# Distributed Sensor Array Implementation Guide

**DeepShield Systems, Inc.**

*Document Version: 2.4*

*Effective Date: January 15, 2024*

*Classification: Confidential & Proprietary*

## 1. Purpose and Scope

1. This Implementation Guide ("Guide") governs the deployment, configuration, and maintenance of DeepShield Systems' Distributed Sensor Array ("DSA") technology within protected operational technology ("OT") environments.

2. This Guide is binding upon all authorized implementers, system integrators, and end-users of DeepShield DSA systems.

## 2. Definitions

1. "Sensor Node" means any individual monitoring device within the DSA network that collects and transmits operational data.

2. "Array Configuration" means the physical and logical arrangement of Sensor Nodes within the protected environment.

3. "Security Mesh" means the interconnected network of Sensor Nodes operating as a unified detection system.

4. "OT Asset" means any operational technology equipment, control system, or industrial component subject to DSA monitoring.

## 3. Implementation Requirements

1. Physical Deployment

a) Sensor Nodes must maintain minimum separation distances of 3 meters unless specifically authorized.

b) Installation locations shall optimize coverage while avoiding RF interference zones.

c) Each Sensor Node requires dedicated power supply meeting specifications in Appendix A.

2. Network Configuration

a) Sensor Nodes shall operate on isolated VLAN segments.

b) All inter-node communication must utilize DeepShield's proprietary encryption protocol.

c) Backup communication paths must be established for each critical node.

3. System Integration

a) DSA systems shall integrate with existing SCADA infrastructure via approved protocols only.

b) Integration testing must validate all safety interlocks and fail-safe mechanisms.

c) System redundancy requirements per Section 5.2 must be maintained.

## 4. Security Controls

1. Access Control

a) Physical access to Sensor Nodes restricted to authorized personnel.

b) Multi-factor authentication required for all administrative functions.

c) Access privileges reviewed quarterly per DeepShield security policy.

2. Data Protection

a) All sensor data encrypted at rest using FIPS 140-2 validated algorithms.

b) Data retention periods configured according to customer requirements.

c) Secure data destruction procedures enforced upon decommissioning.

## 5. Performance Standards

1. Monitoring Requirements

a) Sensor sampling rate minimum 1000Hz for critical systems.

b) Maximum latency 50ms for alert generation.

c) False positive rate shall not exceed 0.01% under normal conditions.

2. Reliability Standards

a) 99.999% uptime requirement for critical infrastructure deployments.

b) N+1 redundancy minimum for all core components.

c) Automatic failover capability required for all critical nodes.

## 6. Maintenance Procedures

1. Scheduled Maintenance

a) Quarterly physical inspection of all Sensor Nodes.

b) Monthly firmware updates per release schedule.

c) Annual recalibration of all sensing elements.

2. Emergency Procedures

a) 24/7 emergency support contact procedures defined in Appendix B.

b) Maximum 4-hour response time for critical failures.

c) Spare parts inventory requirements per Section 6.3.

## 7. Compliance and Documentation

1. All implementations must maintain compliance with:

a) IEC 62443 Industrial Network Security Standards

b) NIST SP 800-82 Industrial Control Systems Security

c) Customer-specific security requirements

2. Required Documentation

a) As-built network diagrams

b) Sensor Node inventory and location maps

c) Integration test results

d) Security assessment reports

## 8. Proprietary Rights

1. All intellectual property rights in the DSA technology, including patents, trade secrets, and know-how, remain the exclusive property of DeepShield Systems, Inc.

2. This Guide and its contents are confidential and proprietary to DeepShield Systems, Inc.

## 9. Disclaimer

This Implementation Guide is provided "as is" without warranty of any kind, either express or implied. DeepShield Systems, Inc. reserves the right to modify this Guide at any time without notice.

## 10. Authorization

This Implementation Guide is authorized and approved by:

_

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

**Date: _**