DESIGN AND IMPLEMENTATION OF AN AUTOMATED SAFETY LOCK SYSTEM WITH MULTIPLE AUTHENTICATIONS AND ALARM PROTECTION

Slavčo Premčeski¹, Dame Korunoški², Anastasija Ignjatovska², Damjan Pecioskii²

¹Student at Faculty of Mechanical Engineering, “Ss. Cyril and Methodius” University in Skopje
²Faculty of Mechanical Engineering, “Ss. Cyril and Methodius” University in Skopje, P.O.Box 464, MK-1001 Skopje, Republic of North Macedonia
slavco.premceski@gmail.com

Abstract: As a result of continuous technological development, repetitive manual tasks can be performed by automated systems which are required to meet the challenges and requirements of the modern world. An ordinary lock would also allow a higher level of flexibility when dealing with multiple users of an object. This paper proposes a combination of electronic components and a mechanical lock controlled by an Arduino controller. There are three main subsystems: an authentication system, an output system (locking mechanism), and an alarm system. The proposed standard password authentication can be performed by both physical input on a keypad or through Bluetooth communication via a mobile application. The alarm subsystem allows additional safety from unauthorized access. The locking mechanism is driven by a servo motor and can be implemented on several types of access points such as doors, drawers, safes, and so on.

Key words: automation; safety lock; alarm; design; Arduino controller

1. INTRODUCTION

User authentication is a useful tool for ensuring limited access to a device by verifying the user’s identity. Only the user(s) that know the password can enter the access point. The motivation behind this idea comes from the necessity of an automated lock system that allows the privacy of user authentication within a physical domain. It enables easier control of the desired access point (door), without the concern of where someone has left their keys. There are diverse designs that allow automatic door authentication and access. I. Yugashini et al. [1] proposed a complex algorithm of face recognition
using a magnetic door. If the user were to be recognized, the controller would send a signal to unlock the door. The system incorporates a GSM (Global System for Mobile communication) modem that sends a message to the host if the face of the person trying to enter has not been recognized. The system ranges from home appliances to large-scale installations. Its drawback is the rare use of GSM applications and the cost of the algorithm. O. Doh and I. Ha [2] proposed a digital lock system controlled by a Raspberry Pi computer. The validation of the user can be achieved through a standard password, Bluetooth communication or facial recognition. If an intruder tries to open the door with an impact, the system can detect it, take a picture of the intruder, and send it to the server through wireless communication. The computer serving as a controller is much more powerful, but also less cost-effective. P. Bhushan et al. [3] proposed a complex door lock system that incorporates a server installed on the door. Authentication is done by combining RFID (Radio Frequency Identification) and biometrics. The server controls the digital lock and communicates with the smartphone. Its downside is using a whole server just to control a door which is not effective. S. Goswami et al. [4] proposed a door lock system controlled by an "8051 controller". In this paper, the proposed system is powered by AC (alternating current) voltage. The authentication is performed by inputting a password through a 7-segment display. T. H. Thong and Dr. Z. Ma Ma Myo [5] proposed a system that is implemented on university entry counters. A PIR (passive infrared) sensor detects a person’s motion and opens the entry with the use of a stepper motor. This paper, however, does not focus on safety and authentication. A more elegant and more complex approach was proposed by T. Adiono et al. [6], whose paper revolves around the idea of smart home application. The main controller is a Raspberry Pi computer, where the validation of the user is performed over a smart application that connects to the controller through cloud storage. It is GPS (Global Positioning System) based, meaning that the phone sends its coordinates to the user. The lock serves as an on/off solenoid switch that receives a signal from another controller through the main host. This kind of system has two controllers and GPS is rarely used for safety lock applications. H.-S. Lee and L.-C. Hsieh [7] proposed a design of a mechanism for car-door opening. The actuator for this design is a DC (direct current) motor. Its motion is converted to linear with a worm gear, which then transfers its output motion to a screw pair. This enables linear motion of the screw slider, which matches the kinematic requirement of a car-door.

This paper does not focus on the control of the motion, but rather on the motion itself. Downs et al. [8] designed a residential door opener that enables motion with a wire and set of pulleys. Their concept also includes detailed technical documentation and dynamic analysis as proof of concept. The motion is performed by a motor which is controlled by an Arduino controller. This paper focuses on the motion of the mechanism, rather than the safety of the object.

A review of relevant literature shows that distinct types of systems have their own deficiencies, which mainly revolve around complexity and cost-effectiveness. This paper, which is a part of a bachelor’s degree thesis, proposes a design of an automated safety lock with an equivalent safety level while keeping low costs and simplicity.

2. METHODOLOGY

Developing a safety system that is reliable and grants a high-security level, which is low-cost and effective, is the aim of this paper. Such a system requires automatic actuation and control, as well as real-time information sharing. In this regard, low-budget equipment has been chosen for the prototype of this system. In the proposed system, the required manual task for unlocking a mechanical lock is substituted with an electrical signal from an Arduino controller. Figure 1 shows a block diagram of the overall system architecture and its levels of communication. The locking mechanism will be presented more specifically in the next section. The user could cross the access point over two different and independent ways of authentication. The first authentication is standard, by inputting a previously memorized password. The user could enter the password on a keypad, and once the password is confirmed by the controller, the access point would automatically unlock. The system has indicators of the state of the access point. There would be two indicators, one showing the locked state and the other one showing the unlocked state.

The second authentication can be achieved via Bluetooth communication. The proposed system incorporates wireless access which can be achieved by a smartphone application through another previously memorized password. When the password is confirmed and the connection is established, a simple command on the smartphone would unlock the access point.
3. DESIGN OF THE SYSTEM

a) System architecture

The chosen components and their features are shown in Table 1. The system consists of eight components:

- Arduino which controls the system,
- diodes that show the state of the lock,
- an actuator that enables lock control,
- a button that allows control of the lock from the inside,
- a Bluetooth module that is used for wireless communication,
- an alarm subsystem that consists of an ultrasonic distance sensor and a buzzer; multiple sensors could be used to cover all possible entry points,
- a buzzer that generates a high-frequency sound in case the sensor detects an intruder.

Table 1

<table>
<thead>
<tr>
<th>Component</th>
<th>Specification</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diodes</td>
<td>Red and green</td>
<td>Shows state</td>
</tr>
<tr>
<td>Button</td>
<td>3 terminals</td>
<td>Inside-control</td>
</tr>
<tr>
<td>Keypad</td>
<td>HC-543 4x4</td>
<td>Authentication</td>
</tr>
<tr>
<td>Motor</td>
<td>SG90 Servo</td>
<td>Mechanism control</td>
</tr>
<tr>
<td>Controller</td>
<td>Arduino MEGA 2560</td>
<td>Controls the system</td>
</tr>
<tr>
<td>Bluetooth device</td>
<td>HC-05 module</td>
<td>Authentication and control</td>
</tr>
<tr>
<td>Alarm sensor</td>
<td>HC-SR04 ultrasonic distance sensor</td>
<td>Intruder detection</td>
</tr>
<tr>
<td>Buzzer</td>
<td>Active 5v digital</td>
<td>Alarming</td>
</tr>
</tbody>
</table>

b) Design of the mechanism

The proposed mechanism is controlled by a SG-90 model servo-motor. The most suitable type of mechanism is the slider-crank mechanism. The functional part of the lock is designed to be of a cylinder type. The whole mechanism is assembled in a box that can be mounted on or inserted into the access point. The internal view of the assembly is shown in Figure 3 and the length and legend of the mechanical components is given in Table 2.
Within Figure 6 the relative change of position of the cylinder slider shown on the y-axis is approximately 21 mm \((p \approx 21\, \text{mm})\). The total time for which the simulation takes place is shown on the x-axis and it is 0.075 s. These results have been achieved for a change of angular position of the motor shaft of 45° \((\alpha = 45\, ^\circ)\).

4. ANALYSIS OF THE SYSTEM

a) Kinematic analysis

The kinematic analysis is performed to verify the reliability of the proposed model. Figure 4 shows the kinematic diagram of the proposed model.

A Simulink model is built using the schematic diagram of a crank mechanism with one degree of freedom. Kinematic analysis of the mechanism is performed using Simulink and the obtained results are shown in Figure 5 which shows the position change of the locking cylinder with one degree of movement freedom.

b) Dynamic analysis

After the combination of design and kinematic analysis, a dynamic analysis is essential to check the stress strength of the mechanism. Consider a case when an intruder is trying to open the door by force. To check if this is possible, FEA (finite element analysis) using the SolidWorks Simulation module is performed. The break-in force is an input to the analysis, while the highest stress value is an output and a result of the simulation. The input force is obtained according to the fastest recorded acceleration generated by a human being \([9, 10]\). The obtained result is:

\[ a \approx 10\, \text{m/s}^2. \]  

(1)

This would be a theoretical case because a person cannot achieve this acceleration when hitting a door with the whole body. A person with a mass equal to 100 kg would generate a force of:

\[ F = ma = 1000\, \text{N}. \]  

(2)

The results from the analysis are shown in Figure 6. From the analysis, the highest stress value using the Von Mises principle for calculation is 154 MPa. The stressed part would be designed of a low-carbon structural steel (S185). The value of the maximum stress allowed for the used material for the mechanism is 185 MPa.

The safety factor can be calculated as a proportion of the maximum stress value allowed and the highest stress value of the analysis. For this analysis, it has a value of:
Design and implementation of an automated safety lock system with multiple authentications and alarm protection

\[ S = \frac{\sigma_{\text{max}}}{\sigma_{\text{obj}}} \approx 1.2. \] (3)

Since \( S > 1 \), the mechanism can withstand the projected impact force, hence the dynamic analysis is successful and completed.

5. EXPERIMENTAL RESULTS AND DISCUSSION

The experimental results are defined by 4 cases:
1. Correct keypad password.
2. Incorrect keypad password.
3. Wireless unlocking and alarm commands.
4. Illegal break-in.

Figure 7 shows the experimental setup of the designed safety lock system. The mechanism is locked by default, and the red diode is turned on.

In the first case, the user enters the password from the keypad. When the password is confirmed, the mechanism unlocks, while the green light turns on. The user can enter the access point, and then simply press the button from the inside to lock the mechanism.

For the second case, if the password is incorrect, the red-light blinks and the buzzer beeps three times as a warning. The password automatically resets.

The third case is represented by pressing the commands on the phone app. Previously, a connection must be established via Bluetooth, which also requires a password. The mechanism is controlled by pressing the commands “OPEN” and “CLOSE”. There are also commands for the alarm control.

In the fourth case, the experiment included a purposeful unauthorized break-in. When the sensor detects intrusion, the response is automatically triggered. The alarm can be turned off in two ways: By inputting the correct password through the keypad, or by pressing the command “AL OFF” on the interface of the phone application, as can be seen in Figure 8.

In Figure 8, the display of the interface of the application is shown with multiple experiments and their corresponding messages.
6. CONCLUSION

In this paper, an automated safety lock system with multiple authentications and alarm protection has been designed. Its purpose is to improve the usability and security of an everyday repetitive manual task. The techniques used for its design are standard and cost-effective, so it can easily be commercialized.

The proposed system has all the features that the established solutions on the market do. The combination of the lock with the alarm is considered a great advantage since most of the existing solutions come independently of each other. Its downside is the inability to check whether someone has tried to hack the password. To improve it, a server that can save the messages from the module has to be added. The server would also have to be able to resend the messages to the host. Future efforts can improve safety while keeping the effectiveness and usability.

REFERENCES