AMR FLEET COMMUNICATION PROTOCOL REFERENCE MANUAL

AMR FLEET COMMUNICATION PROTOCOL

NaviFloor Robotics, Inc.

Document Version: 3.2.1

Effective Date: January 15, 2024

Classification: CONFIDENTIAL

1. INTRODUCTION AND SCOPE

-

1. This AMR Fleet Communication Protocol Reference Manual ("Protocol M

2. This Protocol Manual is a controlled document subject to NaviFloor Robo

2. DEFINITIONS

-

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

-

2. "Fleet Control System" or "FCS" means NaviFloor's proprietary fleet man

-

3. "Protocol Stack" means the hierarchical implementation of communicatio

-

4. "Safety Critical Communication" means any data transmission related to c

3. COMMUNICATION ARCHITECTURE

-

1. Primary Communication Channel

-

Operating Frequency: 5.8 GHz industrial band

-

Channel Width: 20 MHz

-

Maximum Latency: 50ms

-

Encryption: AES-256

-

2. Backup Communication Channel

- Operating Frequency: 2.4 GHz industrial band
- Channel Width: 10 MHz
- Maximum Latency: 100ms
- Encryption: AES-256

- 3. Emergency Communication Channel
- Operating Frequency: 900 MHz industrial band
- Dedicated channel for Safety Critical Communication

Maximum Latency: 10ms

-

Priority Override Capabilities

4. PROTOCOL IMPLEMENTATION REQUIREMENT

-

1. Each AMR unit shall maintain simultaneous connections to:

-

Primary Fleet Control System

-

Minimum of two (2) nearest AMR units

-

Local emergency stop system

Environmental mapping subsystem

-

2. Communication Priorities

a) Safety Critical Communication

b) Navigation and positioning data

c) Task execution status

d) Diagnostic information

e) System updates

-

3. Bandwidth Allocation

-

Safety Critical Communication: 40% reserved

Operational Data: 35% allocated

-

System Health: 15% allocated

-

Reserved: 10%

5. SECURITY REQUIREMENTS

-

1. All inter-unit communication must implement:

-

Certificate-based authentication

-

End-to-end encryption

- Rotating session keys
- Integrity verification

- 2. Security Audit Requirements
- Daily automated security checks
- Weekly protocol compliance verification
- Monthly penetration testing
- Quarterly security review

6. FAULT TOLERANCE AND RECOVERY

-

1. Communication Failure Protocols

-

Immediate activation of backup channel

-

Local autonomous operation mode

-

Graceful task termination

-

Safe state positioning

-

2. Recovery Procedures

Automatic channel restoration attempt

-

Progressive backup system activation

-

Manual override capabilities

-

System state verification

7. COMPLIANCE AND TESTING

-

1. Required Testing Intervals

-

Daily: Basic communication checks

Weekly: Full protocol stack verification

-

Monthly: Stress testing and failure simulation

-

Quarterly: Complete system audit

-

2. Documentation Requirements

-

Test results retention: 24 months

-

Incident reports: 36 months

-

Configuration changes: 48 months

Security audit results: 60 months

8. PROPRIETARY RIGHTS AND CONFIDENTIALIT

-

1. This Protocol Manual and all contained information is the exclusive prope

-

2. Unauthorized disclosure, reproduction, or use is strictly prohibited and ma

9. VERSION CONTROL AND UPDATES

-

1. This Protocol Manual shall be reviewed and updated quarterly.

2. All updates require approval from:

- Chief Technology Officer

- Chief Research Officer

- Head of Safety Compliance

- Director of Fleet Operations

10. CERTIFICATION

The undersigned hereby certifies that this Protocol Manual has been reviewe

approved for implementation.

_

Marcus Depth

Chief Technology Officer

NaviFloor Robotics, Inc.

Date: January 15, 2024

_

Dr. Elena Kovacs

Chief Research Officer

NaviFloor Robotics, Inc.

Date: January 15, 2024

```
```

End of Document