IEC 62443 Implementation Evidence Package

DeepShield Systems, Inc.

Document Reference: IEC-62443-EV-2024-001

Version 1.2 | January 11, 2024

1. Executive Summary

This Implementation Evidence Package documents DeepShield Systems, Inc.'s ("DeepShield") compliance with IEC 62443 standards for industrial automation and control systems security. This package provides comprehensive evidence of conformance across all applicable requirements for our integrated industrial cybersecurity platform and associated services.

2. Scope of Implementation

1. This evidence package covers the following DeepShield products and systems:

- DeepShield OT Security Platform v4.2
- Maritime Defense Module v2.1
- Subsea Protection Suite v1.8
- SCADA Shield Component v3.5
- Industrial Network Monitor v4.0

2. Implementation Boundaries:

- Control system integration points
- Network security architecture
- System hardening measures
- Access control mechanisms
- Threat detection systems
- Incident response protocols

3. Compliance Framework

1. Primary Standards Referenced:

- IEC 62443-2-4: Security program requirements for IACS service providers
- IEC 62443-3-3: System security requirements and security levels

- IEC 62443-4-1: Secure product development lifecycle requirements
- IEC 62443-4-2: Technical security requirements for IACS components

2. Security Level Achievement:

- SL 3 capability for core platform components
- SL 4 capability for critical infrastructure implementations
- SL 2 capability for auxiliary systems

4. Technical Controls Implementation

1. Identification and Authentication Control

- Multi-factor authentication implementation
- Role-based access control (RBAC) framework
- Privileged access management system
- Certificate-based device authentication

2. Use Control

- Session management protocols
- Concurrent session controls
- Remote access security measures
- Mobile code restrictions

3. System Integrity

- Input validation mechanisms
- Error handling procedures
- Session authenticity verification
- Message integrity checking

4. Data Confidentiality

- Encryption standards implementation
- Key management procedures
- Data-at-rest protection
- Communication channel security

5. Development Process Evidence

1. Security Development Lifecycle

- Threat modeling documentation
- Security requirements traceability
- Code review procedures
- Security testing protocols

2. Configuration Management

- Version control implementation
- Change management procedures
- Release management process
- Security patch management

6. Operational Security Measures

1. Network Security Architecture

- Network segmentation implementation
- Defense-in-depth strategy
- Security perimeter definition
- Communication flow control

2. System Hardening

- Baseline configuration standards
- Port and service restrictions
- Operating system hardening
- Application security controls

7. Testing and Validation

1. Security Testing Evidence

- Penetration testing results
- Vulnerability assessment reports
- Security function verification
- Integration testing documentation

2. Third-Party Validation

- Independent security assessments
- Certification body reviews
- Compliance audit results

8. Maintenance and Support

1. Security Update Process

- Patch management procedures
- Vulnerability handling
- Security advisory system
- Emergency response protocols

2. Incident Management

- Security incident response plan
- Investigation procedures
- Recovery protocols
- Stakeholder communication

9. Documentation and Records

1. Required Documentation

- System security plans
- Configuration procedures
- Operation manuals
- Maintenance records

2. Compliance Records

- Audit trails
- Security event logs
- Change management records
- Training documentation

10. Certification Statement

DeepShield Systems, Inc. hereby certifies that the implementation evidence provided in this package accurately represents our compliance with IEC 62443 standards. This implementation has been verified through internal validation and third-party assessment.

11. Legal Disclaimer

This Implementation Evidence Package is confidential and proprietary to DeepShield Systems, Inc. The information contained herein is provided for compliance verification purposes only and may not be reproduced or distributed without written authorization. While DeepShield has made reasonable efforts to ensure the accuracy of the information contained in this package, no warranties or guarantees are provided regarding the completeness or accuracy of the implementation evidence.

Authorized by:

/s/ Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: January 11, 2024

/s/ James Morrison

VP of Engineering

DeepShield Systems, Inc.

Date: January 11, 2024