# WatRooms

## Waterloo's Student Number Authentication System for Accessing Study Rooms Via Student Numbers

## [Design Document]

Chris, Ishan, & Luka

# Table of Contents

# Needs Assessment

## Client/Customer Definition

The target customers for the WatRooms device are Waterloo students. The project aims to create a device that enables secure communication and access to study rooms through Bluetooth. [10]

**Key Customer Attributes** [12]

- *Demographic:* The primary customers are Waterloo students, enrolled at the University of Waterloo, comprising a population of about 42,000 students.

- *Geographic:* The device is designed for use within the University of Waterloo campus, focusing on access to study rooms and facilities that often require keys or passcodes.

- *Economic:* The customers are campus security, faculty, and staff who seek low-cost solutions that provide efficient and secure access to study rooms without requiring infrastructure changes.

**Challenges Faced by Clients** [11]

This device addresses the problem of changing passcodes for secure room access. Current systems often have passcodes that are rarely updated due to the inconvenience and time required to make changes. The device proposes a solution that allows access to study rooms by using student numbers and booked time as authentication, making it easier for students and security to manage access.

**The stakeholders involved are:**

- *Waterloo students:* Main users of the device.

- *Campus security, faculty, and staff:* Responsible for granting access to rooms.

- *Suppliers (Digi-Key and Rigidware):* Provides components for the device.

- *Installation staff:* Requires a device that is easy to integrate with doors.

- *The graduate TA:* Grades and marks our project.

- *Special interest groups (universities):* Might have interest in the design.

## Competitive Landscape

The WatRooms device is designed to offer easy access to systems by allowing users to enter their student number. However, there are several technological and social challenges that are present.

**Manual passcode entry for students - Technological:**

- *Challenges* [22]*:*
    - Users must remember passcodes, which can be inconvenient and prone to errors.
    - Passcodes are often static and infrequently updated, leading to security vulnerabilities.
- *How to address it:*
    - Users input a passcode on a keypad that is their student number.
    - Denies entry if the student number isn't allocated to the booked time.

**Manual passcode entry for staff - Technological:**

- *Challenges* [17]*:*
    - Staff must have a specific booked time as well to access study rooms for cleaning or maintenance.
    - Only one student number can be used to book a time.
- *How to address it:*
    - Staff will have specific passcodes that all full-time access to all study rooms, regardless of a booked time.

**Student number tracking - Social:**

- *Challenges* [18]*:*
    - If a study room is left a mess or vandalized, there is no way to find the culprit(s) and take appropriate action.

- *How to address it:*

    - All data, including the student number and booked time are stored in a csv file, giving staff access to who and what time(s) vandalism or an inappropriate act occurred.

## Requirement Specification

The system will meet the following functional, technical, and safety requirements:

**Functional Requirements:**

- Communication Distance: The device will send signals over at least 6 inches between microcontrollers to reliably
- Transmission Speed: The device will send signals at a certain frequency that is released by the HC-05 Bluetooth module (2.4 GHz) [6]
- Signal Accuracy: The device will keep at least 90% accuracy over a minimum of 6 inches

**Technical Requirements:**

- Code Implementation: Software will be in C++ on the STM32, no Arduino libraries
- Signal Modulation: The device will use Bluetooth signals via 2 HC-05 Bluetooth module to send and receive data clearly over a frequency of 2.4 GHz from a “master” to a “slave” module [4]

**Safety Requirements:**

- Low Power Use & Energy Limit: The device will use less than 30W and will store less than 500mJ of energy to avoid safety hazards
- No High Voltage: The device will not connect to high voltage without a safety review

# Analysis

## Design

Our solution to our problem is to create an authenticated access keypad for room access throughout the Waterloo campus, especially in the E7 ECE Garages. In order to fairly distribute access to the study rooms, we devised a booking system in which a user can book a room for a set amount of time and enter their Waterloo Student Number on a keypad to unlock the room. If the user enters their Student Number and they have booked the room, then the second NUCLEO-F401RE will move a Servo Motor 90° counter clockwise to unlock the study room door.

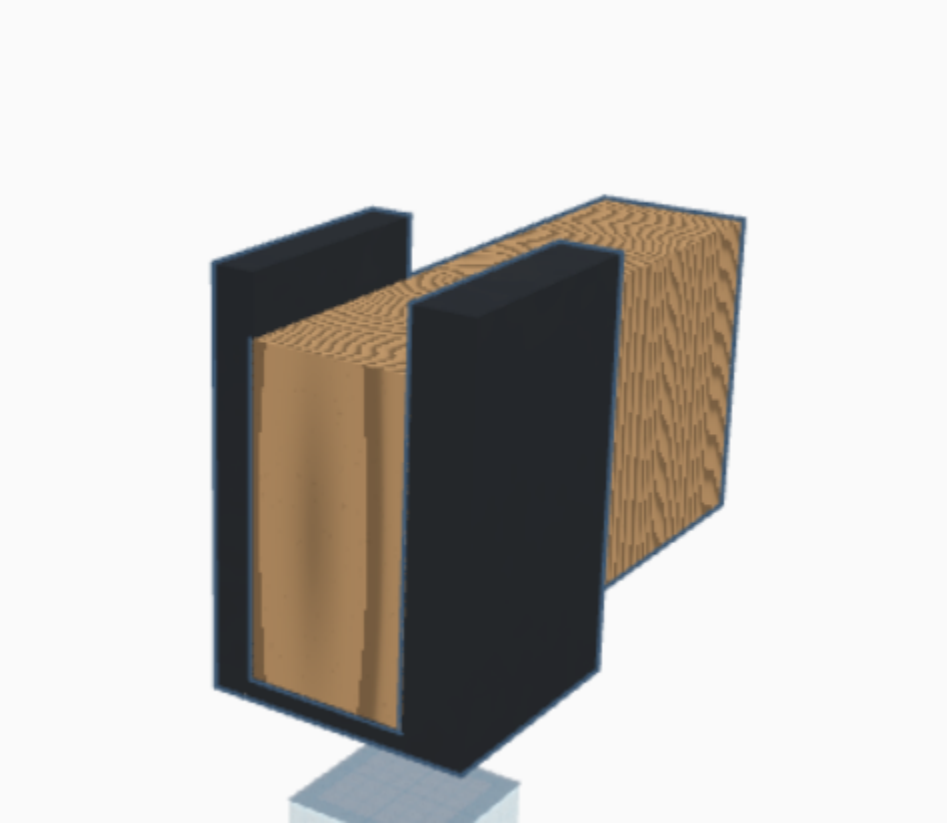

Fig. 1, The Locking Mechanism for the study room incorporating a wooden beam and a plastic U-Bracket

Fig. 2, The front face of the locking mechanism

Fig. 3, The side face of the locking mechanism

Fig. 4, The rear of the locking mechanism showing the slot for the servo to move the beam up and down

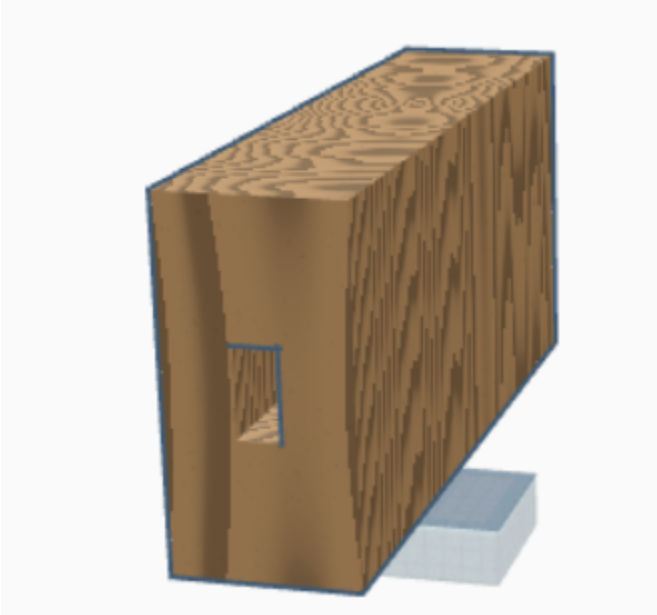

Fig. 5, The wooden beam to lock the door

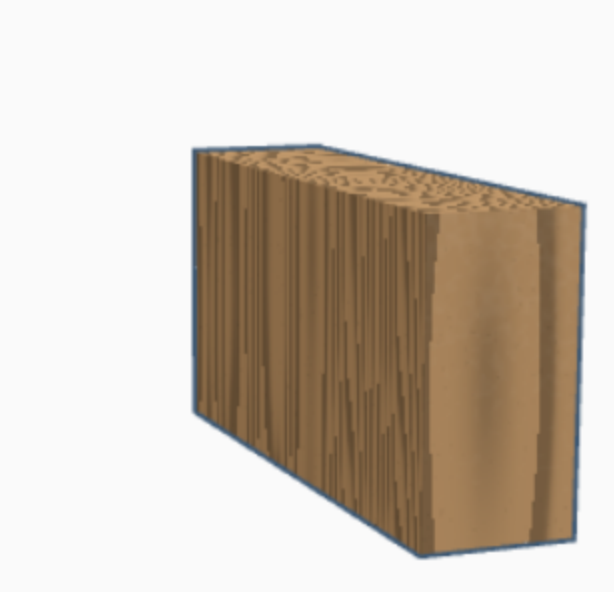

Fig. 6, An alternate view of the wooden beam

Fig. 7, The plastic U-Bracket for the locking mechanism

Fig. 8, Side view of the U-Bracket

Initially we planned to use the Fourier integral along with a Laplace Transformation to transfer the student number along radio waves by modulating a carrier wave. However, this proved to be quite challenging since there was complex math involved which we would easily make mistakes with, thus forcing us to move on to Bluetooth. We also initially planned on making a pager system but through analysis we realized that that is not a novel solution but rather a 75 year old invention that doesn't solve a problem, thus leading us to scrap it as an idea.

This is accomplished by writing the keypad input and a timestamp to a txt file and using the IEEE 802.15.1 protocol via an HC-05 module to build a Personal Area Network (PAN). Therefore, employing Frequency Hopping Spread Spectrum (FHSS) radio technology and Universal Synchronous and Asynchronous Receiver-Transmitter (USART) protocol to transmit data over air between the two STM microcontrollers [6].

Using FHSS in conjunction with BT Classic, which contains 79 channels, results in a fairly low collision probability of 1.27% [1]. On the secondary microcontroller, the .txt file with the user's student number is received and cross referenced against a .csv file that acts as a database of all the student numbers scheduled for that day and the time in which they are booked for. If the student is both booked for that day and that time, a signal is broadcast to unlock the room, wait 30 seconds, and re-lock the room.

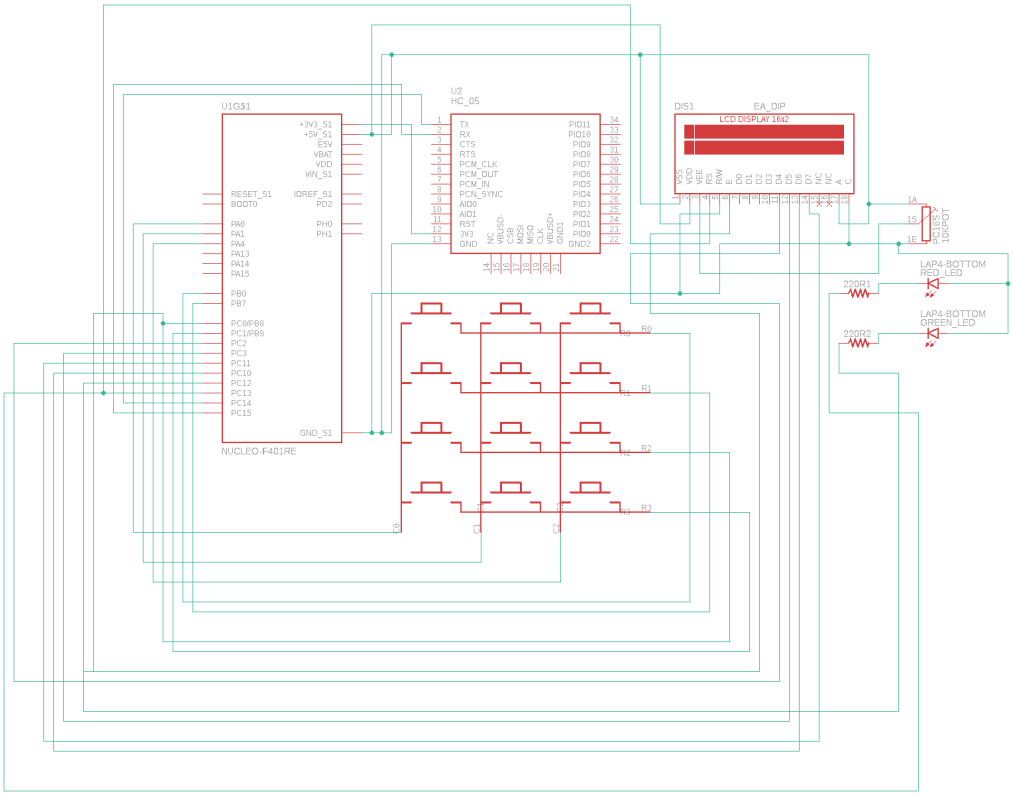


Fig. 9, The Schematic of the User's Interface containing a STM32, 4x3 Matrix Keypad, HC-05, LCD, 2 LEDs, 2 Resistors, and a Potentiometer.

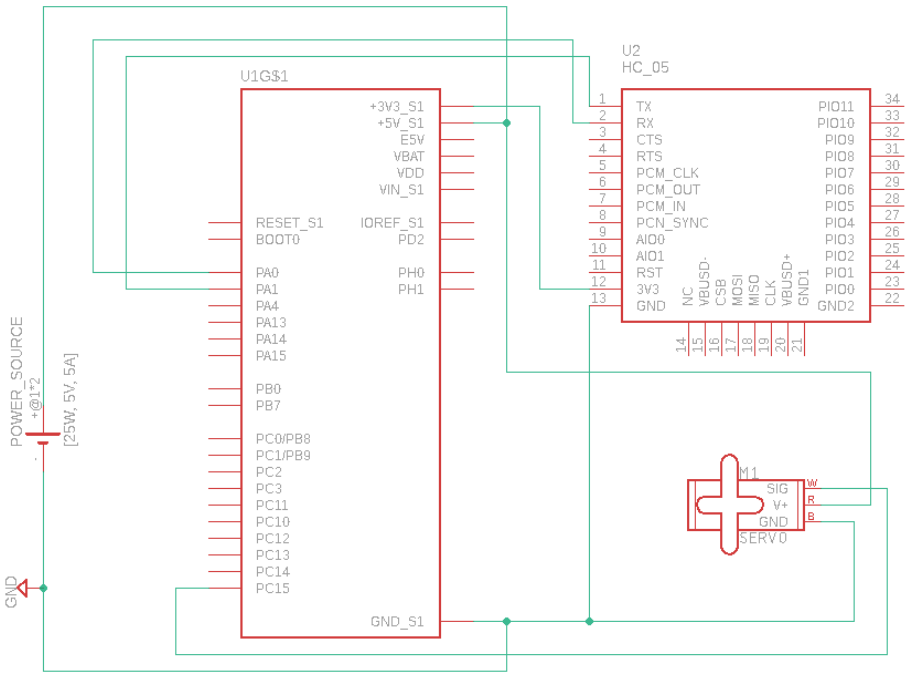


Fig. 10, The Schematic of the back end containing a STM32, HC-05 Module, and a Servo Motor

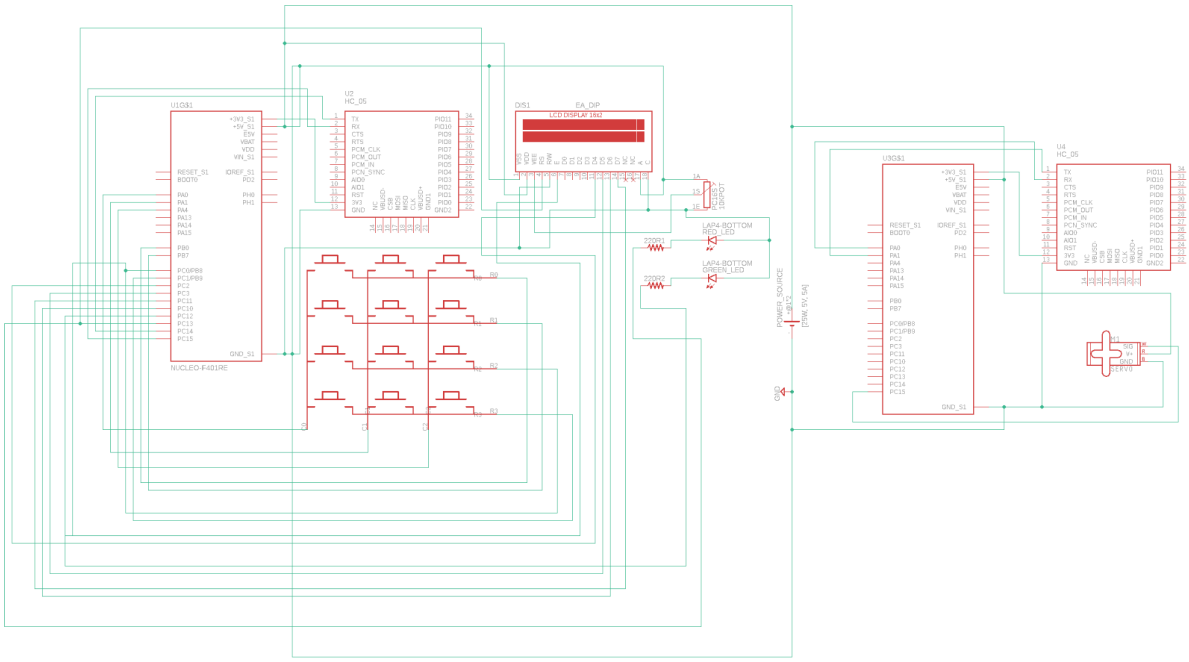

Fig. 11, A Schematic for the entire circuit including both Fig. 1, Fig. 2, and the power supply

## Technical Analysis

Our project employs several mathematical and scientific principles such as Signal-Noise Ratio (SNR), Shannon's Capacity, and Personal Area Networks (PAN).
With our HC-05 module, we will also use Gaussian Frequency Key Shifting (GFKS) to modulate the frequency of our binary transmission based on the binary value of our transmitted data (0 or 1) using the formula $f_m(t) = f_c + \Delta f \cdot b(t)$ where $f_c = 2.4\,GHz$, $\Delta f = \pm 500\,Hz$, thus $f_m(t) = (2.4 \times 10^9)Hz + 500\,Hz \cdot b(t)$. GFSK is a digital modulation technique used by Bluetooth where the carrier frequency is shifted based on binary data [20]. This reduces the bandwidth and improves resistance to interference.

Our HC-05 Bluetooth Module is a class 2 Bluetooth Module that excels at short-range wireless communication due to its transmission power rating of +4 dBm [3]. From the Friis transmission formula: $\frac{P_r}{P_t} = D_t D_r (\frac{\lambda}{4\pi d})^2$; where $P_r$ is power received, $P_t$ is power transmitted, $D_t$ is the directivity of the transmitting antenna, $D_r$ is the directivity of the receiving antenna, $\lambda$ is the signal wavelength, and $d$ is the distance between the two antennas [7]. The distance between the two antennas must be large enough such that they are in the far field of each other, which is the region with normal EM radiation or where the radiated power is inversely proportional to $d^2$, ( $d >> \lambda$) [9]. The free-space path loss is the loss factor that is due to distance or wavelength such that the ratio of power transmitted to received have no directivity ($D_t = D_r = 1$) [19].

$FSPL = (\frac{4\pi d}{\lambda})^2 = (\frac{4\pi df}{c})^2$.
FSPL can also be represented in terms of DeciBels:

$FSPL(dB) = 10log_{10}((\frac{4\pi df}{c})^2)$

$FSPL(dB) = 20log_{10}(\frac{4\pi df}{c})$

$FSPL(dB) = 20log_{10}(d) + 20log_{10}(f) + 20log_{10}(\frac{4\pi}{c})$

$FSPL(dB) = 20log_{10}(d) + 20log_{10}(f) - 147.55$

This formula is true using the standard SI unit meters for distance, hertz ($s^{-1}$) for frequency, meters per second ($m/s$) for c where c = 299 792 458 m/s in a vacuum.
The FSPL for up to 3 meters, which is the highest likely distance for our device to operate at, is $= 20log_{10}(3) + 20log_{10}(2.4 \times 10^9) - 147.55 \approx 49.597\,dB$
Using this, we can calculate the Power received using
$P_r = P_t - FSPL(dB) = 4dBm - 49.597\,dB = -45.497\,dBm$

Then, we can evaluate the Noise power for our HC-05 which uses a 1 MHz Bandwidth at room temperature [3]:

$N = kTB$; Where $k = 1.38 \times 10^{-23} J/K$ is Boltzmann's Constant which shows the fundamental relationship between temperature and energy, $T = 290K$ which is room temperature measured in degrees Kelvin, and $B = 10^6 Hz$ which is the bandwidth of the HC-05.

$N = (1.38 \times 10^{-23} J/K)(290K)(10^6 Hz) = 4.002 \times 10^{-15} W$

$N_{dB} = 10log_{10}(N) + 30 = 10log_{10}(4.002 \times 10^{-15} W) + 30 \approx -113.98\, dBm$

Finally, we can find the SNR which is

$SNR = P_r - N_{dB} = -45.497\, dBm + 113.98\, dBm = 68.483\, dB$

This is a fairly high SNR, thus showing we have a relatively strong signal relative to the noise meaning our device will be able to operate well at a wireless distance of 3 meters.

We can evaluate how optimized our HC-05 is by applying Shannon's Capacity which is:

$C = B \cdot log_2(1 + SNR) = 10^6 \cdot log_2(69.483) = 6118588.14\, bps = 6118.58814\, kbps$

Bluetooth Classic has a Capacity of 720 kbps and our HC-05 under ideal conditions has a theoretical capacity of 6120 kbps which exceeds the capacity of Bluetooth Classic, thus we are able to use the maximum capacity of Bluetooth Classic. In future iterations we might choose to use Bluetooth V2.0+EDR which has a capacity of 2 Mbps using 8DPSK modulation. The HC-05 has a theoretical capacity of 6 Mbps, however the HC-05 can only use up to Bluetooth V2.0+EDR technology meaning the module can only be 32.7% efficient.

A Personal Area Network or PAN is a wired or wireless network, often used in Bluetooth communications to transfer data, that connects several electronic devices together [2]. FHSS is a method of transmitting signals by quickly changing the carrier frequency among a specific range thus enabling the device to occupy a large spectral band [13]. USART is a protocol that enables devices to communicate via serial ports by writing data to the serial ports of a microcontroller. However USART uses a clock signal to communicate faster in synchronous mode. USART is commonly used in industrial equipment and Embedded Systems applications [21].

# Costs

## Manufacturing and Implementation Costs

**Bill of Materials (BOM):**

| Quantity | Part Number | Description | Cost ($ CAD) | URL |
|---|---|---|---|---|
| 1 | P160KN2-0QA25B10K | 10K Ohm 3-Pin Potentiometer | 2.86 | https://www.digikey.ca/short/wd7vnp3w |
| 2 | MFR-25FBF52-220R | 220 Ohm Resistor | 0.15 | https://www.digikey.ca/short/zpr3jhh5 |
| 1 | LCD-18160 | LCD Module - 2x16 Display | 27.17 | https://www.digikey.ca/short/fpv8www9 |
| 1 | 154 | Servo | 18.71 | https://www.digikey.ca/short/z5r34q9q |
| 1 | 151051SS04000 | Red LED | 0.39 | https://www.digikey.ca/short/h52bww18 |
| 1 | 151051VS04000 | Green LED | 0.41 | https://www.digikey.ca/short/wzbj9p31 |
| 1 | VGS-25W-5 | 25W Power Supply Unit - 5V, 5A | 19.52 | https://www.digikey.ca/short/529jdmm5 |
| 2 | 113990636 | HC-05 Bluetooth Module | 3.52 | https://www.digikey.ca/short/bprvtz5f |
| 2 | NUCLEO-F401RE | STM32 NUCLEO-F401RE Development Board | 20.31 | https://www.digikey.ca/short/9vw3c0b3 |
| All Parts | | | 117.02 | |

# Risks

## Energy Analysis

Voltage and current are relatively low but still have some risks. They can cause electric shock, burns, explosions, arcing, or fires. This can not only damage the design but also the public [5].

STM32-401RE [16]:

- Has a maximum voltage of 3.6V
- Assuming all I/O ports and timers were used at once, maximum power is 3.32W (using P = I*V)

Bluetooth Module [8]:

- Has a maximum voltage of 6V
- Maximum current of 30mA which means maximum power of 0.18W (using P = I*V)

Keypad [23]:

- Maximum voltage of 5V
- Maximum current of 500mA which means maximum power of 2.5W (using P = I*V)

LCDs [14]:

- Maximum voltage of 2.4V
- Maximum current of 1.1mA which means maximum power of 0.0026W (using P = I*V)

Locking Mechanism [15]:

- Maximum voltage of 6V
- Maximum current of 650mA which means maximum power of 3.9W (using P = I*V)

Maximum Possible energy consumption:

- Adding up all the powers, there is a maximum wattage of about 10W, well below the maximum allowed of 30W.
- Given our analysis above, it is impossible to exceed physical power and energy limits required on the design.
- There will be no storage of electric potential energy since there are no capacitors or batteries.

## Risk Analysis

Risks from intended use:

- If the door fails to unlock or lock, it can cause users to become annoyed and dissatisfied.
- Locking mechanism might get stuck and therefore cause the door to be unable to move
- The database of allowed users may be unable to be updated in the case of a wifi outage

Risks from incorrect use:

- Unauthorized access due to code sharing may lead to security breaches if shared with people who aren't authorized to enter certain spaces.
- Attempting to force open the door without proper access can lead to potential damage.

Risks from misuse:

- Attempting to reprogram or override access codes
- Tampering with the keypad or bluetooth device may render it unusable
- May cause electrical shocks if tampered with the connection to the electrical outlet, potentially harming user

Possible sources of malfunction:

- Short circuits may occur due to poor insulation or faulty connections, which may cause fires, electrical shocks or complete failure
- If water penetrates the design, it can lead to corrosion or short circuits
- Unexpected movements or impacts may break sensitive components which could impact the safety of the system.

# Testing and Validation

## Test Plan

Keypad works to input characters:

- Setup: Connect the keypad to the system, ensure the system is configured properly and has a stable power supply.
- Environment: Conduct a test in a common use environment (indoors, about 20$^{O}$C and proper humidity).
- Test Inputs: Input our student IDs into the keypad.
- Measurement: Verify that each key pressed is accepted by the system in reasonable time (eg 100ms).
- Pass Criteria: Imputed code appears on the screen in correct order with no errors in a reasonable time.

LCD Display:

- Test Setup: Connect the LCD display to the system, ensure the system is configured properly and has a stable power supply.
- Environment: Conduct a test in a common use environment (indoors, about 20$^{O}$C and proper humidity).
- Test Inputs: Send the string “12341234” from the control system to the LCD.
- Measurement Standard: Verify that the entire string appears on the LCD without distortion, flickering, or character loss.
- Pass Criteria: The string “12341234” appears fully and clearly on the display in a reasonable time.

Locking mechanism:

- Test Setup: Connect the locking mechanism to the system, ensure the system is configured properly and has a stable power supply.
- Environment: Conduct a test in a common use environment (indoors, about 20$^{O}$C and proper humidity).
- Test Inputs: Send a command to unlock the locking mechanism.
- Measurement Standard: Verify that lock has been successfully unlocked after a reasonable amount of time.
- Pass Criteria: The lock mechanism has successfully unlocked and the user is able to open the door.

Names are stored and can be called from database:

- Test Setup: Connect the database to the system. Set up a test database with names and the system with read and write permissions.
- Environment: Conduct a test in a common use environment (indoors, about 20$^{O}$C and proper humidity).
- Test Inputs: Enter and store the names "Chris" "Ishan" and "Luka" into the database. After, retrieve each name.
- Measurement Standard: Verify each name is stored and retrieved accurately.
- Pass Criteria: Each stored name can be retrieved accurately.

Bluetooth connection:

- Test Setup: Place a device in Bluetooth pairing mode within 2 meters of the locking mechanism.
- Environment: Conduct a test in a common use environment (indoors, about 20$^{O}$C and proper humidity).
- Test Inputs: Pair and connect the device with the system’s Bluetooth.
- Measurement Standard: Confirm that the connection remains stable without interruption for at least 30 seconds.
- Pass Criteria: The connection establishes remains stable for at least 30 seconds without disconnection

# Works Cited


1. Cho, Hae-Keun & Lim, Yeon-June & Hwang, In-Kwan & Pyo, Cheol-Sig. (2006). Collision Probability md Traffic Processing Time Analysis for RFID System using FHSS Scheme. The Journal of Korea Information and Communications Society. 31. https://www.researchgate.net/publication/263650701_Collision_Probability_md_Traffic_Processing_Time_Analysis_for_RFID_System_using_FHSS_Scheme/citation/download
2. Cloudflare. (2024). *What is a personal area network (PAN)?*. Cloudflare. https://www.cloudflare.com/learning/network-layer/what-is-a-personal-area-network/
3. Components101. (2010, June 18). *HC-05 - Bluetooth to Serial Port Module* . HC-05 Datasheet. https://components101.com/sites/default/files/component_datasheet/HC-05%20Datasheet.pdf
4. ControllersTech. (n.d.). STM32 communication using HC-05 . STM32 Communication using HC-05. https://controllerstech.com/stm32-communication-using-hc-05/
5. Electrical Safety UK, “What are electrical hazards? | Dangers of electricity,” *elecsafety.co.uk*, Jul. 10, 2020. https://elecsafety.co.uk/what-are-electrical-hazards/
6. Electronic Wings. (2024). Bluetooth module HC-05 Pinout, at Commands & Arduino programming .. Bluetooth Module HC-05 Pinout, AT Commands & Arduino Programming. https://www.electronicwings.com/sensors-modules/bluetooth-module-hc-05-
7. H. T. Friis, "A Note on a Simple Transmission Formula," in Proceedings of the IRE, vol. 34, no. 5, pp. 254-256, May 1946, doi: 10.1109/JRPROC.1946.234568. https://ieeexplore.ieee.org/document/1697062
8. “HC-05 Bluetooth Module Pinout, Specifications, Default Settings, Replacements & Datasheet,” *Components101.com*, Jul. 16, 2021. https://components101.com/wireless/hc-05-bluetooth-module
9. Johnson, R. C., Jasik, H. (1984). Antenna Engineering Handbook. United Kingdom: McGraw-Hill. https://www.google.ca/books/edition/Antenna_Engineering_Handbook/_mxGAAAAYAAJ?hl=en&gbpv=1&bsq=isbn:0070322910&dq=isbn:0070322910&printsec=frontcover
10. Northeast Protection Partners. (2022, August 25). *8 important campus security solutions for Colleges & Universities*. Northeast Protection Partners. https://www.nepps.com/blog/campus-security-solutions-for-colleges-universities/
11. Prowten, M. (2022, March 28). *Bluetooth’s access control benefits*. Campus Safety. https://www.campussafetymagazine.com/news/bluetooths-access-control-benefits/111460/
12. “Quick facts | About Waterloo,” uwaterloo.ca. https://uwaterloo.ca/about/facts
13. Rohde & Schwarz. (2024). *Fundamentals of hopping signals*. Technology fundamentals. https://www.rohde-schwarz.com/ca/knowledge-center/technology-fundamentals/hopper-signals/hopper-signals_256050.html

14. “Specification for LCD Module 1602A-1 (V1.2),” 2010. Available: https://www.openhacks.com/uploadsproductos/eone-1602a1.pdf
15. “Specification of Product V2.0 Specification -30℃～80℃.” Accessed: Oct. 30, 2024. [Online]. Available: https://cdn-shop.adafruit.com/product-files/2442/FS90R-V2.0_specs.pdf
16. “STM32F401RE,” *STMicroelectronics*. https://www.st.com/en/microcontrollers-microprocessors/stm32f401re.html
17. University of Waterloo. (2024, October 30). *Library*. Q. How do I book a study room? https://libanswers.uwaterloo.ca/UsetheLibraryandServices/faq/40638
18. University of Waterloo. (n.d.). Study Rooms. Library. https://uwaterloo.ca/library/services/study-rooms
19. Whitaker, J. C. (1996). *The Electronics Handbook*. CRC Press. https://books.google.ca/books?id=DSHSqWQXm3oC&dq=f%22free+space+path+loss%22&pg=PA1321&redir_esc=y#v=onepage&q&f=false
20. Woolley, M. (2020a, December 9). Bluetooth Core Specification Version 5.2 Feature Overview. https://www.bluetooth.com/wp-content/uploads/2020/01/Bluetooth_5.2_Feature_Overview.pdf
21. Wright, G. (2022, November). *USART (universal synchronous/asynchronous receiver/transmitter)*. WhatIs. https://www.techtarget.com/whatis/definition/USART-Universal-Synchronous-Asynchronous-Receiver-Transmitter
22. Yıldırım, M., Mackie, I. Encouraging users to improve password security and memorability. *Int. J. Inf. Secur.* 18, 741–759 (2019). https://doi.org/10.1007/s10207-019-00429-y
23. “4x4 Matrix Membrane Keypad (#27899).” Available: https://cdn.sparkfun.com/assets/f/f/a/5/0/DS-16038.pdf