CSCI/CINF/IT Senior Projects Spring 2024

Project Vision, Scope & Plan

DUE: Tuesday February 20th, 2024

Next Assignment consists of: **Project Vision, Scope and Plan Document**

# 1. Problem Statement

### a) Project background

Our team is looking to achieve attendance and control systems using RFID technology, keeping our motto "Securing Today, Safeguarding Tomorrow" in mind. We hope to create an innovative security system with adaptability for present and future needs.

### b) Stakeholders

- Team Lead: Responsible for final decisions, ensuring project progression.
- Project Manager: Oversee the execution and success of the project, setting weekly goals for completion.
- Programing Coordinator: Coordinates programming tasks and activities within the team.
- System Programmers: Develop and maintains the software components of the project.
- Hardware Builder:  esigns and assembles the hardware elements of the system.
- Project Consultant: Provides expert advice and guidance to enhance project outcomes.

### c) Users

Low Security Users

Individuals (students, employees, etc.)

- ❏ Utilize the system for access and attendance marking.
- ❏ Generally have low security clearance.

**School Example:**

- Students marking attendance and accessing designated areas and rooms
- Employees using the system for routine access

**Workplace Example:**

- Employees marking attendance and accessing specific areas

**Mid-Security Users -**

- ❑ Faculty and managers
- ❑ Similar access to Low Security Users
- ❑ Additional privileges include accessing attendance logs and clearance for higher-risk access points

**School Example:**

- Faculty accessing attendance logs
- Managers with clearance for higher-risk access points

**Workplace Example:**

- Managers accessing attendance logs
- Supervisors with clearance for higher-risk access points

High-Security Users.

- ❑ Possess all functionalities of Low and Mid-Security Users
- ❑ Additional capabilities include creating/removing access points and accessing high-risk areas

**School Example:**

- System Administrators managing access points
- Accessing high-risk areas for system maintenance

**Workplace Example:**

- IT Administrators managing access points
- Accessing high-risk areas for system maintenance

## d) Risks

- ❑ **Hardware Malfunction:**

The hardware in use may experience malfunctions, or specific components might break.

- ❑ **Hardware Delay:**

Some tasks may be delayed due to incomplete or unavailable hardware, particularly relying on Arduino software tests.

- ❑ **Missing Team Member:**

Absence or delay of a team member could disrupt workflow, requiring task redistribution.

- ❑ **Hardware Incompatibility:**

There may be insufficient power to support all components, causing potential operational issues.

- ❑ **Engineering Lock Error:**

The lock mechanism could malfunction, either through programming errors or mechanical parts failure.

- ❑ **Programming Incompatibility:**

Certain sections of the program might not seamlessly integrate, necessitating rework for proper functionality.

❑ **Database RFID Incompatibility:**
The RFID sequence might encounter difficulties during input due to size-related issues in the system.

### e) Assumptions

- RFID tokens/cards are compatible with scanner and system.
- The system is connected through a physical medium, i.e., a USB cord.
- The database is running with default configurations.
- RFID tokens/cards available are known and documented for assignment; the current system doesn't scan for assignment.
- The administrator possesses prior knowledge in SQL for efficient database creation; otherwise, manual entry will be done individually.
- RFID cards have unique IDs.
- Higher security levels have access to all clearances of lower security levels.
- Security levels are correctly assigned.

# 2. Vision of the Solution

### a) Vision statement (vision of the project- different than the vision of the team that was included in the team charter).

Our goal for our project is to create a scalable, robust attendance and access security system using RFID technology. Allowing for quick, automated access to doors, and automated tracking attendance, users will use RFID tokens and cards to access these features. Administrators and faculty will have access to the same facilities plus access to attendance lists.

### b) List of features

**Administration- User and Access Point (AP) Control**

Administrators have full control, creating, removing, and editing users and access points.

Security levels for users and access points are adjustable.

**User Access and Attendance**

Users can scan for attendance or access at access points.

**Administration - Attendance Access**

Administrators will be able to access the attendance list.

Alternatively administrators can also see the attendance denied list

**Automated Archival**

Database lists like attendance will be archived.

**c) Desirable features that will not necessarily be developed**

**Wired to Wireless:**

**Website for attendance:** Create an interface where the administrator can access the attendance without being connected to the system.

**Additional / optional security measures:** Add keypads, or biometrics for alternative/additional/voice recognition for ways of entry.

**Closed Door Detection** : Detects when the door is closed.

Auto lock Function:

# 3.Project Plan should consist of:

**Statement of Work (SOW) for Gatekeeper Solutions**

**List of Features and Phases**

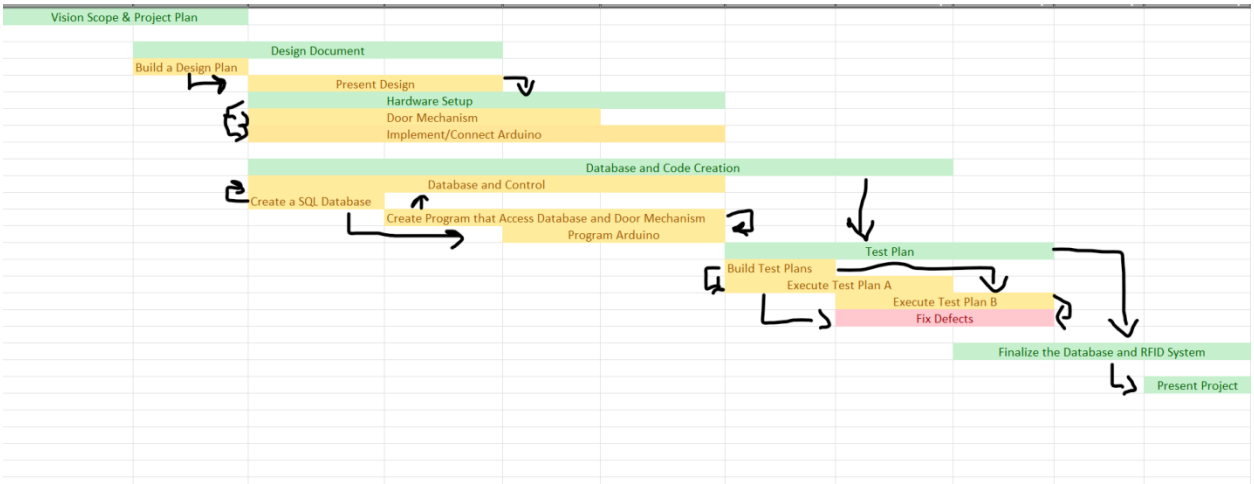
**Features**

- Feature 1: Database and Control
  - Part 1: Create a SQL database.
  - Part 2: Create a program that can access the database
    - Part 2a: Create Users and access points ability.
    - Part 2b: Edit Users and Access points ability.
    - Part 3b: Search user and access point
  - Part 3: Connect Control program with Arduino
- Feature 2: Door mechanism
  - Part 1: Design Mechanism
    - Part 1a: 3d-model design
    - Part 1b: 3d-print design
  - Part 2: Build Lock mechanism
  - Part 1: Design Mechanism
- Feature 3: Arduino
  - Part 1: Design Arduino build.
  - Part 2: Build Arduino build
  - Part 3: Program Arduino
    - Part 3a: Read RFID
    - Part 3b: Contact Control System
    - Part 3c: Send signal to Door Mechanism

### Work Breakdown

- **Feature 1: Data Base and Control**
  - **Designer Lead**: Ryan
  - **Implementation:** The whole team
- **Feature 1b: Control**
  - **Designer Lead**: Alejandro
  - **Implementation**: The whole team
- **Feature 2: Door Mechanism**
  - **Designer Lead**: Manuel
  - **Implementation**:The whole team
- **Feature 3: Arduino :**
  - **Designer Lead**: Jon
  - **Implementation**:The whole team

## Project Schedule



**Hardware and Software Resources**

**RFID Scanner:**

- **Arduino**
- **RFID Scanner**
- **Wires**
- **Power Source**
- **RFID Tokens**
- **C++**

**Security Program:**

- **Python and C++**

**Database  (server program)**

- **Hosting application**
- **MYSQL**
- **Phpmyadmin**
- **Apache**

| Name | Risk planning script |
| --- | --- |
| Purpose | To develop any mitigating risks that might and be able as a team to<br><br>Assess those risks. We will also develop a risk plan. |
| Summary | Our risk plan will be covered in three sections:<br><br>The first section will cover our brainstorming so we can identify any risks.<br><br>The second section covers probability and the impact scores of those risks.<br><br>The third section is where we will come up with a satisfactory plan to avoid any risks. This will give us a sound course of action that we can incorporate into our project. |
| Work Products | Assess the input:<br><br>Look over all documentation that has been created thus far.<br><br>What is the output:<br><br>Create a risk plan<br><br>Carefully go over all of our assumptions in the vision and scope<br><br>Document. |
| Entry Criteria | Our team leader will call a meeting (generally an hour or two) to assess the risks that may affect our project. |

| | |
|---|---|
| **Basic Course of Events** | **We will implement a three-step process for our risk assessment.**<br><br>**1. Collective thoughts on potential risks. Our team leader will gather all members for a brainstorming session so we can pinpoint any risks to our project.**<br><br>**2. Next we will gauge the probability of each risk. This will be done by creating a number system, typically 1 to 10 (highly unlikely to very likely to occur). Then create a number system of impact such as 1-5 (low impact to high impact).**<br><br>**3. Finally we will create a risk plan. We will identify those areas that we deem are high -priority risks and document those plans.** |
| **Exit Criteria** | **After all documentation has been completed and all risks have been categorized then our risk plan will be implemented into our overall project.** |

| **Risk plan for project** | **RFID Attendance/Entrance Control System** | | | | |
|---|---|---|---|---|---|
| **Assessment team members** | **Alejandro Martinez, Jon Nguyen, Ryan Pierce, Manuel Santos** | | | | |
| **Risk** | **Probability 1-10** | **Impact 1-5** | **Priority** | **Actions** | |
| **Hardware delay** | **4** | **4** | **16** | **Ryan will get an ETA from Professor as to when we can expect the hardware.** | |
| **Jon becomes very sick for 2 weeks** | **5** | **5** | **25** | **Ryan will ask Manuel and Alejandro to pick up the extra slack until Jon returns.** | |
| **Programming Incompatibility** | **3** | **5** | **15** | **Ryan and Jon will move into a different direction in terms of programming.** | |

| | | | | | |
|---|---|---|---|---|---|
| **Hardware Malfunction** | **4** | **5** | **20** | **Manuel will ensure we have extra backup to replace unusable hardware.** | |
| **Database RFID incompatibility** | **3** | **5** | **15** | **Alejandro will trouble shoot any and all problems with our database.** | |