# REAL-TIME MONITORING SYSTEM TECHNICAL GUIDE

**DeepShield Systems, Inc.**

*Document Version: 3.2*

*Last Updated: January 11, 2024*

*Classification: CONFIDENTIAL*

## 1. INTRODUCTION

1. This Technical Guide ("Guide") describes the architecture, implementation, and operational parameters of DeepShield Systems' Real-time Monitoring System ("RMS") for industrial control systems and operational technology environments.

2. This document is proprietary and confidential to DeepShield Systems, Inc. ("DeepShield") and contains trade secrets protected under 18 U.S.C.   1836 et seq.

## 2. SYSTEM ARCHITECTURE

1. Core Components

- Deep Layer Security Protocol (DLSP) v4.2
- Neural Network Monitoring Engine (NNME)
- Adaptive Response Framework (ARF)
- OT Network Integration Module (OTNIM)

2. Network Architecture

The RMS employs a distributed architecture with the following elements:

- Primary monitoring nodes (PMN-series)
- Secondary validation nodes (SVN-series)
- Redundant backup systems (RBS-2000)
- Secure communication channels utilizing AES-256 encryption

## 3. MONITORING CAPABILITIES

1. Real-time Detection Parameters

- Protocol anomaly detection (ICS/SCADA)
- Behavioral pattern analysis

- Process variable monitoring
- Command verification systems
- Network traffic analysis

2. Response Mechanisms

The system implements graduated response protocols based on threat levels:

- Level 1: Logging and notification
- Level 2: Active monitoring and alerts
- Level 3: Automated countermeasures
- Level 4: System isolation protocols

## 4. IMPLEMENTATION REQUIREMENTS

1. Hardware Specifications

- Processing Units: Intel Xeon E7-8894 v4 or equivalent
- Memory: Minimum 128GB ECC RAM
- Storage: 4TB NVMe SSD (primary), 8TB SAS HDD (backup)
- Network: Dual 10GbE interfaces

2. Software Dependencies

- DeepShield Core Platform v7.2 or higher
- Operating System: Hardened Linux kernel 5.15+
- Database: PostgreSQL 14.0+
- Security Modules: DSS Security Suite v3.5

## 5. OPERATIONAL PROCEDURES

1. System Initialization

a) Network topology discovery

b) Baseline profile creation

c) Security policy implementation

d) Alert threshold configuration

2. Maintenance Requirements

- Weekly system health checks
- Monthly security updates
- Quarterly performance optimization
- Annual architecture review

## 6. COMPLIANCE AND CERTIFICATION

1. Regulatory Standards

- IEC 62443 Series
- NIST SP 800-82r3
- ISA/IEC 62443
- NERC CIP Standards

2. Certification Requirements

All implementations must maintain certification with:

- ISO/IEC 27001:2022
- IEC 62443-4-1
- Common Criteria EAL4+

## 7. INTELLECTUAL PROPERTY PROTECTION

1. All components of the RMS, including but not limited to algorithms, source code, documentation, and implementation methodologies, are protected by U.S. Patents:

- US 11,234,567 B2
- US 11,345,678 B2
- US 11,456,789 B2

2. Additional patent applications are pending under USPTO Application Numbers 17/123,456 and 17/234,567.

## 8. LIABILITY AND WARRANTY

1. DeepShield warrants the RMS will perform substantially in accordance with the specifications contained in this Guide when properly implemented and maintained.

2. EXCEPT AS EXPRESSLY SET FORTH HEREIN, DEEPSHIELD MAKES NO WARRANTIES,

EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## 9. CONFIDENTIALITY

1. This Guide contains confidential and proprietary information of DeepShield Systems, Inc. and is protected under applicable trade secret and copyright laws.

2. Recipients are prohibited from disclosing any information contained herein without prior written authorization from DeepShield Systems, Inc.

## 10. DOCUMENT CONTROL

Document Owner: Dr. Elena Rodriguez, Chief Security Architect

Technical Reviewer: James Morrison, VP of Engineering

Legal Reviewer: Corporate Legal Department

Document Number: TG-RMS-2024-001

Classification: Confidential and Proprietary

---

*[End of Document]*