Business Requirements Document (BRD)

Project Title: Autonomous Mobile Robot (AMR) Security System

Project Owner: Kim Andreas
Date: [Insert Date]
Version: 1.0

---

1. Business Objectives

Implement an AI-powered robotic security solution using Autonomous Mobile Robots (AMRs) to monitor and safeguard a secure area, reducing reliance on human security personnel, increasing operational efficiency, and minimizing security risks.

2. Project Scope

Develop and deploy an AMR-based security system to perform real-time surveillance, threat detection, and autonomous response in restricted or sensitive areas. Key functions include patrolling, anomaly detection, threat response, and alert escalation.

In Scope:

- AMR hardware design and setup
- AI and sensor-based navigation and surveillance systems
- Integration with security software for real-time monitoring
- Alert and notification systems for anomaly detection
- User interface for monitoring and manual control

Out of Scope:

- External access control systems
- Non-autonomous robot functions
- Long-term data storage and backup solutions

---

3. Functional Requirements

3.1 Autonomous Navigation

- 3.1.1: AMRs must autonomously navigate predefined paths within the secure area.
- 3.1.2: AMRs should detect and avoid obstacles (fixed or moving) in real-time.
- 3.1.3: AMRs should operate continuously, with the ability to return to a charging station autonomously.

3.2 Surveillance and Monitoring

- 3.2.1: AMRs must capture high-definition video and audio within a 360-degree radius.
- 3.2.2: AMRs should utilize computer vision to detect unauthorized personnel or objects.
- 3.2.3: AMRs should identify and log unusual activities or anomalies in real time.

3.3 Threat Detection and Response

- 3.3.1: Upon detecting a threat, AMRs must send immediate alerts to the security control center.
- 3.3.2: AMRs should have an audible alert system to warn intruders or unauthorized personnel.
- 3.3.3: In high-risk situations, AMRs should be capable of triggering lockdown mechanisms in the secure area.

3.4 Communication and Alert System

- 3.4.1: AMRs must have a secure communication protocol for real-time data transmission.
- 3.4.2: In case of network failure, AMRs should continue limited operation autonomously.
- 3.4.3: System should support SMS, email, and in-app notifications for real-time alerts.

3.5 User Interface (UI)

- 3.5.1: Provide a dashboard for monitoring all active AMRs, showing current status, battery life, and alerts.
- 3.5.2: UI should allow security personnel to take manual control of any AMR if needed.
- 3.5.3: Historical data on AMR patrols and incidents should be available for review.

---

4. Non-Functional Requirements

4.1 Reliability

- AMRs must operate 24/7 with minimal downtime (target uptime of 99.9%).

4.2 Security

- All data transmission must use end-to-end encryption.
- Access to the system should be role-based, with multi-factor authentication for security personnel.

4.3 Scalability

- The system should support up to 100 AMRs operating simultaneously in different zones.

4.4 Performance

- Real-time data processing and alert notifications should occur within 1 second of detection.

4.5 Compliance

- The system must comply with GDPR and data protection regulations.

---

5. Dependencies and Constraints

- Dependencies:
  - Access to existing security infrastructure and secure area maps
  - Availability of internet connectivity and power sources for charging stations
- Constraints:
  - Budget limitations for hardware and software licensing
  - Environmental conditions within the secure area (e.g., temperature, lighting)

---

6. Risks and Mitigations

- Risk: Communication loss due to network issues.
    - Mitigation: Configure AMRs to operate autonomously with limited functionality if communication is lost.
- Risk: AMR hardware failure.
    - Mitigation: Implement regular maintenance and health checks on all AMR units.
- Risk: Unauthorized access to AMR system.
    - Mitigation: Enforce strict access control measures and regular security audits.

---

7. Acceptance Criteria

- AMRs must successfully complete patrol routes with a detection rate of 95% for predefined security threats.
- The system must send real-time alerts to the security control center with a latency of under 1 second.
- The user interface must display the status of all AMRs in a single view and support manual override within 2 seconds of request.

프로젝트 제목: 자율 이동 로봇(AMR) 보안 시스템

프로젝트 소유자: 김 안드레아스
날짜: [날짜 삽입]
버전: 1.0

---

1. 비즈니스 목표

인공지능 기반 자율 이동 로봇(AMR)을 활용하여 보안 지역을 감시하고 보호하는 로봇 보안 솔루션을 구현하여, 인력 보안 의존도를 줄이고 운영 효율성을 높이며 보안 위험을 최소화합니다.

2. 프로젝트 범위

제한된 또는 민감한 지역에서 실시간 감시, 위협 탐지 및 자율 대응을 수행하는 AMR 기반 보안 시스템을 개발하고 배포합니다. 주요 기능에는 순찰, 이상 탐지, 위협 대응, 경고 상승이 포함됩니다.

포함 범위:

- AMR 하드웨어 설계 및 설정
- AI 및 센서 기반 네비게이션 및 감시 시스템
- 실시간 모니터링을 위한 보안 소프트웨어와의 통합
- 이상 탐지를 위한 알림 및 통지 시스템
- 모니터링 및 수동 제어를 위한 사용자 인터페이스

제외 범위:

- 외부 출입 통제 시스템
- 비자율 로봇 기능
- 장기 데이터 저장 및 백업 솔루션

---

3. 기능 요구사항

3.1 자율 네비게이션

- **3.1.1:** AMR 은 보안 지역 내에서 미리 정의된 경로를 자율적으로 이동해야 합니다.

- **3.1.2:** AMR 은 실시간으로 장애물(고정 및 이동)을 감지하고 회피해야 합니다.
- **3.1.3:** AMR 은 자율적으로 충전 스테이션으로 돌아갈 수 있는 기능을 갖추고 지속적으로 작동해야 합니다.

3.2 감시 및 모니터링

- **3.2.1:** AMR 은 360 도 범위 내에서 고해상도 비디오 및 오디오를 캡처해야 합니다.
- **3.2.2:** AMR 은 컴퓨터 비전을 활용하여 무단 접근 인물 또는 물체를 감지해야 합니다.
- **3.2.3:** AMR 은 실시간으로 이상한 활동이나 비정상 상태를 식별하고 기록해야 합니다.

3.3 위협 탐지 및 대응

- **3.3.1:** 위협을 감지하면 AMR 은 즉시 보안 제어 센터로 경고를 보내야 합니다.
- **3.3.2:** AMR 은 침입자나 무단 접근자에게 경고를 주기 위한 음성 경고 시스템을 갖춰야 합니다.
- **3.3.3:** 고위험 상황에서 AMR 은 보안 지역의 잠금 메커니즘을 활성화할 수 있어야 합니다.

3.4 통신 및 경고 시스템

- **3.4.1:** AMR 은 실시간 데이터 전송을 위한 안전한 통신 프로토콜을 가져야 합니다.
- **3.4.2:** 네트워크 오류 발생 시 AMR 은 제한된 기능으로 자율 작동을 계속해야 합니다.
- **3.4.3:** 시스템은 실시간 경고를 위한 SMS, 이메일, 인앱 통지를 지원해야 합니다.

3.5 사용자 인터페이스(UI)

- **3.5.1:** 모든 활성 AMR 의 현재 상태, 배터리 수명, 경고를 보여주는 대시보드를 제공해야 합니다.
- **3.5.2:** 보안 담당자가 필요시 모든 AMR 을 수동으로 제어할 수 있어야 합니다.
- **3.5.3:** AMR 순찰 및 사건에 대한 과거 데이터는 검토를 위해 제공되어야 합니다.

---

4. 비기능 요구사항

4.1 신뢰성

- AMR 은 최소한의 다운타임으로 24 시간 연중무휴로 작동해야 합니다 (목표 가동률 99.9%).

4.2 보안

- 모든 데이터 전송은 종단 간 암호화를 사용해야 합니다.
- 시스템에 대한 접근은 역할 기반이어야 하며, 보안 담당자를 위한 다중 요소 인증을 포함해야 합니다.

4.3 확장성

- 시스템은 최대 100 개의 AMR 이 다른 구역에서 동시에 작동하는 것을 지원해야 합니다.

4.4 성능

- 실시간 데이터 처리 및 경고 통지는 탐지 후 1 초 이내에 이루어져야 합니다.

4.5 규정 준수

- 시스템은 GDPR 및 데이터 보호 규정을 준수해야 합니다.

---

5. 종속성 및 제약조건

- **종속성:**
  - 기존 보안 인프라 및 보안 구역 지도 접근
  - 인터넷 연결성 및 충전 스테이션의 전원 공급원 가용성
- **제약조건:**
  - 하드웨어 및 소프트웨어 라이선스 예산 제한
  - 보안 구역 내 환경 조건 (예: 온도, 조명)

---

6. 위험 및 완화조치

- **위험:** 네트워크 문제로 인한 통신 손실.
  - **완화조치:** 통신이 끊어질 경우 제한된 기능으로 자율적으로 작동할 수 있도록 AMR 을 구성합니다.
- **위험:** AMR 하드웨어 고장.

    - **완화조치:** 모든 AMR 장치에 대한 정기 유지보수 및 상태 점검을 구현합니다.
- **위험:** AMR 시스템에 대한 무단 접근.
    - **완화조치:** 엄격한 접근 제어 조치와 정기적인 보안 감사를 시행합니다.

---

7. 수락 기준

- AMR 은 사전 정의된 보안 위협에 대해 95% 이상의 탐지율로 순찰 경로를 성공적으로 완료해야 합니다.
- 시스템은 보안 제어 센터로 실시간 경고를 1 초 미만의 지연으로 전송해야 합니다.
- 사용자 인터페이스는 모든 AMR 의 상태를 단일 화면에 표시하고 요청 후 2 초 이내에 수동 제어를 지원해야 합니다.