QATAR GAS TERMINAL SECURITY ASSESSMENT REPORT

CONFIDENTIAL AND PRIVILEGED

Prepared by: DeepShield Systems, Inc.

Report Date: January 10, 2024

Reference: QGT-SA-2024-001

1. EXECUTIVE SUMMARY

This security assessment report documents the comprehensive evaluation of operational technology (OT) security controls and cybersecurity infrastructure at the Qatar Gas Terminal Complex ("QGT") conducted by DeepShield Systems, Inc. ("DeepShield") between November 15-30, 2023. The assessment focused on critical control systems, SCADA networks, and industrial automation infrastructure supporting LNG processing and storage operations.

2. SCOPE OF ASSESSMENT

1. Physical Infrastructure Evaluated

- Main Control Room (MCR) systems and networks
- Emergency Shutdown Systems (ESD)
- Distributed Control Systems (DCS)
- Terminal Automation Systems (TAS)
- Loading/unloading control systems
- Storage tank monitoring systems
- Fire and gas detection networks

2. Network Architecture Review

- OT network segmentation
- Industrial protocol security
- Remote access systems
- Wireless infrastructure
- Backup and redundancy systems

3. METHODOLOGY

1. Assessment Framework

Assessment conducted using DeepShield's proprietary Deep-Layer Security Architecture(TM) methodology, incorporating:

- ISA/IEC 62443 standards
- NIST Cybersecurity Framework
- API 1164 Pipeline SCADA Security guidelines
- Qatar Energy Security Standards

2. Testing Procedures

- Network architecture analysis
- Control system vulnerability assessment
- Protocol analysis
- Access control review
- Incident response capability evaluation
- Recovery procedures assessment

4. KEY FINDINGS

1. Critical Vulnerabilities

- Outdated firmware versions on 23% of PLCs
- Insufficient network segmentation between corporate and OT networks
- Unencrypted MODBUS communications on legacy systems
- Default credentials found on 3 remote terminal units

2. High-Risk Issues

- Limited monitoring of east perimeter network traffic
- Incomplete patch management procedures
- Non-redundant communication paths to storage area networks
- Aging automation hardware approaching end-of-support

3. Medium-Risk Issues

- Inconsistent access control documentation
- Informal change management procedures
- Limited security awareness training

- Incomplete asset inventory

5. DETAILED RECOMMENDATIONS

1. Immediate Actions (0-3 months)

Implement enhanced network segmentation

Update PLC firmware to current secure versions

Deploy encrypted protocols across all control systems

Establish formal patch management program

Implement comprehensive access control system

2. Short-Term Actions (3-6 months)

Deploy additional network monitoring solutions

Upgrade automation hardware

Enhance backup communication infrastructure

Implement formal change management procedures

Develop comprehensive asset inventory

3. Long-Term Actions (6-12 months)

Establish security operations center

Implement advanced threat detection

Deploy AI-driven anomaly detection

Enhance disaster recovery capabilities

Develop comprehensive training program

6. IMPLEMENTATION ROADMAP

1. Phase 1: Critical Security Enhancement

- Timeline: Q1-Q2 2024
- Estimated Budget: $2.8M USD
- Key Deliverables: Network segmentation, firmware updates, encryption deployment

2. Phase 2: Infrastructure Modernization

- Timeline: Q2-Q3 2024

- Estimated Budget: $3.5M USD
- Key Deliverables: Hardware upgrades, monitoring solutions, backup systems

3. Phase 3: Advanced Security Implementation

- Timeline: Q3-Q4 2024
- Estimated Budget: $4.2M USD
- Key Deliverables: SOC establishment, AI implementation, training program

7. RISK ASSESSMENT MATRIX

1. Current Risk Profile

- Critical: 4 findings
- High: 4 findings
- Medium: 4 findings
- Low: 6 findings

2. Post-Implementation Risk Profile

- Critical: 0 findings
- High: 0 findings
- Medium: 2 findings
- Low: 4 findings

8. LEGAL DISCLAIMERS

This report is provided pursuant to the Master Services Agreement between DeepShield Systems, Inc. and Qatar Gas Terminal dated October 1, 2023. The information contained herein is confidential and proprietary. This assessment represents a point-in-time evaluation of security controls and may not reflect current conditions. DeepShield makes no warranties, express or implied, regarding the completeness or accuracy of this assessment.

9. CERTIFICATION

This security assessment report has been prepared and reviewed by qualified DeepShield security professionals in accordance with industry standards and best practices.

Prepared by:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Reviewed by:

James Morrison

VP of Engineering

DeepShield Systems, Inc.

Date: January 10, 2024

[END OF REPORT]