Safeguarding Industry 4.0

Securing the future of tomorrow

Securing Operational Technology in a Liquefied Natural Gas (LNG) Facility

Overview

A prominent Liquefied Natural Gas (LNG) Facility responsible for converting natural gas into liquid form, storing it, and facilitating its transportation sought DTS's expertise to enhance the security of its Operational Technology (OT) systems.

This facility operates critical systems such as liquefaction units, storage tanks, boil-off gas (BOG) compressors, regasification processes, and supervisory control and data acquisition (SCADA) systems. These systems are vital to ensuring the efficient, safe, and continuous production of LNG, as well as meeting international transportation requirements.

As the LNG industry faces growing cyber threats, the facility's OT systems are susceptible to cyberattacks that could cause operational disruption, safety risks, or environmental disasters. The station must also comply with DoE standards and adhere to IEC 62443 for the protection of its infrastructure and to mitigate risks to its operations.

DTS was engaged to implement a comprehensive cybersecurity strategy, focused on securing communications between vital OT systems, enabling continuous threat detection, and ensuring operational continuity while protecting infrastructure from evolving threats.

Client Challenges

Outdated Technology Infrastructure

The facility relied on older OT systems, such as legacy SCADA controllers and unpatched sensors in its liquefaction and storage units. These systems, without modern cybersecurity features, posed a critical vulnerability that could be exploited by sophisticated cyberattacks.

Complex System Integration

The challenge of integrating old infrastructure (such as pressure control valves and legacy metering systems) with new technologies created gaps in security, which exposed the facility to vulnerabilities from legacy equipment interacting with modern control systems.

External Vendor Access Complications

With third-party vendors providing essential remote support and maintenance services for OT systems, the potential for cyberattack vectors due to poor external security measures became a pressing concern.

Regulatory Adherence

The LNG station needed to meet the growing cybersecurity regulations such as DoE directives and IEC 62443, leaving it vulnerable to penalties and operational risks if the regulatory requirements were not fully integrated into the security

Limited Real-Time Threat Monitoring

Due to the absence of a centralized monitoring system, the facility lacked comprehensive visibility into the performance of its critical OT assets, increasing the risk of cyberattack delays and missed early warning signs of threats.

Key Systems and Associated Risks

1. SCADA Systems

RISK - Vulnerable to manipulation, allowing attackers to compromise operations like LNG production or storage control, leading to severe safety risks.

2. Liquefaction Units

RISK - Cyberattacks targeting liquefaction units could compromise the cryogenic processes and endanger LNG production, affecting the entire supply chain..

3. Storage Tanks and Gauging Systems

RISK - The risk of tampering with storage tank levels could lead to inaccurate inventory data, tank overflows, and unsafe storage conditions

4. Boil-Off Gas Compressors

RISK - If BOG compressors are compromised, it could result in a failure to manage pressure in the LNG storage process, causing inefficiencies or safety hazards.

5. Regasification Units

RISK - Manipulation of regasification units could disrupt the regasification process, affecting the supply of natural gas to consumers or causing environmental harm.

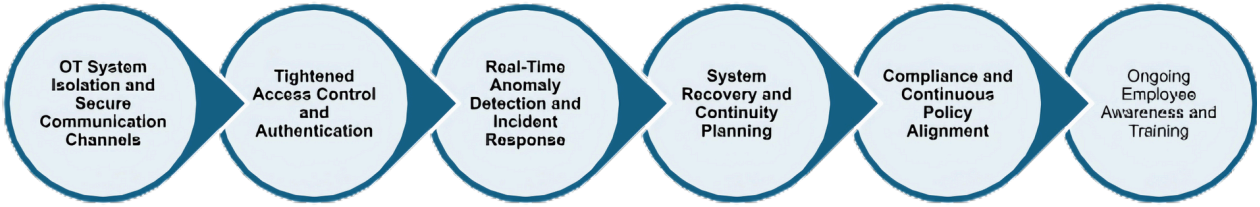
6. Fire and Gas Detection Systems

RISK - An attack on fire detection systems could cause critical delays in responding to fires or gas leaks, leading to catastrophic consequences.

Emergency Shutdown Systems (ESD)

RISK - A compromised ESD system would delay safety actions in case of operational anomalies, increasing the risk of disastrous situations

Approach / Methodology



1.OT System Isolation and Secure Communication Channels

The first step was to establish network segmentation between the Operational Technology (OT) and Information Technology (IT) networks, minimizing the risk of lateral movement in case of a breach. Secure communication protocols such as VPNs and multi-factor authentication (MFA) were applied to safeguard critical access, especially for third-party vendors requiring remote monitoring capabilities.

DoE Alignment

- **Operational Network Segmentation: This initiative follows DoE's security principle of isolating OT systems from IT to prevent a single attack vector from compromising both networks. The segmentation protects high-risk systems, such as liquefaction units and SCADA, by isolating them from broader network threats.**

---

2. Tightened Access Control and Authentication

The LNG facility enforced strict access control policies by implementing role-based access control (RBAC) and least privilege access. Vendor and employee access to OT systems was restricted based on job responsibilities, ensuring minimal exposure of critical control systems. To enhance security, multi-factor authentication (MFA) was deployed for all remote vendor access.

DoE Alignment

- **Access and Identity Management: This aligns with DoE guidelines that stress the need to ensure that only authorized personnel can access critical systems. RBAC and MFA reduce the risk of unauthorized access and mitigate insider threats.**

---

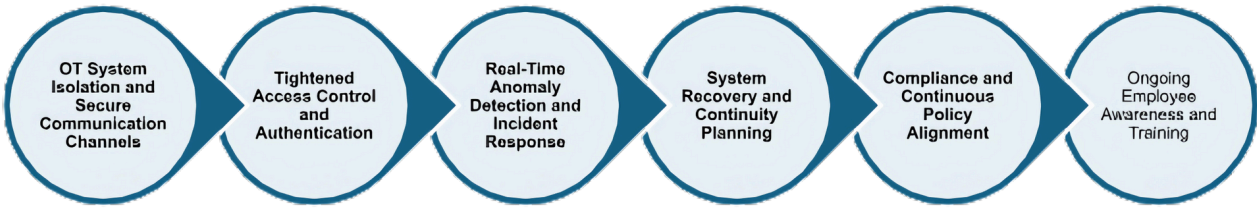
3. Real-Time Anomaly Detection and Incident Response

The LNG facility enforced strict access control policies by implementing role-based access control (RBAC) and least privilege access. Vendor and employee access to OT systems was restricted based on job responsibilities, ensuring minimal exposure of critical control systems. To enhance security, multi-factor authentication (MFA) was deployed for all remote vendor access.

DoE Alignment

- **Real-Time Threat Detection: The implementation of SIEM systems and continuous monitoring is a direct application of the DoE's strategy to detect and respond to cyber threats before they cause harm, providing real-time visibility into the facility's critical OT operations.**

Approach / Methodology



4. System Recovery and Continuity Planning

A robust disaster recovery plan was put in place, allowing for the quick restoration of key OT systems in the event of a cyberattack or system failure. The facility integrated offline backups for critical configurations, ensuring that system data could be recovered to a safe state. Simulated cyberattack scenarios, including failures in fire & gas detection or regasification systems, were used to test recovery protocols.

DoE Alignment

- **Business Continuity and Disaster Recovery: This initiative follows DoE's recommendation of having an effective recovery strategy that ensures the LNG station can maintain safe operations even in the event of a major disruption.**

---

5. Compliance and Continuous Policy Alignment

All measures were aligned with DoE's cybersecurity domains, and the facility's security policies were updated to comply with IEC 62443. Regular audits and vulnerability assessments were conducted to ensure ongoing compliance with both national and international standards.

DoE Alignment

- **Regulatory Compliance: The LNG facility's adherence to DoE's cybersecurity framework guarantees regulatory compliance, mitigating the risk of legal repercussions and ensuring that security practices are aligned with global standards.**

---

6. Ongoing Employee Awareness and Training

The facility implemented an extensive cybersecurity training program for employees and third-party contractors. The training covered critical OT systems, such as SCADA, liquefaction, and storage units, with a focus on recognizing potential threats, phishing prevention, and how to report suspicious activity. Additionally, scenario-based tabletop exercises were held to practice responding to cyberattacks.

DoE Alignment

- **Training and Cybersecurity Awareness: This aligns with DoE's emphasis on educating staff and contractors to identify and mitigate cyber threats, ensuring that everyone at the LNG facility is prepared for potential cyberattacks.**

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.