WIRELESS COMMUNICATION PROTOCOL FOR ROBOT FLEETS

WIRELESS COMMUNICATION PROTOCOL F

PROPRIETARY AND CONFIDENTIAL

NaviFloor Robotics, Inc.

Version 3.2 | Effective Date: January 15, 2024

1. PURPOSE AND SCOPE

1. This Wireless Communication Protocol ("Protocol") establishes the

2. This Protocol applies to all NaviFloor AMR deployments utilizing the

2. DEFINITIONS

1. "AMR Fleet" means any group of two (2) or more NaviFloor AMRs

2. "NaviMesh(TM)" means NaviFloor's proprietary mesh networking p

3. "Security Event" means any unauthorized access, breach, or attem

3. TECHNICAL SPECIFICATIONS

1. Frequency Bands and Channels

-

Primary Band: 5 GHz (IEEE 802.11ac)

-

Secondary Band: 2.4 GHz (IEEE 802.11n)

Emergency Fallback: 900 MHz proprietary protocol

2. Network Architecture

- Mesh topology with dynamic node allocation
- Maximum nodes per subnet: 128 AMRs
- Minimum signal strength requirement: -70 dBm
- Maximum latency tolerance: 50ms

3. Bandwidth Allocation

-

Control signals: 10% reserved bandwidth

-

Navigation data: 40% allocated bandwidth

-

Sensor data: 30% allocated bandwidth

-

System telemetry: 20% allocated bandwidth

4. SECURITY REQUIREMENTS

1. Encryption Standards

-

AES-256 encryption for all data transmission

-

RSA-4096 for key exchange

- Perfect Forward Secrecy (PFS) implementation

2. Authentication

- Multi-factor authentication for system access
- Certificate-based device authentication
- Rotating security tokens with 4-hour expiration

3. Network Segmentation

- VLAN isolation for each customer deployment
-

Separate control and data planes

-

Air-gapped emergency control system

5. OPERATIONAL PROCEDURES

1. Network Initialization

a) Primary node selection and validation

b) Mesh network formation and testing

c) Security certificate distribution

d) Bandwidth allocation verification

2. Runtime Operations

a) Continuous network health monitoring

b) Dynamic load balancing

c) Automated failover procedures

d) Real-time latency management

3. Emergency Procedures

a) Communication loss protocols

b) Fallback mode activation

c) Emergency stop procedures

d) System recovery sequences

6. COMPLIANCE AND MONITORING

1. The Protocol shall maintain compliance with:

-

IEEE 802.11 standards

-

ISO/IEC 27001:2013

-

NIST Cybersecurity Framework

-

Customer-specific security requirements

2. Monitoring Requirements

-

24/7 network performance monitoring

-

Security event logging and alerting

-

Bandwidth utilization tracking

Latency and packet loss monitoring

7. INTELLECTUAL PROPERTY

1. This Protocol and all associated technologies, including but not limi

2. All rights reserved. No part of this Protocol may be reproduced, mo

8. MODIFICATIONS AND UPDATES

1. NaviFloor Robotics reserves the right to modify this Protocol at any

2. All modifications shall be documented and communicated to affecte

9. EXECUTION AND APPROVAL

This Protocol is approved and executed by the undersigned authorized representatives of NaviFloor Robotics, Inc.

APPROVED BY:

Dr. Sarah Chen

Chief Executive Officer

Date: _

Marcus Depth

Chief Technology Officer

Date: _

Dr. Elena Kovacs

Chief Research Officer

Date: _

10. DOCUMENT CONTROL

Document Number: WCP-2024-001

Version: 3.2

Last Updated: January 15, 2024

Next Review Date: July 15, 2024

Classification: CONFIDENTIAL