Universidad Tecnológica de Tijuana

SOFTWARE REQUIREMENTS SPECIFICATION (SRS)

IoT Access Control System for Restricted Areas

Dr. Ray Brunett Parra Galaviz

Design and Implementation of an Intelligent Security System

TSU in Information Technology

Meza Osuna Juan Manuel

Alvares Salazar Erick Sidrac

Sanchez Murillo Eduardo

Gameros Garcia Angel Geovanny

4B

Document file

Date	Revision	Author	Verified dep. quality.
20/01/2025		Meza Osuna Juan Manuel Alvares Salazar Sidrac Gameros Garcia Angel Geovanny Sanchez Murillo Eduardo	

Document validated by the parties on date:

By the customer	By the supply company
Mrs.	Mrs./Mrs.

Content

Introduction

This document will present the Software Requirements Specification (SRS) corresponding to the project under development, detailing in a structured way the functional and non-functional requirements related to the security system intended for industrial environments.

Purpose

Provide a security solution to control access in sensitive industrial facilities.

The system should ensure that only authorized personnel can enter restricted areas, improving security and reducing the risks of unauthorized access. The system should allow for efficient permit management and real-time auditing of activities within the facility.

Scope

The system will provide a security solution, using IoT devices, an interface for permit management, real-time monitoring of accesses, auditing of security events, as well as monitoring and managing the rounds made by security personnel

Access Control with IoT:

- Implementation of IoT devices (RFID readers, biometric sensors) to authenticate and register access to restricted areas.
- Real-time access authorization through valid credentials (RFID cards).

Permit Management:

- Create and manage user profiles with configurable access permissions.
- Assigning permissions to specific users to access specific areas within the facility, at certain times.

Real-time monitoring:

- Real-time access display with details such as user, area, and time.
- Real-time alerts for unauthorized access attempts or security breaches.

Security Patrol System:

- **Control Points:** Strategic points will be defined where security personnel must register their presence during night patrols.

- **Round Registration**: Staff will scan their RFID card or use a mobile app to register their presence at checkpoints. This will ensure that the rounds are being carried out according to plan.

- **Alerts:** If the guard does not arrive at a checkpoint in time, the system will send alerts to administrators, just like with unauthorized access.

- **Rounds Reports:** The system will generate reports on the rounds performed, detailing the times and any recorded incidents.

Interfaz Administrativa:

- Development of a web and mobile interface for system administrators, which allows managing IoT devices, permissions and viewing access statistics.
- Functionality to configure and update access devices.

Out-of-Reach Features

Integration with External Systems:

The system does not include integration with other third-party security systems, although it can be considered as a future extension of the system.

Access Control in External Environments:

The system is specifically designed for restricted areas within industrial facilities. Access control for external or off-site environments is not included.

Personnel Management or Human Resources:

The system will not handle complete personal data of employees, such as salary, employment, or medical history information. It will only handle information relevant to access control.

1.1 Staff involved

Name	Person 1
Role	Project Leader
Professional category	Software Developer
Responsibilities	• Monitor the overall progress of the project and ensure that deadlines and objectives are met. • Coordinate team tasks and assign responsibilities. • Ensure that the integration of hardware (IoT devices) and software (web/mobile application) is carried out correctly. • Review and approval of the design and development phases of the system.
Contact Information	+1234567891
Approval	Yes

Name	Person 2
Role	Backend Developer
Professional category	Software Developer
Responsibilities	• Develop server logic and integration with IoT devices (RFID readers, biometric sensors). • Create the database to manage access, rounds and report generation. • Implement the necessary APIs for communication between the mobile application and the database.
Contact Information	+1234567891
Approval	Yes

Name	Person 3
Role	Frontend Developer
Professional category	Software Developer
Responsibilities	• Design and develop the user interface for the web and mobile application. • Ensure that the interface is user-friendly and suitable for rounding, access, and reporting management. • Work on integration with backend logic, displaying data clearly and efficiently. • Implement functionalities for real-time monitoring and alert generation.
Contact Information	+1234567891
Approval	Yes

Name	Person 4
Role	IoT Security Specialist
Professional category	Software Developer
Responsibilities	• Supervise the installation and configuration of IoT devices (RFID readers). • Ensure proper communication between IoT devices and the backend platform. • Implement and maintain physical security features for data and device protection. • Evaluate and test the patrol system to ensure that the checkpoints are working properly.
Contact Information	+1234567891
Approval	Yes

1.2 Definitions, acronyms and abbreviations

Access Control System (ACS): A set of technologies and processes that allow managing and controlling the access of people to restricted areas within a facility.

IoT (Internet of Things): A set of physical devices connected to the Internet, capable of collecting, sending and receiving data autonomously.

RFID (Radio Frequency Identification): Technology that uses radio waves to uniquely identify objects or people using tags or cards.

Control Point: Physical location within the facility where security personnel must register their presence during surveillance rounds.

Security Patrols: Activity in which security personnel visit specific points within the facility to ensure that areas are protected.

Security Audit: Process of reviewing and analyzing access logs and rounds to assess compliance with security policies.

UI: User Interface

UX: User Experience

1.3 References

Reference	Title	Date	Author
#1	RFID Reader Handbook	January 2025	Juan Pérez
#2	IoT Security Standards	March 2024	Carlos Rodríguez
#3	AES Encryption and Encryption Standards	December 2024	Laura Garcia

1.4 Summary

This paper describes the development of an IoT Access Control System for Restricted Areas, designed to improve security in industrial facilities. The system includes IoT devices to authenticate and control access, as well as a patrol system to manage security rounds.

2 Overview

2.1 Product Outlook

The Restricted Area IoT Access Control System is a standalone product that integrates into industrial facilities to manage access and monitor security rounds. This system is designed to be autonomous in its operation, but can be extended or integrated into a larger industrial safety management system if necessary.

The system does not require a previously existing security infrastructure, but can interface with other systems if necessary, such as security alarms, surveillance cameras, or personnel management systems. The product consists of:

1. **IoT devices**: RFID readers, biometric sensors, and other devices that are installed at strategic points in the facility to verify the identity of users and register their access.
2. **Web/Mobile Application**: Platform to manage access and monitor security rounds, as well as generate detailed reports on the activities carried out by security personnel.
3. **Security Patrol System**: A module that allows security personnel to carry out controlled rounds, with defined control points where they must register their presence using IoT devices.

2.2 Product Functionality

The IoT Access Control System for Restricted Areas offers a number of key functionalities to securely and efficiently manage access to sensitive areas within industrial facilities. The main functionalities of the product are summarized below:

Access Authentication:

The system allows users to be authenticated using IoT devices, such as RFID readers and biometric sensors.

Access to restricted areas is controlled by permissions configured for each user, ensuring that only authorized personnel can enter.

Permit Management:

System administrators can configure access permissions for each user from the web/mobile app.

Permissions can be assigned by area, time and level of access, allowing granular control of who accesses and when.

Real-Time Access Monitoring:

The system allows access to be monitored in real time through the management interface.

Any unauthorized access attempts are logged and generate automatic alerts for supervisors.

Registration of Security Rounds:

Security personnel are to make rounds at checkpoints set up within the facility.

During the rounds, staff register their presence using IoT devices (RFID readers or the mobile app), which ensures that security procedures are followed.

Generation of Reports:

The system generates detailed reports on accesses, including date, time, place and person involved.

Reports are also generated on the security rounds carried out, showing compliance with the established checkpoints and any incidents recorded.

Security Alerts:

The system sends real-time notifications about unauthorized access, security breach attempts, or if security personnel fail to comply with rounds within the set time.

Alerts are sent to administrators or supervisors for immediate action.

Data Security:

Access data and security rounds are securely stored in the system's database, with high-security encryption.

Authentication and authorization mechanisms are implemented to protect sensitive information.

Friendly User Interface:

The system offers an intuitive web/mobile interface, accessible to administrators and security personnel.

Users can manage permissions, view logs, and receive alerts from the platform easily and efficiently.

2.3 User characteristics

User Type	System Administrator
Formation	Degree in Systems Engineering, Computer Security, or related areas. Minimum experience of 2 years
Skills	• Knowledge in management of access control and security systems. • Ability to configure access permissions, manage the database, and monitor the overall operation of the system. • Basic knowledge of networks, databases and computer security.
Activities	• Configure and manage user access permissions. • Real-time monitoring of accesses and security rounds. • Generation of reports on accesses and activities. • Security alert management and incident resolution. • Supervision and maintenance of the security system.

2.4 Restrictions

IoT Device Compatibility: The system must be compatible with RFID readers and specific biometric sensors that will be used at the checkpoints. These devices must meet connectivity requirements, such as support for Wi-Fi or Bluetooth**.**

Power Requirements: Some IoT devices may have power consumption restrictions, so plan to use long-lasting batteries or integrate appropriate power sources.

Software Restrictions

IoT Standards and Protocols: IoT devices must support standard protocols such as MQTT or HTTP to ensure efficient and secure communication with the web and mobile application.

Operating System: The web application must be accessible through modern browsers on operating systems such as Windows, Linux and macOS. Mobile apps must be compatible with iOS and Android.

Integration with External Systems: Although the system is designed as a standalone solution, in some cases it may be necessary to integrate the system with other existing security systems in the facility, such as surveillance cameras or alarms. This integration may be limited by the compatibility of communication protocols.

2.5 Assumptions and dependencies

Assumptions

Network Infrastructure Availability:

Industrial facilities are assumed to have a stable, wide-ranging Wi-Fi network that allows for the constant connection of IoT devices.

Internet access is available for the operation of web and mobile applications, if necessary.

Hardware Compatibility:

It is assumed that the selected IoT devices (RFID readers, biometric sensors, etc.) are compatible with the protocols and standards used in the system. IoT devices will be installed and configured appropriately according to the design specifications.

Availability of Human Resources:

End users, including administrators and security personnel, will be properly trained to use the system.

Operating Environment:

It is assumed that the system will be implemented in an operating environment with adequate conditions (temperature, constant electrical energy, etc.) to ensure the correct functioning of IoT devices.

Compliance with Deadlines:

It is assumed that there will be no significant disruptions to the project schedule and that all components will be available as planned.

Dependencies

Hardware Vendor Dependency:

The operation of the system depends on the acquisition and installation of specific IoT devices, such as RFID readers and biometric sensors. Delays or problems with suppliers could affect project timelines.

Development Platform Unit:

The implementation of web and mobile applications depends on development platforms such as native React, and its compatibility with current versions of Android, iOS and modern web browsers.

Standards and Regulations Unit:

The system depends on compliance with local and international data security and privacy regulations, such as the GDPR or local regulations related to the protection of personal data.

Technological Infrastructure Unit:

The system depends on the availability of servers to host the database and web applications. Any issues with the technology infrastructure could affect the functionality of the system.

Reliance on Third-Party Software:

The use of third-party libraries, frameworks, and tools for system deployment can lead to dependencies. Any changes or discontinuities in these tools could require adjustments in development.

2.6 Foreseeable evolution of the system

1. Expansion of Functionalities

- **Integration with Surveillance Systems**: Incorporation of security cameras to associate images or videos in real time with the recorded access events.
- **Advanced Patrol Management**: Implementation of predictive analysis algorithms to optimize security patrol routes based on historical events and risk patterns.
- **Support for Multiple Locations**: System scalability to manage access and security rounds in different facilities from a single centralized platform.

2. Security Improvements

- **Multi-factor authentication (MFA):** Implementing additional authentication methods to ensure more secure access, such as dynamic passwords or physical tokens.
- **Advanced Encryption**: Upgrading encryption protocols to more advanced standards to protect data as cybersecurity threats evolve.

3. Performance Optimization

- **Cloud Storage**: Partial or full migration of access data and roam logs to cloud solutions to improve accessibility and scalability.
- **Support for Next-Generation IoT Devices**: Updated support for emerging IoT devices that offer better capabilities and lower power consumption.

4. Data Analysis and Reporting

- **Artificial Intelligence and Machine Learning**: Incorporation of AI-based data analytics to identify anomalous access patterns or predict potential security incidents.
- **Customizable Reports**: Development of tools to generate more detailed reports adapted to the specific needs of each facility.

5. User Experience

- **Multi-Language Interface**: Expanded support to multiple languages to accommodate international users.
- **Offline Access**: Development of functionalities that allow IoT devices and mobile applications to operate without a temporary connection and synchronize data once connectivity is restored.

6. Regulations and Compliance

- **Updates to Comply with New Regulations**: Continuous adaptation to emerging regulations related to data privacy and security in different regions.

3 Specific requirements

Functional requirements

Requirement Number	**RF1**
Requirement Name	User Management
Description	The system should allow administrators to manage registered user information, providing options to: • Create a new user. • Modify a user's existing data, such as name, role, and access permissions. • Remove a user from the system. • Check the list of registered users and their associated details.
Guy	□ Requirement □ Restriction
Requirement Source	Design team and industrial customer
Requirement Priority	□ High/Essential □ Medium/Desired □ Low/Optional

Requirement Number	**RF6**
Requirement Name	Management of Patrols
Description	The system must manage the patrol activities assigned to security personnel, allowing: 1. Assign patrols with predefined checkpoints to security guards. 2. Automatically record the validation of each control point through IoT devices (such as RFID readers). 3. Generate alerts if any checkpoint is not completed within the allotted time. 4. Provide a summary of the compliance status of the patrols, including dates, times, and any anomalies detected.
Guy	□ Requirement □ Restriction
Requirement Source	Design team and industrial customer
Requirement Priority	□ High/Essential □ Medium/Desired □ Low/Optional

Non-functional requirements

Requirement Number	**RF2**
Requirement Name	Management of Patrols

Description	The system must manage the patrol activities assigned to security personnel, allowing: 1. Assign patrols with predefined checkpoints to security guards. 2. Automatically record the validation of each control point through IoT devices (such as RFID readers). 3. Generate alerts if any checkpoint is not completed within the allotted time. 4. Provide a summary of the compliance status of the patrols, including dates, times, and any anomalies detected.
Guy	□ Requirement □ Restriction
Requirement Source	Design team and industrial customer
Requirement Priority	□ High/Essential □ Medium/Desired □ Low/Optional

3.1 Common interface requirements

- The web interface should be intuitive, with a design based on material design, using neutral colors and minimal visual elements to avoid distractions.
- Main screen: Admin panel with quick access to user options, patrols and IoT devices.
- The mobile app should offer a responsive design, with quick access to assigned rounds and active alerts.
- Accessibility requirements: Support for screen readers and expandable text for visually impaired users.

3.1.1 User Interfaces

The web interface should be intuitive, with a design based on material design, using neutral colors and minimal visual elements to avoid distractions.

Main screen: Admin panel with quick access to user options, patrols and IoT devices.

The mobile app should offer a responsive design, with quick access to assigned rounds and active alerts.

Accessibility requirements: Support for screen readers and expandable text for visually impaired users.

3.1.2 Interfaces the hardware

IoT devices: RFID readers and biometric sensors must be connected to the main network using standard protocols such as MQTT or HTTP.

Configuration: Devices must be initialized from the web interface with configuration options such as static IP or DHCP.

Signals: LED indicators and audible alerts for approved (green) or denied (red) access.

3.1.3 Software Interfaces

- **Operating System**: Windows and Linux
- **Database**: Use of MySql for storage of access data and patrols.
- Integration with REST APIs: Allows interoperability with other industrial systems.

3.1.4 Communication Interfaces

- **The web interface should be intuitive**, with a design based on material design, using neutral colors and minimal visual elements to avoid distractions.
- **Main screen**: Admin panel with quick access to user options, patrols and IoT devices.
- **The mobile app should offer a responsive design**, with quick access to assigned rounds and

active alerts.

- **Accessibility requirements:** Support for screen readers and expandable text for visually impaired users.

3.2 Functional requirements

3.2.1 Functional Requirement 1: User Management

The system must allow you to register, update and delete users from the web interface.

Validations: Avoid duplicates in records through unique identification.

Relationship: Each user is linked to specific roles and permissions.

3.2.2 Functional Requirement 2: Access Control

Validate credentials in real-time using IoT devices.

Generate access logs that include date, time, user and area.

3.2.3 Functional Requirement 3: Management of Patrols

Assign checkpoints to guards and record their automatic compliance.

Alert about incomplete points or points outside the estimated time.

3.2.4 Functional Requirement 4: Generation of Reports

Generate detailed reports of accesses and patrols in PDF format.

Allow you to filter reports by user, area, or date range.

3.3 Non-functional requirements

3.3.1 Performance requirements

- The system must process requests in less than 2 seconds to ensure smooth access.
- Support up to 200 concurrent users on the web interface without performance degradation.

3.3.2 Safety

- Sensitive data encryption with AES-256.
- Require two-factor authentication (2FA) for administrators.

3.3.3 Reliability

- Ensure a mean time between failure of at least 100 days on IoT devices.

3.3.4 Availability

- It's 24 hours from him.

3.3.5 Maintainability

- Provide on-interface diagnostic tools to verify the status of IoT devices.
- Automatic software updates via a central server.

3.3.6 Portability

- Compatible with modern browsers and mobile apps on Android and iOS.
- Using Docker to facilitate migration between servers.