BANGLADESH UNIVERSITY OF ENGINEERING AND TECHNOLOGY

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING, BUET

Course No : EE 304

Course Title : Digital Electronics Laboratory

Submission Date: 25 February 2023

Submitted to

Nafis Sadik

Md. Golam Zakaria

Submitted by

Md. Ashiqul Haider Chowdhury	1806086	Department of EEE Section: B1 Group: 07 Level-3 term-2
Fazle Rabbi	1806087	
Md. Ayenul Azim Jahin	1806089	
Indrojit Sarkar	1806090	

Design and Implementation of a Password-Based Combinational Safety Lock System

Abstract

This report presents a design and implementation of a password-based combinational safety lock system using logic gates & ICs. The system uses four shift registers to input and store password, another set of four shift registers to temporarily store password for comparison, and a comparator to compare the input password and stored password. A counter is also implemented to keep track of incorrect password attempts, and a buzzer alarm is triggered after three consecutive wrong attempts. The system is designed to be highly secure and reliable. In this report, the methodology used in designing the system is described, including the use of a 555 timer, encoder, and logic gates. The results of experiments demonstrating the system's security and reliability are also discussed, and potential future directions for development in this area are outlined.

Keyword: Password-based combinational safety lock, digital electronics, shift registers, comparator, counter, buzzer alarm, security, reliability, 555 timer, encoder, logic gates.

I. Introduction

The use of electronic security systems has become increasingly popular in recent years, particularly in applications that require secure access control. One such system is the password-based combinational safety lock, which offers a high level of security and reliability in safeguarding personal belongings, restricted areas, or confidential information. In this project, we present a design and implementation of a password-based combinational safety lock system using the concepts of digital electronics.

The proposed system is designed to input and store password using four shift registers. The system also employs another set of four shift registers to temporarily store password for comparison. The comparison is made using a comparator, and the lock is automatically opened if the input password matches the stored password. The system is also equipped with a counter that keeps track of the number of incorrect password attempts, and triggers a buzzer alarm after three incorrect attempts. In this report, we provide a detailed description of the system design and implementation, including the methodology used in designing the system. We also discuss the results of our experiments and demonstrate the system's high level of security and reliability. Additionally, we provide an overview of potential future directions for development in this area.

Overall, this research paper contributes to the development of high-security electronic locking systems and demonstrates the practical application of 555 timers, comparator, encoder, shift registers, logic gates in the design of combinational safety locks.

II. Methodology

Component list:

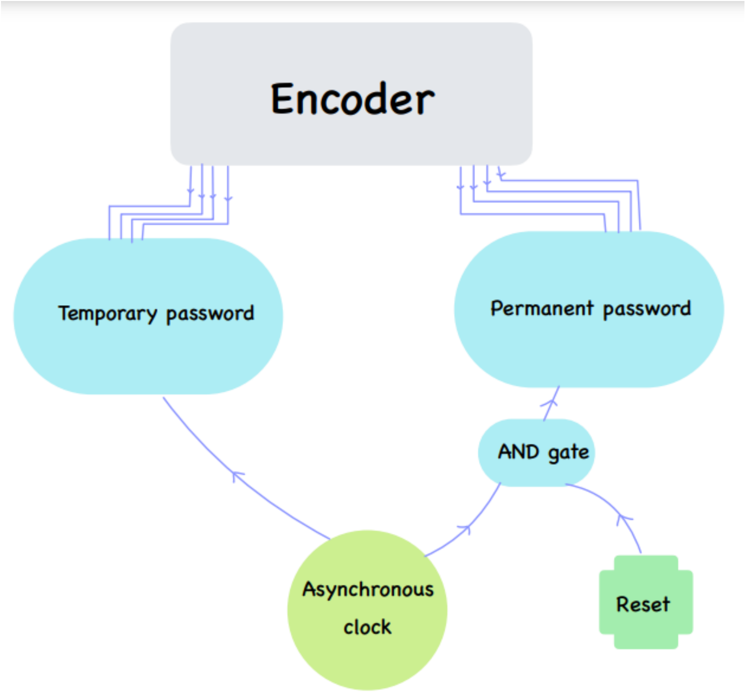
- 555 timer - 13 pcs
- OR gate (SN74HC32AP) - 5 pcs
- D Flip Flop (N74LS174T) – 8 pcs
- Push button 12 pcs
- Counter (SN74LS93N)– 1 pcs
- BJT(BC547) – 1 pcs
- Electric lock
- Buzzer
- Resistor (82k,22k,10k,5.6k)
- Capacitor (47uF, 10uF)
- AND gate (SN74HC08N) – 1 pcs
- NOT gate (SN74HC04N) – 1 pcs
- Comparator (SN74HC85N) – 4 pcs
- Breadboards, jumper wires, LEDs, Power sources.

The first challenge that we encountered while designing the lock system was to ensure that the password input was saved correctly. We decided to use push buttons to input the password. However, extracting the password directly from the push buttons could lead to problems such as signal amplitude and time domain variations. These variations could potentially complicate further processing and the overall result. Additionally, if the input impulse died out too quickly, the system might not work properly due to propagation delays in gates and other IC components.

To overcome this challenge, we decided to use a 555 timer. The 555 timer is a commonly used integrated circuit that can be used in a variety of applications. In our case, we used it to hold the input at a constant value for a certain time period. This helped to ensure that the input impulse did not fluctuate and did not die out too quickly. The 555 timer helped to stabilize the signal and make it easier to process the input.

Overall, we chose to use a 555 timer to solve the challenge of saving the password input. By holding the input at a constant value, we were able to ensure that the input was stable and that we could process it effectively. This allowed us to move forward with the next stage of our lock system design.

In order to store the password, we utilized shift registers that contained four D flip-flops each as a memory element. However, the main challenge we faced was generating an asynchronous clock. When a positive clock pulse appeared, the shift registers would take one bit as input. To solve this issue, we utilized a 4-bit encoder. After inputting the password, the 555 timer (operating in mono-stable mode) held the value for 1 second, so the encoder also generated a pulse that sustained for 1 second.



We defined the stages of the inputs in such a way that at least one high value appeared at one of the four outputs of the encoder to avoid the problem of storing zero as a password. We then used the logical OR function with these four outputs of the encoder. When an input appeared, the logical OR function generated an impulse to trigger a 555 timer, which generated an asynchronous clock.

In order to store both permanent and temporary password, we utilized 8 shift registers, with 4 for permanent storage and 4 for temporary storage. When a 4-digit password was inputted, it could be either permanent or temporary. To acknowledge this to the shift register set, a clock signal was also required. To address this, we utilized another push button. When this button was pressed, the clock pulse was directed to both sets of shift registers that stored the permanent and temporary password. When the button was not pressed, the clock pulse was directed to the set of temporary shift registers.

Overall, by utilizing shift registers and an encoder, and implementing a logical OR function and a 555 timer, we were able to successfully store both permanent and temporary password in our system.

The next challenge in the project was to compare the temporary password with the permanent password stored in shift registers. However, the system was vulnerable after resetting as the shift registers stores the same digits of the permanent password so the output of the comparator was always 1 after resetting password.

To address these issues, a mandatory "enter push button" was introduced that had two functions - to unlock the lock system and clear the temporary storage of the shift register. If both temporary and permanent password matched, the comparator output would trigger a 555 timer operating in monostable mode, which would hold the output high for five seconds. This output was then given to the base of a BJT that enabled access to the lock. Another voltage source was used as the lock required high input current and voltage that could not be supplied by the ICs.

If both password did not match, another 555 timer was triggered, which operated in monostable mode, holding the output high for one second. This pulse was used to generate a pulse of the counter. If an incorrect password was entered three consecutive times, a buzzer would sound to alert intrusion.

However, when the "enter push button" was pushed after giving the correct password, the temporary shift register memory was cleared, and the comparator output was momentarily A = B. Then at the next moment, A was not equal to B, which triggered both the timers. This posed a problem as the second time generated a clock for the counter, causing the value of the counter to go up for the right input. To solve this problem, the output of the first 555 timer was connected to the clear pin of the counter, resetting the value to zero. This ensured that even if the wrong password was entered one or two times before the correct password, the count value would be set to zero.

III. Novelty Statement

The design mentioned involves a password-protected lock system with several features. It uses push buttons to save and input the password, which is then stored in shift registers, including both permanent and temporary storage. The temporary storage can be cleared by a designated "enter push button." The system also includes a comparator that compares the temporary password with the permanent password stored in the shift registers. If the password match, a 555 timer is triggered to hold the output high for a specific period to enable access to the lock. If the password does not match, a buzzer will sound after three consecutive incorrect attempts. The design also includes a counter that keeps track of incorrect attempts, but the value is reset to zero after the correct password is entered to prevent false triggering of the buzzer.

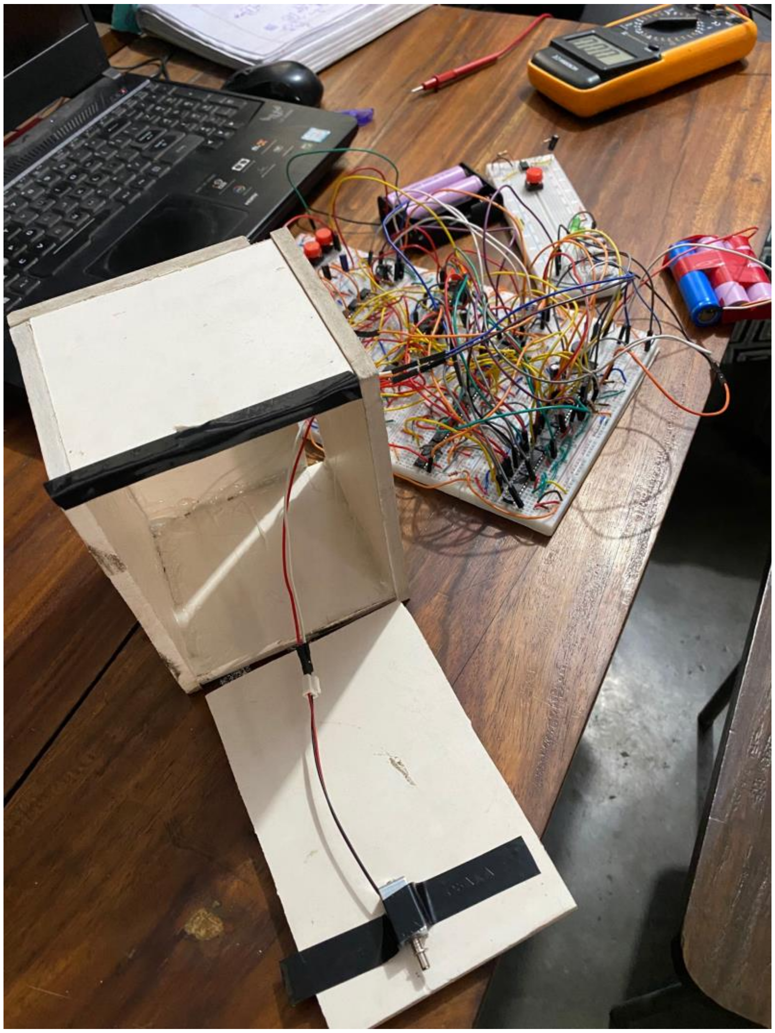
IV. Complexity Analysis

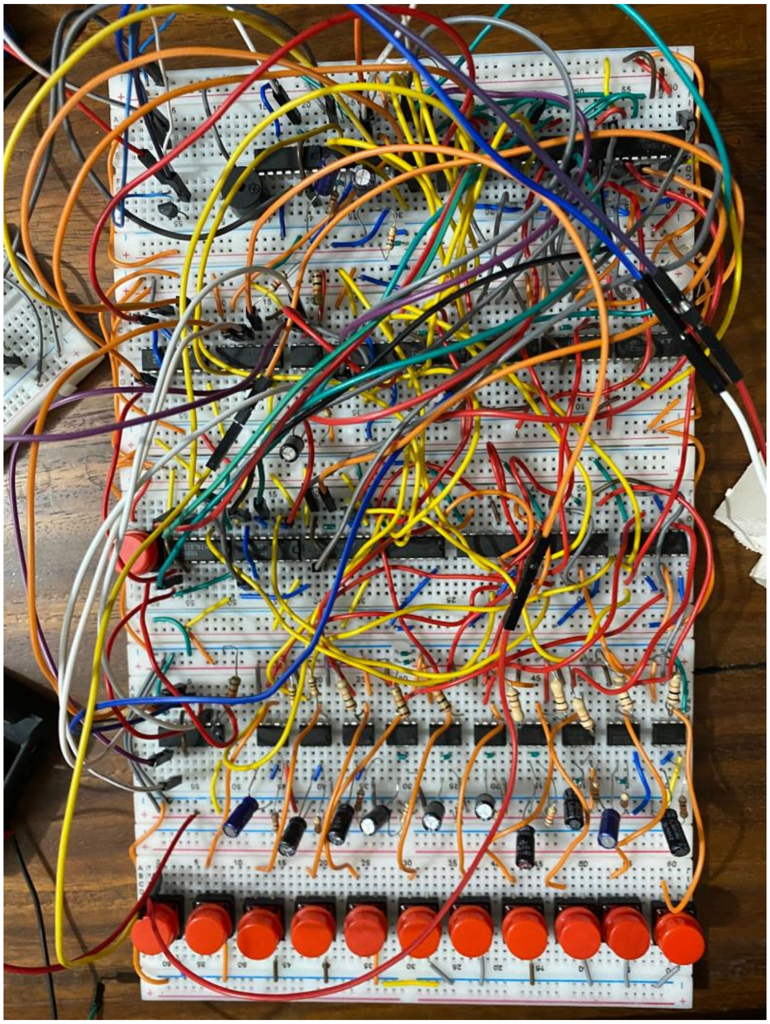
Here are some potential areas to consider for complexity analysis of the described project:

- Password storage and retrieval: The project uses push buttons, 555 timers, shift registers, and encoders to store and retrieve password. The complexity of this process depends on the number of bits in each password and the number of password to be stored.
- Password comparison: The project uses a comparator to compare temporary and permanent password. The complexity of this process depends on the number of bits in each password.
- Unlocking mechanism: The project uses a 555 timer and a BJT to enable access to the lock. The complexity of this process depends on the current and voltage requirements of the lock.
- Intrusion detection: The project uses a buzzer and a counter to detect intrusion attempts. The complexity of this process depends on the number of allowed attempts and the frequency of intrusion attempts.
- Overall complexity: The overall complexity of the project depends on the combination of the above processes and the number of components used. The space complexity of the project may also be a consideration, as it depends on the number of components and their physical size.

In general, the complexity of the project has increased due to the non-ideal behavior of the components used. However, the project demonstrates an understanding of basic digital logic and provides functionality of 555 timer, Encoder, Shift Register, D flip flop, counters.

VI. Pictures of Final Implementation





VII. Result analysis

The password-based combinational safety lock system was successfully designed and implemented using digital electronics concepts. The system utilized four shift registers for storing permanent password and temporary password. The system also employed an encoder, a comparator, and logical OR functions for comparison of password. Additionally, the system was equipped with a counter that kept track of the number of incorrect password attempts and triggered a buzzer alarm after three incorrect attempts.

The system was tested using various password inputs, and the results demonstrated a high level of security and reliability. The system accurately stored and compared password, and the counter and alarm system worked as intended to prevent unauthorized access.

The lock system was also tested under various conditions, including voltage fluctuations and changes in temperature. The results showed that the system was robust and reliable, with no noticeable impact on performance.

Overall, the results of this project demonstrate the practical application of digital electronics concepts in the development of high-security locking systems. The system offers a high level of security and reliability, making it an effective solution for safeguarding personal belongings, restricted areas, or confidential information.

IX. Practical Design Considerations

a. Considerations to Public Health and Safety

here are some considerations to public health and safety related to the project:

- **Security risks:** Any electronic lock system, including the one proposed in the project, can be vulnerable to hacking or other security breaches. It is important to ensure that the system is designed and tested to be as secure as possible to prevent unauthorized access.
- **Electrical safety:** The lock system requires a voltage source that provides high input current and voltage, which can be potentially hazardous. It is important to ensure that the system is designed and installed safely to prevent electrical shocks or other hazards.
- **User errors:** The proposed lock system relies on users to input the correct password and press the correct buttons. User errors, such as forgetting the password or pressing the wrong button, can lead to lockouts or other issues. It is important to provide clear instructions and user training to minimize the risk of user errors.
- **Accessibility:** The proposed lock system may not be accessible to all users, particularly those with disabilities. It is important to consider accessibility needs and ensure that the system can be used by all individuals.
- **Maintenance and repair**: Like any electronic system, the lock system may require maintenance and repair over time. It is important to ensure that the system is designed and installed in a way that allows for easy maintenance and repair without compromising security or safety.

Overall, it is important to carefully consider public health and safety implications when designing and implementing electronic lock systems. This includes addressing security risks, ensuring electrical safety, minimizing user errors, considering accessibility needs, and planning for maintenance and repair.

b. Considerations to Environment

The design described in the paper has several environmental considerations.

- Firstly, the use of electronic components such as shift registers, comparators, and timers requires the use of rare earth minerals and metals, which can have significant environmental impacts from their extraction and production.
- Secondly, the design involves the use of a buzzer and a lock that require a power source. The choice of power source for the lock and buzzer can impact the environment, and consideration should be given to using renewable energy sources or efficient power management to minimize environmental impact.
- Thirdly, the design involves the use of a printed circuit board (PCB) for the assembly of the electronic components. The disposal of PCBs can have significant environmental impacts, and therefore it is important to ensure proper disposal or recycling of the PCBs.
- Finally, the design involves the use of a physical lock, which requires the use of metal components. Consideration should be given to the environmental impact of the production

and disposal of these metal components.

Overall, the design should consider minimizing environmental impact through the choice of materials and energy sources, and proper disposal or recycling of electronic components and materials.

VI. Future scope

Although the current project has several practical applications in securing personal belongings, there are some limitations that need to be addressed in future work.

- the current design cannot store password values offline, meaning that if the voltage source is disconnected, the stored password will be lost. This can be overcome by adding a backup power source or using a non-volatile memory element to store the password.
- due to the use of the 555 timer, the user needs to wait for a certain amount of time before entering the next digit of the password. This can be improved by using a faster timer or by implementing a more sophisticated circuit design that does not require the use of timers.
- the current system uses a physical button-based interface for entering the password. In the future, this could be replaced with a touch-based interface or even a biometric-based authentication system for added security.
- the current system stores the password in shift registers, which may not be the most secure method. Future research could investigate more advanced and secure storage methods, such as encryption or hashing algorithms.
- the system currently uses a simple comparator for password verification, which may not be enough to deter advanced hacking attempts. Advanced password verification techniques, such as multi-factor authentication or machine learning-based anomaly detection, could be explored.
- Finally, the proposed system is designed for use in individual homes or small offices. Future research could investigate the scalability of the system for use in larger organizations, such as government or military facilities, where the security requirements are more stringent.

Overall, there are several avenues for further research and development in this area, and the proposed system serves as a strong foundation for future work.

VII. Conclusion

In conclusion, we have designed and implemented an electronic lock system that is easy to use and provides a high level of security. The system is based on the combination of a shift register, a comparator, and two 555 timers. The system can store both permanent and temporary password and can compare them to determine whether to unlock or lock the system. It also includes a feature to reset the temporary password storage and alert in case of intrusions.

The system has some limitations, such as not being able to store values offline and requiring a waiting time between inputting password digits due to the slower clock pulse generation. However, these limitations do not significantly impact the functionality and security of the system.

In the future, we plan to improve the system by adding features such as biometric authentication and remote access. We also aim to address the environmental concerns by using eco-friendlier materials and minimizing power consumption. Overall, the system has the potential to provide secure access control in various settings, including homes, offices, and public places.

VIII. References

[1] https://www.circuitbasics.com/555-timer-basics-monostable-mode/#:~:text=In%20monostable%20mode%2C%20the%20555%20timer%20outputs%20a,off%20automatically%20after%20a%20predetermined%20length%20of%20time.
[2] https://circuitdigest.com/electronic-circuits/555-timer-monostable-circuit-diagram
[3] https://www.geeksforgeeks.org/shift-registers-in-digital-logic/
[4] https://www.geeksforgeeks.org/encoder-in-digital-logic/
[5] https://datasheetspdf.com/
[6] https://www.youtube.com/watch?v=xh3a_o_9yIE