System Integration Architecture Diagram v2.0

CONFIDENTIAL AND PROPRIETARY

DeepShield Systems, Inc.

Last Updated: January 11, 2024

Document ID: DSS-ARCH-2024-011

1. Document Control

1. This System Integration Architecture Diagram ("Architecture Document") 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:

- Original Version: 1.0 (March 15, 2023)
- Current Version: 2.0 (January 11, 2024)
- Approved By: Dr. Elena Rodriguez, Chief Security Architect
- Technical Review: James Morrison, VP of Engineering

2. System Architecture Overview

1. Core Components

The DeepShield Industrial Control System Security Platform ("Platform") consists of the following primary architectural components:

a) DeepShield Core(TM) (DSC-2000)

- Central processing and analytics engine
- AI-driven threat detection module
- Real-time monitoring system
- Incident response orchestration

b) OT Network Interface Layer (OTNIL)

- Industrial protocol adapters
- SCADA integration modules
- PLC communication interfaces

- Legacy system compatibility modules

c) Maritime Protection Module (MPM-500)

- Subsea infrastructure monitoring
- Maritime vessel security integration
- Offshore platform protection systems
- Port facility security protocols

3. Integration Specifications

1. Network Topology

The Platform implements a hierarchical network architecture with the following layers:

a) Layer 1: Physical Infrastructure

- Industrial ethernet backbone
- Redundant fiber optic connections
- Secure wireless mesh networks
- Hardware security modules (HSM-3000 Series)

b) Layer 2: Control Systems

- SCADA interface controllers
- PLC integration modules
- RTU communication gateways
- Industrial IoT device management

c) Layer 3: Security Operations

- Security information and event management (SIEM)
- Threat intelligence platform
- Incident response automation
- Compliance monitoring system

4. Security Architecture

1. Defense-in-Depth Strategy

The Platform implements multiple security layers including:

a) Perimeter Security

- Advanced firewall systems
- Industrial DMZ
- Network segmentation
- Deep packet inspection

b) Access Control

- Role-based access control (RBAC)
- Multi-factor authentication
- Privileged access management
- Session monitoring and logging

c) Data Protection

- End-to-end encryption
- Secure key management
- Data loss prevention
- Backup and recovery systems

5. Integration Protocols

1. Supported Industrial Protocols

- Modbus TCP/IP
- EtherNet/IP
- Profinet
- OPC UA
- DNP3
- IEC 61850
- BACnet
- S7 Communication

2. Security Protocols

- TLS 1.3

- IPSec
- SSH v2
- SNMP v3
- HTTPS
- SFTP
- Secure MQTT

6. Compliance and Standards

1. The Platform architecture adheres to:

- IEC 62443 Industrial Network Security Standards
- NIST Cybersecurity Framework
- ISO 27001 Information Security Management
- NERC CIP Requirements
- API Security Guidelines
- Maritime Cybersecurity Guidelines (IMO)

7. Legal Notices and Disclaimers

1. Confidentiality

This Architecture Document contains confidential and proprietary information of DeepShield Systems, Inc. Any unauthorized reproduction, disclosure, or distribution is strictly prohibited and may result in civil and criminal penalties.

2. Intellectual Property

All architectural designs, protocols, and methodologies described in this document are protected by U.S. Patents #9,876,543 and #10,234,567, with additional patents pending.

3. Limited License

This document is provided under strict license terms and may only be used for authorized purposes as defined in the applicable license agreement.

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

[DIGITAL SIGNATURE BLOCK]

Hash: 0xf7d8e9c6b5a4321

Timestamp: 2024-01-11 12:00:00 UTC