Safeguarding Industry 4.0

Securing the future of tomorrow

Securing Operational Technology in an LPG (Liquefied Petroleum Gas) Facility

Overview

An LPG (Liquefied Petroleum Gas) Facility, responsible for the storage, distribution, and transportation of LPG to various sectors, approached DTS to enhance the security of its Operational Technology (OT) systems. The facility operates several critical systems, including dehydration system, liquification system, Emergency Shutdown System (ESD), Fire and Gas system ,tank monitoring, loading and unloading systems, pressure control systems, SCADA, Distributed Control Systems (DCS) and custody metering skids. These systems ensure the safe, efficient, and uninterrupted production of LPG and continuous flow of LPG from storage tanks to distribution points, while also maintaining strict safety standards to prevent hazardous incidents.

Given the highly volatile nature of LPG, the facility faces considerable cybersecurity risks. A cyberattack on any of these critical OT systems could lead to catastrophic safety incidents, including gas leaks, explosions, or significant disruptions in the supply chain. The facility also needs to comply with stringent DoE cybersecurity regulations and IEC 62443 standard to safeguard its infrastructure and mitigate potential risks.

DTS was tasked with designing a robust cybersecurity strategy that would secure communications between critical OT systems, provide real-time threat detection, and ensure the ongoing safety and efficiency of the LPG facility's operations.

Client Challenges

Aging Infrastructure and Legacy Systems

Many of the LPG facility's OT systems, such as tank monitoring systems and PLC controllers of ESD and fire and gas ,were based on outdated technologies, leaving them vulnerable to potential cyberattacks due to a lack of modern cybersecurity defenses.

Lack of Network Segmentation

The facility's OT systems were not adequately segmented from the IT network through dual home computers for transferring process data in real time to IT, creating risks that cyber threats targeting the IT network could spread to the critical OT systems controlling safety and operational processes.

Vendor Access and Remote Maintenance Risks

External vendors provided remote maintenance and diagnostic services, raising concerns about unauthorized access and potential exploitation of remote connections.

Regulatory Compliance Challenges

The LPG facility was required to comply with DoE cybersecurity regulations and IEC 62443, which govern the safety and security of industrial control systems. Failure to comply could result in severe penalties, increased vulnerability to cyber threats, and jeopardized safety.

Limited Real-Time Threat Detection and Monitoring

The facility had insufficient centralized monitoring and lacked real-time visibility into the health and status of critical OT systems such as DCS and SCADA, increasing the risk of delayed detection and response to cybersecurity incidents.

Key Systems and Associated Risks

1. SCADA Systems

RISK - Vulnerable to cyberattacks that could manipulate operational data and system controls, such as pressure control in storage tanks or valve operations during loading/unloading, potentially causing dangerous conditions.

2. Pressure Control Systems

RISK - Compromise of pressure control systems could lead to unsafe pressure conditions in tanks, resulting in leaks, explosions, or equipment failures due to overpressure or underpressure.

3. Tank Monitoring Systems

RISK - Manipulation of tank level data could cause inaccurate readings, potentially leading to overflows or dangerous underfilling of tanks, increasing operational risk.

4. Fire and Gas Systems

RISK - Unauthorized manipulation of gas detection thresholds or disabling fire detection loops could have a catastrophic impact on plant safety due to delay or prevention of critical alarms and automatic shutdown systems which significantly increase the risk of fires, gas leaks, or explosions.

5. Loading/Unloading Systems

RISK - Cyberattacks targeting these systems could disrupt the logistics of LPG delivery, leading to delays, inventory inaccuracies, or unsafe loading/unloading operations.

6. Emergency Shutdown Systems (ESD)

Compromise of ESD systems could delay safety responses in emergencies, such as excess operating pressure of storage tanks, Pipeline rupture, leaks or fires, potentially putting both personnel and infrastructure at risk.

7. Communication Networks

RISK - Attacks on communication protocols could disrupt real-time data exchange between OT systems, delaying operational responses and increasing the chance of unsafe conditions and disrupting production and supply of LPG.

7. Gas Analyzers

RISK - Unauthorized access or manipulation of gas analyzers such as gas chromatographs, can result in inaccurate readings of gas compositions which may lead to incorrect operational decisions, causing the production of off-spec products and miscalculated quantities, potentially resulting in significant financial losses and reputational damage.

9. Custody Metering Skids

RISK - Unauthorized manipulation of flow computer configurations can result in inaccurate calculation of LPG. Which can directly lead to financial discrepancies, loss of revenue, and legal or contractual disputes due to incorrect product quantity calculations.

Approach / Methodology

1. Network Segmentation and Secure Communication

To reduce the risk of a cyberattack spreading from IT to OT systems, network segmentation was implemented, isolating critical OT systems such as SCADA, pressure control system , ESD, and tank monitoring from the broader IT network. Secure communication protocols, including VPNs with multi-factor authentication (MFA), were deployed to protect remote access by external vendors and contractors.

DoE Alignment:

- **OT Network Segmentation**: The implementation of network segmentation aligns with DoE's guidelines for isolating OT systems from IT networks, which minimizes the risk of cross-network contamination in the event of a cyberattack.

2. Role-Based Access Control (RBAC) and Authentication

The LPG facility implemented RBAC to ensure that only authorized personnel had access to critical OT systems based on job responsibilities such as liquification package control system, DCS and SCADA. MFA was enforced for all remote connections, and least privilege principles were applied to limit the access of users to only the systems necessary for their roles.

DoE Alignment:

- **Access Control and Identity Management**: RBAC, MFA, and least privilege access align with DoE's emphasis on controlling access to OT systems and ensuring that only authorized personnel can make changes to critical systems, reducing both insider and outsider threats.

3. Real-Time Monitoring and Threat Detection

A Security Operations Center (SOC) was established, and a Security Information and Event Management (SIEM) system was integrated into the OT systems for continuous monitoring without affecting OT' availability or integrity. The SIEM system tracked data from tank monitoring, pressure control systems, and loading/unloading systems, enabling real-time detection of anomalies or cyber threats. Alerts were set up for any unauthorized access or suspicious behavior, ensuring swift responses.

DoE Alignment:

- Real-Time Monitoring and Anomaly Detection: Integrating SIEM systems and continuous monitoring follows DoE's directive for constant vigilance over OT environments to detect threats early and allow for timely mitigation.

Approach / Methodology

4. Incident Response and Recovery Planning

DTS helped develop a comprehensive incident response plan tailored to the LPG facility's OT systems, covering scenarios such as cyberattacks on pressure control systems or ESD failure. The plan included automated isolation of compromised systems, followed by a step-by-step recovery process. Backup and disaster recovery measures were also implemented to ensure the restoration of critical system configurations in the event of an attack.

DoE Alignment:

- The incident response and recovery plan aligns with DoE's recommendations for ensuring business continuity, minimizing downtime, and restoring normal operations in the event of a cyberattack.

5. Compliance with Industry Standards

The LPG facility's cybersecurity measures were mapped to DoE cybersecurity regulations and IEC 62443 standard, ensuring full compliance with regulatory requirements. The facility underwent regular audits and security assessments to maintain its readiness for inspections and to identify and address emerging vulnerabilities.

DoE Alignment:

- Regulatory Compliance and Security Policies: Mapping security controls to DoE regulations and IEC 62443 standard ensures the LPG facility meets regulatory requirements and mitigates the risk of legal penalties and operational disruptions due to non-compliance.

6.Training and Cybersecurity Awareness

A comprehensive cybersecurity training program was implemented for all staff form operation and maintenance teams, focusing on OT systems like SCADA,ESD, pressure control, and loading/unloading systems. Training also emphasized the importance of recognizing phishing attempts, maintaining system integrity, and reporting suspicious activities. Additionally, scenario-based exercises were conducted to prepare staff for potential cyberattacks such as ransomware attack affecting DCS operator workstations.

DoE Alignment:

- Training and Cybersecurity Awareness: DoE's framework highlights the importance of staff training, and this initiative ensures that all personnel are equipped to identify and respond to cybersecurity incidents effectively.

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.