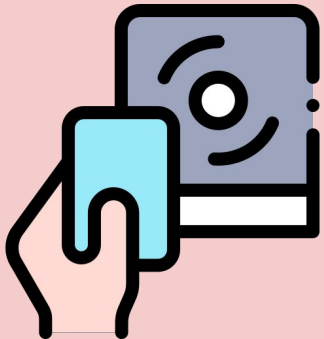

# Requirement Specification

Alejandro Martinez
Jon Nguyen

Ryan Pierce
Manuel Santos

# Discussion Summary

- **Project Background**
  - **Purpose of project**
    - Innovate and integrate advanced features into a RFID Attendance and Control System, ensuring a high level of security for system users.
  - **Scope of project**
    - Utilize Arduino boards to interface with RFID reader modules to allow for access to access points.
    - Integrate magnetic cards with system for user identification
    - Encompasses user registration, attendance tracking, access control, event logging, and reporting.



- **Project objectives**
  - **Known business rules**
    - Some RFID users will have limited access depending on organization hierarchy.
  - **System information and/or diagrams**
    - The server will running as various locations will be secured through RFID technology. These locations will have their security adjusted through the supervisor’s discretion.
  - **Assumptions and dependencies**
    - RFID users will have their cards in possessions at all times
  - **Design and implementation constraints**
    - Python
    - SQL
    - Arduino

# Discussion Summary continued


- **Perspective**
  - **Who will use the system?**
    - We feel that our project will provide the necessary access control and security system for sectors such as industrial, commercial, as well as some high-end residentials such as unit complexes.
  - **Who can provide input about the system?**
    - System Administrators
    - Security Stakeholders
    - Security Personnel
    - IT Department
    - Educational Establishments
    - Compliance Officers
    - Financial Offices

- **Risks**
  - Does not have the ability to differentiate users if the card is on a different possession.
  - RFID IDs can be copied.
  - Weak data transmission security may result in intercepted information.
  - Lack of user training may result in unintentional security breaches.
- **Known future enhancements**
  - Website display of attendance.
  - Integration of additional authentication (e.g., fingerprints facial recognition, keypad entry) for an additional or alternative layer of security.
  - Integration of eco-friendly components or energy-efficient technologies to align with sustainability goals.
  - Incorporating voice command features for hands-free access control and attendance tracking.
- **Open, unresolved or TBD issues**
  - Lock type and Lock maintenance.
  - Develop a training program for the RFID system users, including employees and administrators.

# Requirements vs. Design

The requirements of our project involves both the functional and non-functional aspects of the RFID attendance and control system.  They stem from inputs, objectives, stakeholder needs, and industry standards.

- Requirements entail analyzing gathered information and making sure they are as complete and clear as possible.  Any potential problems will be resolved through strong and concise collaboration.
- The design portion of our project will involve detailed interactions of the RFID system, components and interfaces.  Along with data storage and user interface design.
- Part of the design process will entail getting input from various schools and companies with RFID systems already in place.  This way, we can compare and improve upon our overall design.
- The last section of our design process will involve integrating our components to create a cohesive system.  By testing our design we will verify that our system meets all of our specified requirements and functions.  At the same time, we will meet or excel our goals and needs of the team members and stakeholders.

# Software Requirements Specification

- **Introduction**
  - **Purpose**
    i. The primary purpose of the RFID Attendance and Access Control System is to address the challenges associated with manual attendance monitoring and access control mechanisms. The system purpose is to automate and optimize these critical processes.
  - **Scope**
    i. This scope of the RFID Attendance and Access Control System contains the entire spectrum of attendance monitoring and access management within an organization or institution.
  - **System Overview**
    1. User scans their RFID card or tag into the system.
    2. System checks permissions on database.
    3. System responds appropriate response based on security level check and adds scan into system.
    4. System prepares for next user scan.

- **Definitions**:
  - **Arduino:**
    - Open-source electronics consisting of both hardware and software components. Arduino can be used for developing programmable projects.
  - **RFID (Radio-Frequency Identification):**
    - A technology that employs wireless communication to identify individuals. RFID cards or tags, containing unique identifiers, are utilized in the system for user authentication.
  - **Access Point**
    - A designated location or device serving as an entry or scanning point within a system. It regulates authorized entry, often using authentication methods
  - **Administrator:**
    - A user role with elevated privileges responsible for configuring the system, managing user information, defining access rules, and overseeing the overall functionality of the RFID Attendance and Access Control System.
  - **Database**
    - A collection of organized data that is stored electronically, allowing for efficient retrieval, management, and manipulation of the information.

# Use Cases

**UC-1: User Registration**

- **Summary:** RFID system allows administrators to create new users as well as control their security level.
- **Rationale:** User registration is essential to establish a link between individuals and their respective RFID credentials, enabling them to participate in attendance tracking and access control.
- **Users:** Administrators
- **Preconditions:**
  - Administrator is logged into the system.
  - An available RFID card or tag for each user.
- **Basic Course of Events:**
  1. The administrator selects the "User Registration" option.
  2. System prompts for user information (e.g., name, ID).
  3. Administrator associates a unique RFID card/tag with the user.
- **Alternative Paths:**
  - If RFID card/tag is already associated with another user, system prompts for confirmation or selection of another RFID credential.
- **Postconditions:**
  - New user successfully registered in the system.

# Use Cases

**UC-2: Access Point Registration**

- **Summary:** RFID system allows administrators to create new Access Points as well as control their security level.
- **Rationale:** Access Points Registration is essential to establish a link between Access Points and their respective security credentials for access and attendance.
- **Users:** Administrators
- **Preconditions:**
  - Administrator is logged into the system.
- **Basic Course of Events:**
  1. The administrator selects the "Access Points" option.
  2. System prompts for Access Points information Roomid.
  3. Administrator associates a unique RFID card/tag with the user.
- **Alternative Paths:**
  - If room ID already associated with another access point,  the system prompts for confirmation.
- **Postconditions:**
  - New access point is successfully registered in the system.

# Use Cases

**UC-3: Access**

- **Summary:** Users with RFID cards gain access by scanning their cards, allowing the system to verify permissions and grant or deny access.
- **Rationale:** Enhances security and access control by using RFID cards as keys for access points.
- **Users:** Users with RFID cards.
- **Preconditions:**
  - User with a RFID card or tag.
- **Basic Course of Events:**
  1. User scans RFID card.
  2. System compares permissions.
  3. If match, OK signal sent to access point mechanism.
  4. Door opens, granting acc**ess.**
- **Alternative Paths:**
  - No match: Not OK signal sent, denying access.
- **Postconditions**:
  - Granted access or denied entry.
- **Extensions**:
  - System prompts card renewal for damaged or expired cards.
  - Access logs updated for security monitoring.
  - Procedures for lost or stolen cards, including deactivation and replacement.

# Use Cases

**UC-4: Attendance**

- **Summary:** RFID system adds users to access lists depending on permissions
- **Users:** Users who scanned their RFID.
- **Preconditions:**
  - A user scans their card into the system
- **Basic Course of Events:**
  - RFID system revives the user's point of access and ID.
  - If the security is cleared, the system adds the user to the room attendance database
- **Alternative Paths:**
  - If the user is not cleared then add the user to the access point denied database instead.
- **Postconditions**:
  - Users are added to the appropriate database for some time before being archived.

# Use Cases

**UC-5: User and Access Point Removal**

- **Summary:** RFID system allows administrators to remove users and access points from database
- **Rationale:** When users leave an institute is important to remove  security credentials, locations  and use of access points might change and require different security levels.
- **Users:** Admins
- **Preconditions:**
  - Administrator is logged into the system.
  - Administrator chooses the removal option
- **Basic Course of Events:**
  - Admin is prompted to enter users ID or users RFID
  - System prompts user to confirm removal
- **Alternative Paths:**
  - Admin is prompted to enter access points ID
  - System prompts user to confirm removal
- **Postconditions**:
  - After confirming removal the user or access point is removed from the database.

# Functional Requirements

**User Management (FR1):**

- **Summary:** The system must allow administrators to add, modify, or delete user information, including associating or revoking access permissions.
- **Rationale:** User management is crucial for maintaining an up-to-date record of individuals within the system and managing their access rights.
- **Requirements:**
  - The system shall provide a user interface for administrators to add new users.
  - Administrators shall have the capability to modify existing user information.
  - The system shall allow administrators to delete user records.
  - Access permissions, such as entry to secured areas, can be associated or revoked by administrators.
- **References**
  - Use Case 1 : User Registration
  - Use Case 3: Access Control

# Functional Requirements continued

**Attendance Management (FR2):**

- **Summary:** The system must automatically record attendance upon RFID authentication to generate detailed attendance reports
- **Rationale:** Automated attendance tracking reduces manual efforts and provides accurate data for monitoring and reporting purposes.
- **Requirements:**
  - The system shall record attendance in real-time when a user swipes their RFID card or tag.
  - Attendance records shall include user identification, date, and time.
  - The system shall generate detailed and summary attendance reports for administrators
- **References**
  - Use Case 2 : Attendance Tracking

# Nonfunctional Requirements

**Performance (NFR1):**

- **Summary:** The system must meet performance standards to ensure timely response and efficient processing.
- **Rationale:** Timely response is critical for user satisfaction and overall system efficiency.
- **Requirements:**
  - The system shall respond to RFID authentication within 1 second
  - The system should support a minimum of 1000 registered users simultaneously
- **References:**
  - **UC-1**

# Nonfunctional Requirements continued

**Security (NFR2):**

- **Summary:** Invalid users are still scanned and documented
- **Rationale:** In cases where an unkown RFID is scanned the system should still be able to give a response to the system.
- **Requirements:**
  - Have a negative response to the RFID reader system as the default for when errors/bad scans happen.
- References : UC-4

# Nonfunctional Requirements continued

**Usability (NFR3):**

- **Summary:** : The system must provide a user-friendly interface for administrators to enhance usability and minimize user errors.
- **Rationale:** An intuitive interface promotes ease of use and reduces the learning curve for administrators.
- **Requirements:**
  - The user interface for administrators shall be intuitive and accessible via web-based platforms.
  - TClear and concise instructions for user registration shall be provided.
- Reference:
  - UC-3

# Nonfunctional Requirements continued

**Reliability (NFR4):**

- **Summary:** The system must exhibit high reliability to ensure continuous and dependable service.
- **Rationale:** Reliability is crucial to prevent disruptions in attendance tracking and access control operations.
- **Requirements:**
  - The system shall have a 99% uptime.
  - Regular data backup procedures shall be implemented, and mechanisms for data recovery in case of system failure shall be in place.

# Nonfunctional Requirements continued

**Scalability (NFR5):**

- **Summary:** The system must be scalable to accommodate potential future expansion and increased user capacity.
- **Rationale:** Scalability ensures the system's adaptability to growing organizational needs and technological advancements.
- **Requirements:**
  - The system architecture shall allow for seamless integration with existing infrastructure.
  - The system design shall support scalability to accommodate an increase in the number of registered users.

# Change Control

- The inevitable need for change can occur during the course of our project, which is why we are committed to establishing a formal set of procedures that each of us can be fluid in our final decision making.
  - We will document and track all informal and explicit changes made during the scope of our project.
  - We will thoroughly evaluate all change requests and we will communicate and vote to implement changes.
  - Have multiple versions for inevitable disasters.
- We will comprise a CCB (Change Control Board) made up of all team members as well as get input from professors and the schools system administrator.
  - Our CCB will make well informed decisions and prioritize any changes to our criteria.
  - Any deferments, approvals, objections, or rejections will be handled with concise and expert decision making.
  - The implementation of the CCB is too greatly reduce any bias within the decision making process.
  - The CCB is designed to impose transparency and accountability.

# Change Control

- Our CCB will adhere to the orderly evaluation process.
  - The evaluation process may involve consultation, equal voting or periodic review cycles all of which are designed to reach a majority decision.
  - The CBB has the ultimate authority to either accept or oppose any change requests.
  - If an agreement can not be reached, then the CBB will break down the disagreement to its' core until a satisfying decision can be made.
  - The CBB will communicate and report all relevant decisions to the project team and stakeholders.
  - The CBB will document all final decisions as well as any risk mitigation assessments.