DISPOSABLE NFC BRACELETS AND READER

ECE 445 DESIGN DOCUMENT - SPRING 2023

Project # 42

Brennan Eng, Edson Alpizar, Ege Gunal

Professor: Olga Mironenko

TA: Zicheng Ma

Contents

1 Introduction

1.1 Problem

Waterparks have an issue with optimizing their security, sales, and customer experience. The first example of a problem is customers who manage to sneak past staff and get in for free. There is no easy way to discern between a paying customer and someone who has just snuck in with a fake or old paper armband and even then there is always human error in identifying them. Another problem is if a consumer is currently in the water and becomes hungry they must travel back to their locker/chair to get their card/cash, go to the food stands to purchase the food, go back to their locker/chair to safely re-stash their belongings after eating, and only then can they finally go back to the water. Another niche example of a problem is if a parent loses their child within the park; usually there is no log of where to narrow down the search for the kid or any way to determine their last known location beyond observation.

1.2 Solution

Our solution involves constructing a system that uses cheap, disposable, and reprogrammable NFC bracelets that can be scanned with an NFC chip reader. The solution has two purposes: user-sided actions (to improve user customer experience), and business-sided actions (to optimize profits and security). The purpose of the NFC bracelets for the user is to integrate a seamless low-latency experience for the consumer which takes care of access, payment, and other services if requested. On the other hand, the purpose of the NFC bracelet for the business is that invaluable data that is received from each interaction of the user. Depending on the use case, the NFC chip reader will then access a custom built consumer database that will carry out authenticated user-sided actions. The applications from a business perspective go so far as to use big data to determine localized traffic and popularity of events in a quantitative manner. In addition to the reader and the bracelets, the goal is to create a display of utility by attaching the ultrasonic sensor system onto a door frame ensuring that the count of users entering the site in the database ends up matching that of the ultrasonic sensor.

1.3 Visual Aid

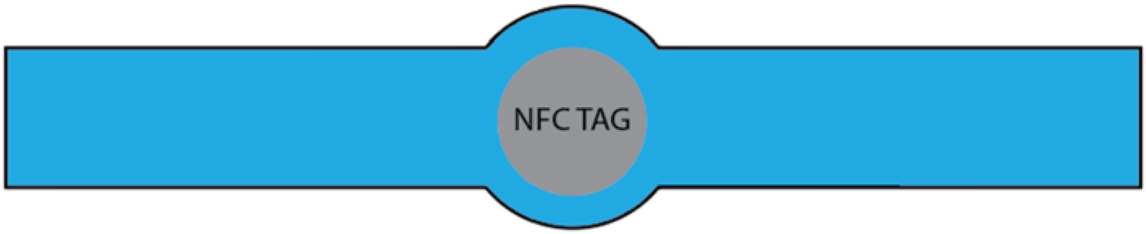


Figure 1: Silicon band with area to insert NFC tag

In most establishments the usage of NFC tags is usually in the shape of a keychain or card. For our project we will be using reprogrammable NFC tags that are inserted to Silicon bands that users will wear when interacting with different locations at an establishment. The NFC tags will be programmable by a server system that will be controlled by the workers of the establishment. The information written to the tags will vary from establishment to establishment. In our project we will use a Raspberry Pi to hold a local server that will also contain the NFC writer.

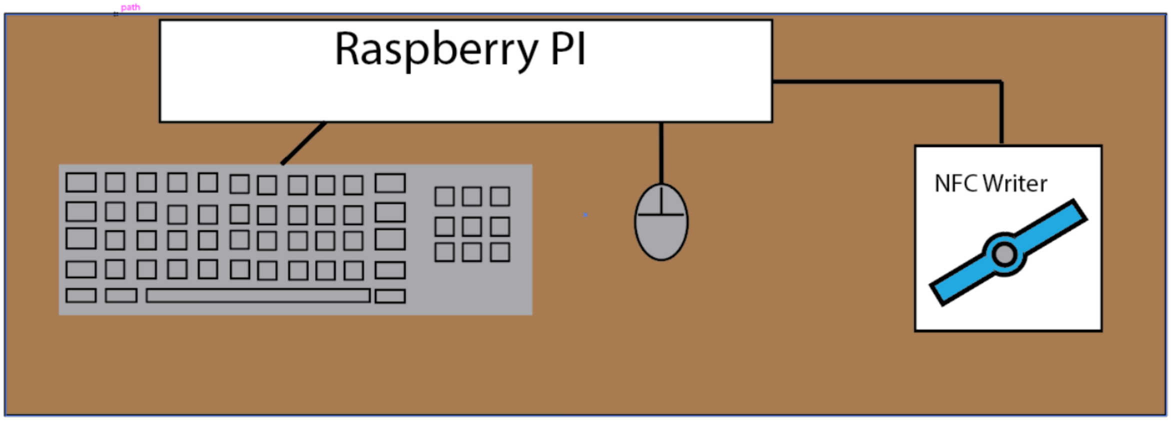


Figure 2: Example setup of server subsystem in the process of writing to NFC Band

We will be giving each NFC tag in our project a unique Identification Number. This ID will be stored in the local server and be used for the purpose of opening a door. The user with the NFC band will interact with a NFC reader system that will do two things: it will either unlock the door the reader system is attached to or will not.

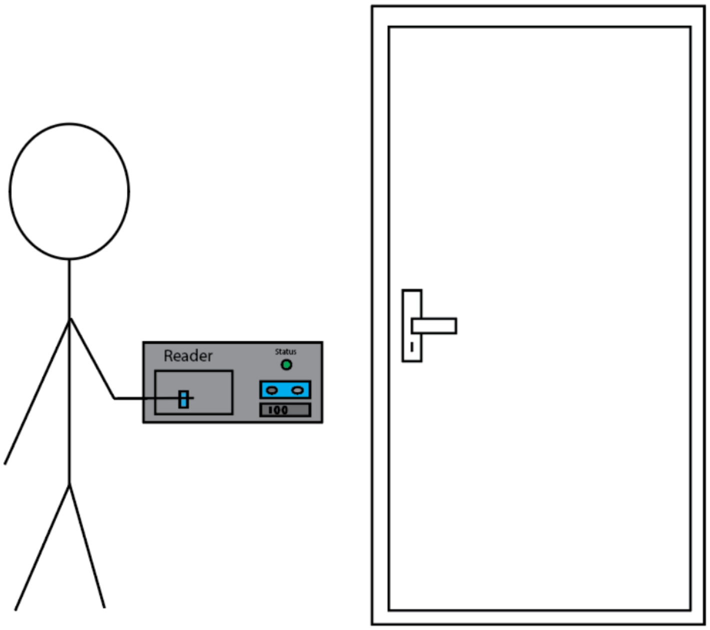


Figure 3: A different implementation of our NFC door opening mechanism, where it is used to open an office door.

1.4 High Level Requirements

We will consider our project to be successful if:

1. Our NFC bands need to check if a user has access with a millisecond-level latency.
2. Our NFC bands need to detect when someone with/without access attempts to pass through checkpoints via sensors, and store this information in a central database that gets cleared at regular intervals, chosen by the employer.
3. Our entry checking mechanism needs to count the number of people who enter, and alert when someone follows another person without tapping their NFC band. This will be done via the sensor subsystem.
4. Our NFC bands need to be linked to a central database linked to user accounts, to which food stalls can send the billing information.

2 Design

2.1 Physical Design

The most important part of our project is the NFC reader system. In our project design we will demonstrate our reader system by attaching it to a door opening mechanism that will also contain a sensor subsystem that will be used to keep track of the number of people that enter said door. Our NFC reader will contain a status LED that will be used to signify whether or not the user will be allowed to enter. If the user scans their tag and the reader recognizes the user the LED will turn green allowing them to enter. When the user enters through the door the ultrasonic sensor will keep track of the people that enter. This sensor will verify that only one person has entered. We will also have a LED display that will show the number of people that have entered said location. If there is a disparity in the number of people that enter per scan then the person that last scanned will be liable for the people that entered without permission.

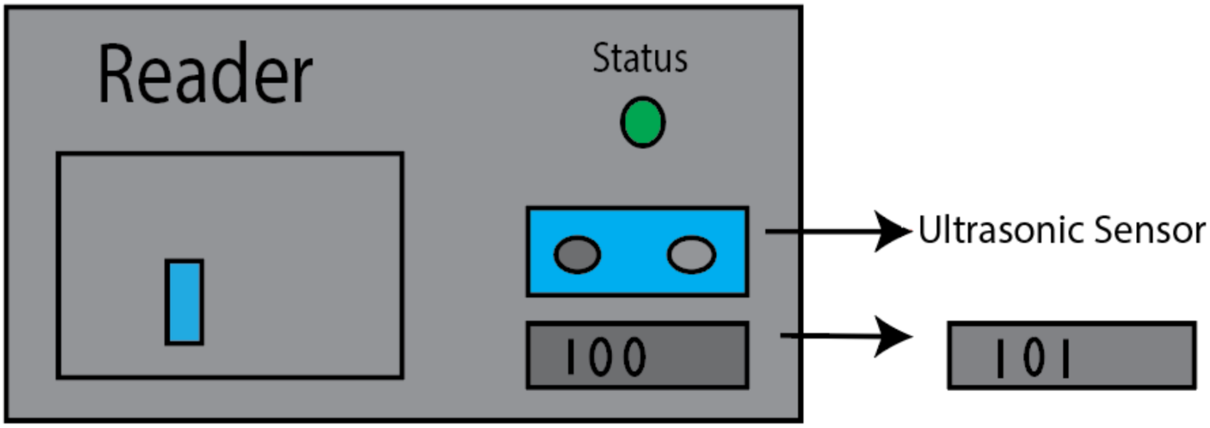
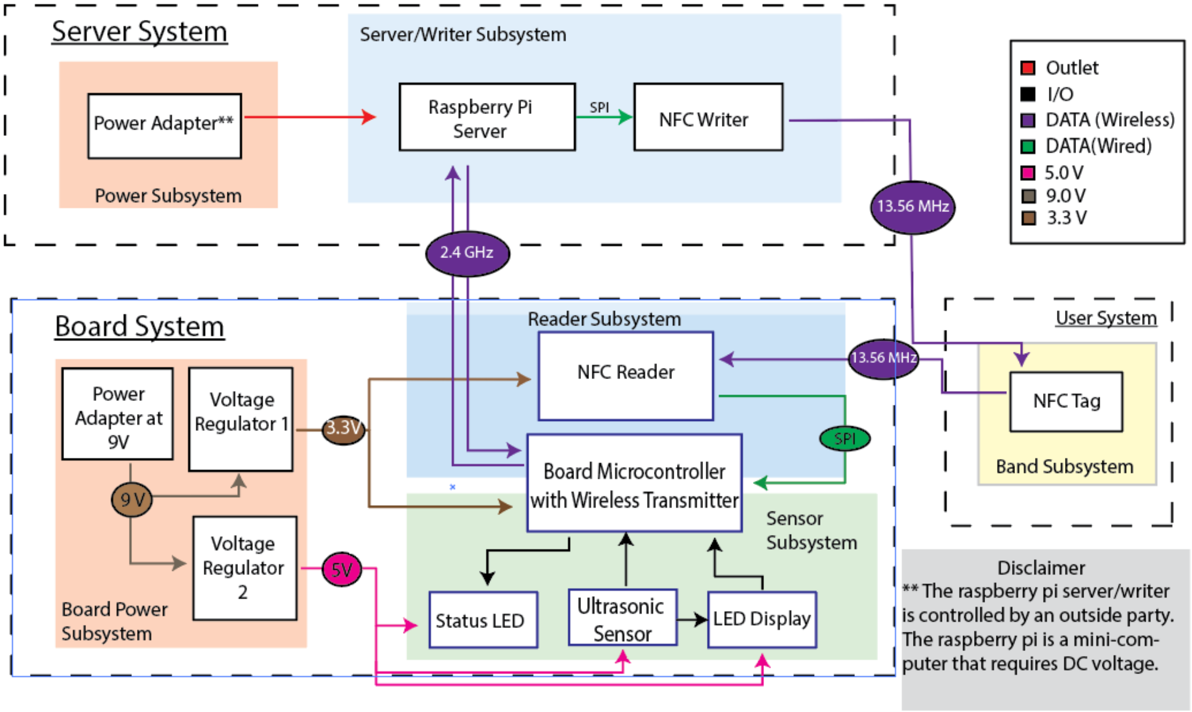


Figure 4: LED Display will increase by one for every person the ultrasonic sensor detects.

The NFC reader and the local server will communicate wirelessly to determine if the user who scans is registered or not.

2.2 Block Diagram



Disclaimer
** The raspberry pi server/writer is controlled by an outside party. The raspberry pi is a mini-computer that requires DC voltage.

Figure 5: Block Diagram

2.3 Subsystem Overview and Requirements

2.3.1 Server Power Subsystem

The server power subsystem is composed of a Type C power supply. This subsystem is responsible for powering up the Raspberry Pi that will hold our local server.

Requirements	Verification
1. Turn on the Raspberry Pi	1. Standard Raspberry Pi Power Adapter

Table 1: Server Power Subsystem - Requirements

2.3.2 Board Power Subsystem

The board power subsystem is responsible for powering up both the Reader and Sensor Subsystems. This will be accomplished by using an adapter connected to a standard wall outlet. The components in sensor subsystems will require 5 Volts to be functional, and the microcontroller and nfc reader require 3.3 Volts. In order to properly power up our components we will have to use voltage regulators on the 9 Volts input to acquire 5 Volts and 3.3 Volts.

Requirements	**Verification**
1. Convert the 9 Volts from adapter to 5 Volts for our ultrasonic sensor and LEDs, 3.3 Volts for nfc reader and microcontroller; zener diodes ensure higher voltages do not get generated 2. Buffer some energy in a large capacitor to ensure safe microcontroller shutdown when power is disconnected.	1. Connect the input power subsystem to a voltage supply and expected outputs to different channels on an oscilloscope with a) open circuit and b) short circuit. 2. Slowly increase the input through the voltage generator, check the oscilloscope readings to make sure they do not fluctuate more than 5% of intended value under both circumstances.

Table 2: Board Power Subsystems Requirements

2.3.3 User System

The user system is a NFC tag attached to a silicon band. The tag will contain user and identification information. This system will interact with both the reader and writer subsystems. The NFC tag will be programmed via the writer subsystem where the raspberry pi will be used to write into the tag. In order to access a particular area the user will have to have their tag be read by the reader in order to allow access to a particular location.

Requirements	Verification
1. The NFC tag should be able to contain the information we program it to have.	1. Reader/Writer from writer subsystem will verify the intended information got written on the NFC tag. 2. When the NFC tag is read the status LED on the reader system should light up green if the user is registered in the database. 3. If the tag is not registered the status LED will light up red.

Table 3: User System Requirements

2.3.4 Server/Writer Subsystem

The server and writer subsystems are combined parts in our project. This is the case because the Raspberry Pi will act as the local server. The server will contain a database in SQL that will use a unique Identification Number for every user in the database. With that unique identification number the host of the server will be able to access any necessary information that is contained in the user NFC bands. The server will be powered by the server power subsystem. In our project design the writer subsystem is connected directly onto the Raspberry Pi, since the raspberry pi is a computer and can be used to write the information we want onto the NFC writer. The writer subsystem will then write the user information onto the NFC tag used in the user system. The server subsystem will also interact with the reader subsystem whenever a user enters a restricted area. The server will figure out if the NFC tag that was read by the reader subsystem has access to a particular location and return a true or false signal that will be indicated by the status LED on the reader subsystem.

Requirements	Verification
1. Store user information in a database. 2. Generate unique UIDs and write that UID	1. Be able to print the contents of the database and see the user input information.

onto NFC tags. 3. Receive entry logs (communicate wirelessly) from reader subsystems and store them in a central database.	2. We can use the status LED on the reader subsystem to show a UID that is registered onto the database and one that is not by allowing access onto the door opening mechanism or not. 3. We can print the contents of a database for a particular user and see when they scan their NFC band.

Table 4: Server/Writer Subsystem Requirements

2.3.5 Reader Subsystem

The reader subsystem will contain the wireless transceiver, NFC reader and microcontroller. This subsystem will be powered up by the board power system since all the components require 5 Volts instead of 9. The reader subsystem will interact with the user system whenever a NFC tag is read. The reader will isolate the unique identification number and send it to the server system to see if the UID is a valid entry. If the user entry is valid then that UID will be stored onto on chip memory to reduce latency whenever the user scans their tag in the same location. The reader will also log information and send it back to the server subsystem. The reader will also communicate with the sensor subsystem. The sensor system will send the number of people the ultrasonic sensor detects to the microcontroller via SPI and then send that information back to the server.

Requirements	**Verification**
1. Receive NFC UID from user bands and share it with the board microcontroller via SPI. 2. Share UID information between the local server and the reader wirelessly. 3. Reduce latency when the user scans for the first time and when they scan in the same spot multiple times.	1. Verify wireless works through serial communication between microcontroller and programming computer. 2. After setting up the server, tap an NFC tag of known UID. 3. Hard code that UID and compare that to what you read. 4. If the comparison succeeds, light up a green LED. Otherwise light up a red LED. 5. Measure the time it takes for the LED

	to light up after tapping. This can be done without instruments, it will be successful as long as there is no visible large delay. 6. Check the server subsystem to see if the UID was logged in the database.

Table 5: Reader Subsystem Requirements

2.3.6 Sensor Subsystem

The sensor subsystem will contain a status LED, an LED display, and an ultrasonic sensor. This part of the subsystem will also be powered by the board power subsystem. The sensor will use an LED indicator that lights up green if the user who scans is eligible to enter and lights up red if the user is not eligible. That information will be communicated between the reader and server subsystem. This will be possible because the sensor and reader subsystem share a microcontroller. When a person walks through the ultrasonic sensor when the status LED is light green it will count how many people enter and send that information to the microcontroller so it can be logged onto the server. If two people were detected entering when only a single user scanned then the owner of an establishment will know who is liable.

Requirements	**Verification**
1. Display whether someone has access via LEDs, as determined by the controller. 2. Display the number of people who have entered on the LED display. 3. Log the number of people that the ultrasonic sensor detects at the time of scan onto the server.	1. Have two NFC tags with UIDs. One of the tags will be registered onto the database and the other will not. The one that is registered will make the green LED light up. The unregistered tag will make the red LED light up. 2. Walk in front of the sensor and see if the counter increments. 3. Write some code that will print onto the raspberry pi the time and the number of people that entered at the time of scan.

Table 6: Sensor Subsystem Requirements

2.4 Tolerance Analysis

A potential risk to the completion of the project would be the failure to read/write the NFC bands with the unique ID in order for the security system to read them correctly to perform a specific task. The issue at hand is ensuring the bands are reprogrammed and overwritten correctly so when the reader scans the band, the system accesses the ID without any issues and performs the task. With this issue, ensuring that the bands are reprogrammed correctly requires our group to heavily research which NFC bands are the best at being reprogrammed as well as a device that can write the values that we require onto the band itself. Wireless components are sometimes a risk due to it being susceptible to interference. That being said, the risk should be mitigated by ensuring our systems optimize the range and accuracy from which we scan these bands in order to reduce the risk of failure.

Some potential risks to the widespread use of our project is working with wireless protocols and ensuring that reader microcontrollers will always get necessary updates to their local user databases. We will be researching how wireless protocols operate to reduce our system's susceptibility to wireless connectivity issues, as well as potentially encrypting each signal to reduce malicious attempts to replicate our NFC arm bands.

3 Cost and Schedule:

3.1 Cost Analysis

- Labor: $40/hr * 10 hr/week * 3 group members = $1200 in labor costs

Name	Description	Manufacturer	Part #	Quantity (units)	Cost ($)
NFC Round Cards	Cheap and disposable NFC chips embedded into a plastic card	Yanzeo	B08Z7P7L3R	20	8
NFC Tag Wristbands	Cheap and programmable NFC wristbands meant to be used as a final product alongside reader and writer	YARONGTE	NTAG215CARD-100	5	12
Reader Module Kit Mifare RC522 Reader Module	NFC Reader IC to be used with the PCB	SunFounder	MFRC522	1	8
NFC HAT for Raspberry Pi	Writer/Reader extension for RPI	Waveshare	PN532	1	28
Raspberry Pi 4	Used to transmit information between NFC tags and pcb	Raspberry Pi	Raspberry-PI-4	1	100
Ultrasonic Sensor	Used to physically verify that the number of entries matches up with the people entering	Smraza	S03sF	1	4

Microcontroller	Used for controlling the reader and sensor subsystems	Espressif Systems	ESP32-S3-WROOM-1-N8	1	4
Adjustable Voltage Regulator	Used to convert downconvert power for pcb subsystems	STMicroelectronics	LM317T	2	2
Miscellaneous Supplies	Wires, resistors, capacitors, other commonplace supplies	n/a	n/a	n/a	5

Table 7: Component costs

Estimated Labor Cost	Estimated Parts Cost	Estimated Total Cost
1200	171	1371

Table 8: Total Costs

3.2 Schedule

- 2/6 - 2/17:
  - Finalize design and planning of project (All team members)
- 2/20 - 2/25:
  - Research and begin buying parts required for project
- 2/27 - 3/3:
  - Begin implementation of proof of concept with disposable NFC chips
  - Begin implementing software required for writing to NFC chips (Edson & Brennan)
  - Design implementation of PCB with interconnecting parts (Ege)
- 3/6 - 3/10:

    - Finalize PCB design and submission (Ege)
    - Finalize the concept of writing information to NFC chips (Edson & Brennan)
- 3/13 - 3/17
    - Spring break
- 3/20 - 3/24
    - Finalize read/write system of NFC tags and transition towards NFC wristbands (Edson)
    - Ensure that raspberry pi and pcb are wirelessly transmitting information with each other seamlessly (Ege)
    - Create database that houses NFC ID information (Brennan)
- 3/27 - 3/31:
    - Begin connect all parts together with physical ultrasonic sensor system (Ege)
    - Begin validation testing (Brennan & Edson)
- 4/3 - 4/14:
    - Quality Assurance testing with products and ensuring system works together seamlessly (All team members)
    - If time allows, ensure the product looks presentable and pass the alpha stage of development.
- 4/17 - 4/21:
    - Mock Demos
- 4/24 - 4/28:

- Final Demos

4 Discussion of Ethics and Safety:

One potential exposure in our project is the data aggregation of user interactions within the premise of a business. It is a concern because it presents the risk of exposure of customer privacy if not handled correctly (IEEE Code of Ethics 1.1). These factors may pose a threat to the privacy of others as well as the mishandling of financial data if payment systems are involved. While these devices pose no physical threat to a user or its customer, the database records and stores all interactions of consumers for the business to make more sound decisions based on the business intelligence it has gathered. That being said, while the data belongs to the business, the release of that data may pose a threat to those involved. To reduce the risk of data breaches, a comprehensive cybersecurity system is necessary as well as vetting of businesses who intend to use these products for malicious purposes (IEEE Code of Ethics 1.2). We will also need to ensure anonymity of long-term stored data and further investigate privacy concerns over data we store, such as California State Law that has a strict emphasis on data privacy (IEEE Code of Ethics 1.6).

5 Bibliography

Core Electronics. “How to Use a NFC Reader with Raspberry Pi.” Core Electronics, 12 Mar. 2018, https://core-electronics.com.au/guides/how-to-use-a-nfc-reader-with-raspberry-pi/.

All About Circuits. “Read and Write on NFC Tags with an Arduino.” All About Circuits, 2021, https://www.allaboutcircuits.com/projects/read-and-write-on-nfc-tags-with-an-arduino/.