System Integration Architecture Diagram v4.0

CONFIDENTIAL AND PROPRIETARY

DeepShield Systems, Inc.

Last Updated: January 11, 2024

Document ID: SIAD-2024-V4.0

1. Document Control

1 This System Integration Architecture Diagram ("Architecture Diagram") is a confidential and proprietary document of DeepShield Systems, Inc. ("Company"). This document is protected under applicable intellectual property laws and trade secret provisions.

2 Version Control:

- Version 4.0 (Current)
- Supersedes: Version 3.2 dated August 15, 2023
- Approved by: Dr. Elena Rodriguez, Chief Security Architect
- Technical Review: James Morrison, VP of Engineering
- Legal Review: Corporate Legal Department

2. System Architecture Overview

1 Core Platform Components

- DeepShield(TM) Unified Security Control Center (USCC)
- OT Network Monitoring Engine (ONME)
- Industrial Protocol Analysis Framework (IPAF)
- Maritime-Specific Security Module (MSSM)
- Subsea Infrastructure Protection Layer (SIPL)

2 Integration Points

The system architecture implements the following critical integration points:

a) External Systems Integration

- SCADA System Interfaces
- Industrial Control System (ICS) Connections

- Manufacturing Execution System (MES) Integration
- Enterprise Resource Planning (ERP) Data Exchange

b) Security Infrastructure Integration

- Identity and Access Management (IAM)
- Public Key Infrastructure (PKI)
- Security Information and Event Management (SIEM)
- Hardware Security Module (HSM) Integration

3. Data Flow Architecture

1 Primary Data Flows

The architecture supports the following primary data flows:

a) Ingestion Layer

- Real-time OT network traffic
- SCADA system telemetry
- Industrial sensor data
- Maritime vessel tracking data
- Subsea infrastructure monitoring feeds

b) Processing Layer

- Anomaly detection processing
- Threat intelligence correlation
- Machine learning model execution
- Pattern recognition analysis
- Risk scoring computation

2 Data Security Controls

- End-to-end encryption (AES-256)
- Zero-trust architecture implementation
- Data segregation mechanisms
- Secure key management
- Audit logging and monitoring

4. Security Architecture

1 Defense-in-Depth Strategy

The architecture implements multiple layers of security controls:

a) Network Security

- Network segmentation
- Firewall rules and policies
- Intrusion Detection/Prevention Systems
- Virtual Private Networks (VPNs)
- DMZ implementation

b) Application Security

- Authentication mechanisms
- Authorization controls
- Session management
- Input validation
- Output encoding

2 Compliance Framework Integration

- ISO 27001 controls mapping
- NIST Cybersecurity Framework alignment
- IEC 62443 industrial security standards
- Maritime cybersecurity regulations
- Critical infrastructure protection requirements

5. Deployment Architecture

1 Deployment Models

The architecture supports the following deployment scenarios:

a) On-Premises Deployment

- Dedicated hardware infrastructure
- Private cloud implementation

- Air-gapped environments
- High-availability configuration
- Disaster recovery setup

b) Hybrid Deployment

- Edge computing components
- Cloud service integration
- Data synchronization
- Failover mechanisms
- Load balancing

6. Proprietary Technologies

1 Protected Components

The following components are protected under U.S. Patent Nos. 11,123,456 and 11,123,457:

a) DeepShield(TM) Core Technologies

- Adaptive Defense Algorithm
- Neural Network-based Threat Detection
- Maritime-specific Security Protocols
- Subsea Infrastructure Protection Mechanisms

b) Proprietary Protocols

- Deep Layer Security Protocol (DLSP)
- Industrial System Security Protocol (ISSP)
- Maritime Security Exchange Protocol (MSEP)

7. Legal Notices

1 This Architecture Diagram contains trade secrets and confidential information of DeepShield Systems, Inc. Any unauthorized use, reproduction, or distribution is strictly prohibited.

2 The architectural components, methodologies, and implementations described herein are protected by various intellectual property rights including patents, copyrights, and trade secrets.

8. Document Authentication

APPROVED AND AUTHENTICATED:

_

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

Date: January 11, 2024

_

James Morrison

VP of Engineering

DeepShield Systems, Inc.

Date: January 11, 2024