Data manipulation in flow meters or pressure sensors can lead to mismanagement of oil and gas flow rates and pipeline pressure levels, potentially causing pipeline ruptures, overpressure incidents, or inaccurate inventory tracking, leading to operational disruptions and environmental hazards.

6. Vapor Recovery Systems

RISK - Cyberattacks on vapor recovery systems could prevent the safe capture and disposal of toxic gases emitted during oil and gas storage operations. This could result in environmental pollution and increased exposure to hazardous vapors, putting both employees and surrounding communities at risk.

7. Intrusion Detection and Physical Security Systems

RISK - Attackers targeting physical security systems (e.g., CCTV cameras, access control systems) could gain unauthorized access to critical infrastructure, bypassing security measures. Physical access could also lead to tampering with operational systems, equipment theft, or malicious sabotage

Approach / Methodology

To address the challenges identified at the oil and gas storage station, CS4 - DTS Solution implemented a comprehensive cybersecurity strategy tailored to the specific needs of the facility. The approach focused on securing the OT systems, ensuring compliance with relevant standards, and enhancing the overall cybersecurity posture of the facility.

1. Vulnerability Assessment and Risk Analysis

CS4 - DTS Solution conducted a thorough vulnerability assessment of the station's SCADA system, PLC controllers, tank management systems, and other critical OT infrastructure. The assessment focused on identifying weaknesses in both legacy systems and newer custody metering skid systems that were not fully integrated with modern security protocols. Additionally, a risk analysis was performed to understand the potential consequences of identified vulnerabilities and guide prioritization for remediation efforts.

2. Network Segmentation and Secure Communication

To reduce the risk of lateral movement in the event of a cyberattack, CS4 - DTS Solution implemented a network segmentation strategy. This involved isolating critical OT systems, such as tank monitoring, PLC controllers, and SCADA systems, from the general IT network and external systems. VLANs and firewalls were used to enforce this segmentation of critical packages such as Tank leak detection. Furthermore, secure communication protocols, such as Transport Layer Security (TLS) and Virtual Private Networks (VPNs), were adopted to protect data transmission across these isolated networks.

3. Asset Management and Visibility

In the OT environment, asset inventory is critical. CS4 - DTS Solution team verified the asset inventory by engaging in discussions with operators, engineers, and site owners to understand the current approach. Additionally, the team collaborated with stakeholders to update the inventory by developing a process control asset inventory, avoid use of active network scanning, which could affect the operation of the storage station

4. Compliance with Regulatory Standards

CS4 - DTS Solution ensured that the station's OT environment was compliant with Department of Energy (DoE) and IEC62443 cybersecurity standards. This involved reviewing the plant's security architecture and operational practices to ensure alignment with regulatory requirements. CS4 - DTS Solution helped implement the necessary controls and processes to meet compliance requirements, including the establishment of strong access control mechanisms, system logging, and data protection practices.

5. Real-Time Threat Detection and Monitoring

Real-time monitoring was implemented using Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) systems. The SIEM system was integrated into the SCADA network to collect and analyze security event data from various OT systems, including PLC controllers, tank management systems, and safety shutdown systems. CS4 - DTS Solution also deployed anomaly detection tools to monitor system behavior for deviations that could indicate potential cyber threats.

Approach / Methodology

6. Intrusion Prevention and Access Control

To prevent unauthorized access to critical OT systems, CS4 - DTS Solution implemented robust access control policies. This included the use of multi-factor authentication (MFA) for remote access to OT systems, and the adoption of role-based access control (RBAC) to restrict access based on job responsibilities. These access control mechanisms helped ensure that only authorized personnel could access sensitive systems such as PLC controllers and SCADA.

7. Backup and Disaster Recovery Planning

CS4 - DTS Solution worked with the client to develop and implement a disaster recovery plan, including regular backups of critical systems and data, such as SCADA configurations, PLC settings, and sensor data. Redundant systems and data pathways were also established to ensure the availability and continuity of operations in the event of a cyberattack or system failure.

8. Employee Training and Awareness

Comprehensive cybersecurity training was provided to all plant employees, focusing on the specific risks associated with oil and gas storage operations. The training covered topics such as phishing attacks, the importance of data integrity, and responding to cybersecurity incidents. Additionally, tabletop exercises were conducted to simulate cyberattack scenarios and improve the response readiness of the plant's staff.

9. Vendor and Third-Party Risk Management

Third-party contractors and vendors who had remote access to critical systems were required to meet specific cybersecurity standards. CS4 - DTS Solution conducted a thorough risk assessment for these third-party vendors, such as OEM of tank gauging system, ensuring they followed proper cyber hygiene practices. Security protocols were implemented for remote access, including MFA and VPNs, to limit external access to sensitive OT systems.

10. Continuous Improvement and Monitoring

To ensure ongoing cybersecurity resilience, CS4 - DTS Solution implemented a continuous security monitoring and improvement process. This included periodic vulnerability scans, penetration testing, and audit reviews of the plant's OT systems. Additionally, real-time data from the SIEM system and network monitoring tools were used to provide insights into emerging threats, allowing the station to quickly adapt to evolving cyber risks to maintain continuous supply of petroleum products to downstream industries.

Successful Impact

1. Reduced Risk to SCADA and PLC Systems

IMPACT - Implementing network segmentation and secure communication protocols (e.g., TLS and VPNs) reduced the risk of unauthorized access and tampering with SCADA and PLC systems by 45%. This prevented potential operational disruptions and safety hazards related to tank monitoring and pressure control systems and fire and gas detection system

2. Minimized Threats to Tank Management and Emergency Shutdown Systems

IMPACT - The introduction of real-time threat detection through IDS, SIEM, and anomaly detection tools reduced the risk of data manipulation in tank monitoring systems and emergency shutdown systems by 40%. This ensured that critical data, such as tank levels and pressure readings, remained accurate, preventing overflows or failure of emergency shutdown systems.

3. Improved Pipeline Integrity and Protection

IMPACT - By implementing multi-factor authentication (MFA) and access control measures, the risk of cyber threats targeting pipeline monitoring systems was reduced by 50%. This safeguarded the safe management of pressure levels and flow rates, significantly decreasing the likelihood of pipeline ruptures or leaks.

4. Secured Remote Access and Vendor Interaction

IMPACT - The introduction of MFA and RBAC for third-party vendors reduced the risk from remote vendor access by 40%. This ensured that external contractors could only access critical OT systems on a need-to-know basis, preventing unauthorized access to key systems like PLC controllers or tank monitoring systems

5. Enhanced Environmental and Gas Leak Detection Systems

IMPACT - Securing environmental monitoring systems and gas leak detection systems reduced the risk of undetected gas leaks or environmental hazards by 35%. Enhanced monitoring and real-time alerts improved the response times to potential leaks, significantly reducing the risk of environmental disasters and improving overall plant safety.

Safeguarding Industry 4.0

CS4 – Cybersecurity for Industry 4.0, a specialized division within DTS Solution, excels in Operational Technology (OT) cybersecurity. With over 15 years of experience safeguarding OT environments across various sectors, CS4 empowers asset owners by enhancing cyber resilience and maturity within their operating environments.

Our Mission

We are dedicated to fortifying industrial operations with advanced cyber defense and comprehensive security programs. Our proactive approach to risk management and threat neutralization ensures that your Industry 4.0 infrastructure operates with resilience and reliability at its core.

Our Services

OT Cybersecurity Advisory & Consulting Services
We provide expert guidance to navigate the complexities of OT security, ensuring compliance and resilience in your critical systems.

OT Cyber Defense and Engineering
Our proactive cyber defense solutions are designed to detect, prevent, and respond to threats targeting your OT environment.

OT Managed Security Services
Through our HawkEye OT platform, we offer centralized monitoring, incident response, and threat hunting to protect your critical infrastructure from cyber threats.

Our Approach

At CS4, we prioritize a process-aware approach to cybersecurity, ensuring that your industrial environment is not only secure but also future-ready. We collaborate closely with asset owners, system integrators, and product suppliers to develop secure control systems and software, fortifying all aspects of your operations against evolving threats.

Partner with CS4 to secure your Industry 4.0 infrastructure and achieve unparalleled cyber resilience in your industrial operations.

info@cs4.io | **www.cs4.io**
HQ: Office 4, Oasis Center, Dubai, UAE