ISA/IEC 62443 Security Level Assessment Report

DeepShield Systems, Inc.

Assessment Date: January 11, 2024

Document Reference: DSS-SL-2024-001

1. Executive Summary

This document presents the formal security level assessment of DeepShield Systems, Inc.'s Industrial Control System (ICS) security platform and associated products according to the ISA/IEC 62443 series of standards. The assessment evaluates compliance with Security Levels (SL) as defined in ISA/IEC 62443-3-3 and determines the achieved security level for each fundamental requirement.

2. Scope of Assessment

1. Products Assessed:

- DeepShield ICS Security Platform v4.2
- DeepShield Maritime Protection Module v2.1
- DeepShield SCADA Defense Suite v3.5
- DeepShield OT Network Monitor v4.0

2. Assessment Parameters:

- System Requirements (SR) as defined in ISA/IEC 62443-3-3
- Component Requirements (CR) as defined in ISA/IEC 62443-4-2
- Development Requirements (DR) as defined in ISA/IEC 62443-4-1

3. Security Level Definitions

1. Security Level 1 (SL-1): Protection against casual or coincidental violation

2. Security Level 2 (SL-2): Protection against intentional violation using simple means

3. Security Level 3 (SL-3): Protection against intentional violation using sophisticated means

4. Security Level 4 (SL-4): Protection against intentional violation using sophisticated means with extended resources

4. Assessment Results

1. Fundamental Requirements Assessment:

Requirement Category	Achieved SL	Target SL	Status
Identification and Authentication Control	SL-3	SL-3	Compliant
Use Control	SL-3	SL-3	Compliant
System Integrity	SL-4	SL-3	Exceeds
Data Confidentiality	SL-3	SL-3	Compliant
Restricted Data Flow	SL-3	SL-3	Compliant
Timely Response to Events	SL-4	SL-3	Exceeds
Resource Availability	SL-3	SL-3	Compliant

5. Detailed Findings

1. Areas of Excellence:

- Advanced threat detection algorithms exceed SL-3 requirements
- Real-time monitoring capabilities surpass standard response time metrics
- Multi-layer authentication protocols provide enhanced security
- AI-driven anomaly detection demonstrates superior system integrity

2. Areas for Monitoring:

- Continuous validation of cryptographic implementations
- Ongoing assessment of supply chain security controls
- Regular review of access control mechanisms
- Periodic evaluation of backup and recovery procedures

6. Compliance Statement

Based on the comprehensive assessment conducted, DeepShield Systems, Inc.'s products meet or exceed the Security Level 3 (SL-3) requirements as specified in ISA/IEC 62443. This assessment confirms the platform's capability to protect against sophisticated cyber threats targeting industrial control systems and critical infrastructure.

7. Validity and Conditions

1. This assessment is valid for twelve (12) months from the date of issuance.

2. The assessment remains valid provided that:

- No significant changes are made to the assessed products
- All security patches and updates are properly implemented
- Regular security maintenance procedures are followed
- No major security incidents occur that compromise the system

8. Legal Disclaimers

1. This assessment represents the security level status at the time of evaluation and does not guarantee future performance or security levels.

2. DeepShield Systems, Inc. maintains responsibility for:

- Maintaining the assessed security levels
- Implementing security updates and patches
- Monitoring and responding to security threats
- Adhering to all applicable security standards and regulations

9. Authorization

Assessed by:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Verified by:

James Morrison

VP of Engineering

DeepShield Systems, Inc.

Approved by:

Sarah Blackwood

Chief Technology Officer

DeepShield Systems, Inc.

Date: January 11, 2024

Location: Wilmington, Delaware

[DOCUMENT ENDS]