Mechanical Engineering – Scientific Journal, Vol. **41,** No. 1, pp. 23–28 (2023)
Number of article: 660
In print: ISSN 1857–5293
Received: Novembet 16, 2022
On line: ISSN 1857–9191
Accepted: December 26, 2022
UDC: 683.336.5:681.518.52]:004.896.056.523
https://doi.org/10.55302/MESJ23411660023p

Original scientific paper

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

Slavčo Premčeski[1], Dame Korunoski[2], Anastasija Ignjatovska[2], Damjan Pecioski[2]

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

A b s t r a c t: 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 can be upgraded with programmable components so that it can be controlled by electrical power. This kind of 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

ДИЗАЈН И ИМПЛЕМЕНТАЦИЈА НА АВТОМАТИЗИРАН БЕЗБЕДНОСЕН СИСТЕМ ЗА ЗАКЛУЧУВАЊЕ СО ПОВЕЌЕ АВТЕНТИКАЦИИ И ЗАШТИТЕН АЛАРМ

А п с т р а к т: Како резултат на постојаниот технолошки развиток, повторливите мануелни активности можат да се извршуваат со помош на автоматизирани системи кои имаат за цел да ги совладаат потребите и предизвиците на модерниот свет. Системот на обична брава може да се надгради со програмабилни компоненти и на тој начин таа да може да се управува со помош на електрична енергија. Ваквата брава исто така би била пофлексибилна во случај на повеќе корисници на некој објект. Во овој труд се предлага дизајн на автоматизирана брава кој комбинира електронски компоненти и механички систем за заклучување управуван од Ардуинов контролер. Се состои од три главни потсистеми: автентикациски систем, излезен систем (механизам за заклучување) и систем за аларм. Предложената проверка може да биде изведена со физички внес на лозинка на тастатура или преку комуникацијата „bluetooth" со мобилна апликација. Алармниот систем овозможува додатна безбедност од пристап на неовластени лица. Механизмот за заклучување е управуван од сервомотор и може да се примени на различни видови пристапни точки, на пример врати, фиоки, сефови итн.

Клучни зборови: автоматизација; безбедносно заклучување; аларм; дизајн; Ардуинов контролер

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. Thoung 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.

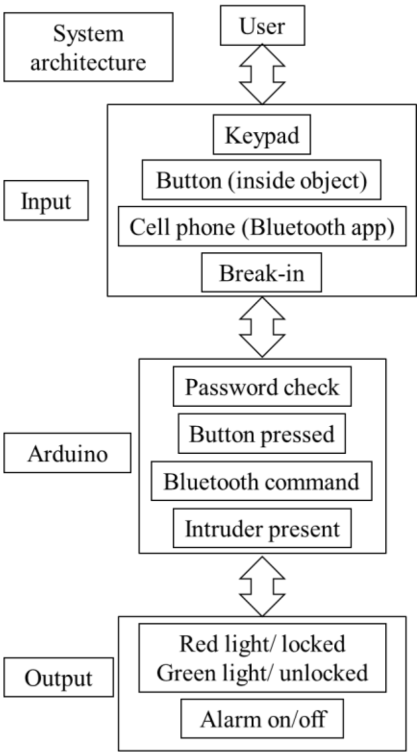

Fig. 1. Integrated architecture of the proposed system

The alarm subsystem works only when the access point is locked. Alarm sensing would be placed on every possible place that could be a subject of a violent and unauthorized break-in. The sensing is performed with a thin ultrasound layer from the top to the bottom of the access point, constantly measuring the distance. If an intruder were to pass, the detected distance would change. Then, a sound reaction would automatically be triggered. The alarm subsystem can be turned off by a command on the application or by typing the correct password on the keypad. The proposed architecture also includes another capability (button) found on the inside of the access point. This button allows (un)locking of the access point and could only be performed from the inside of the object.

Figure 2 shows a block diagram of the Bluetooth communication part of the authentication subsystem. As long as the connection is established, each command performs an adequate operation.

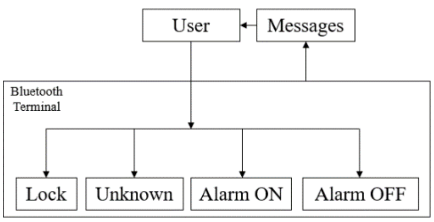

Fig. 2. Architecture of the subsystem for wireless communication

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

Electrical components and their features

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

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.

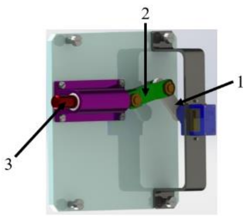

Fig. 3. Internal view of the designed mechanism

Table 2

Mechanical components and their length

Component	Length (mm)	Legend
Crank	26	1
Connecting rod	36	2
Slider	75	3

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.

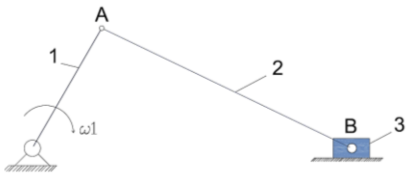

Fig. 4. Schematic diagram of the mechanism

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.

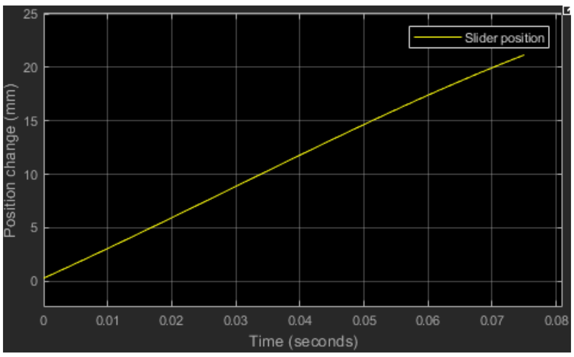

Fig. 5. Change of position of the slider

Within Figure 6 the relative change of position of the cylinder slider shown on the *y*-axis is approximately 21 mm ($p \approx 21$ 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° ($\alpha = 45^\circ$).

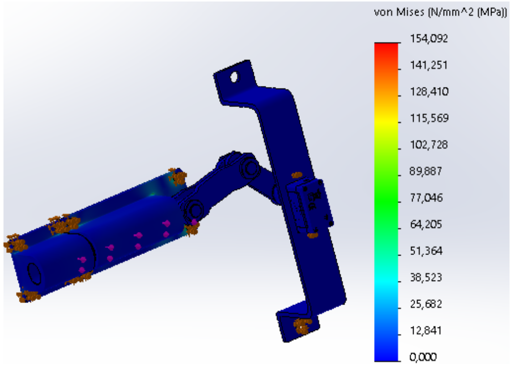

Fig. 6. FEA analysis results

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:

$$a \approx 10\ \frac{\mathrm{m}}{\mathrm{s}^2}\,. \tag{1}$$

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:

$$F = ma = 1000\ \mathrm{N}\,. \tag{2}$$

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:

$$S = \frac{\sigma max}{\sigma ob} \approx 1.2\,. \quad (3)$$

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.

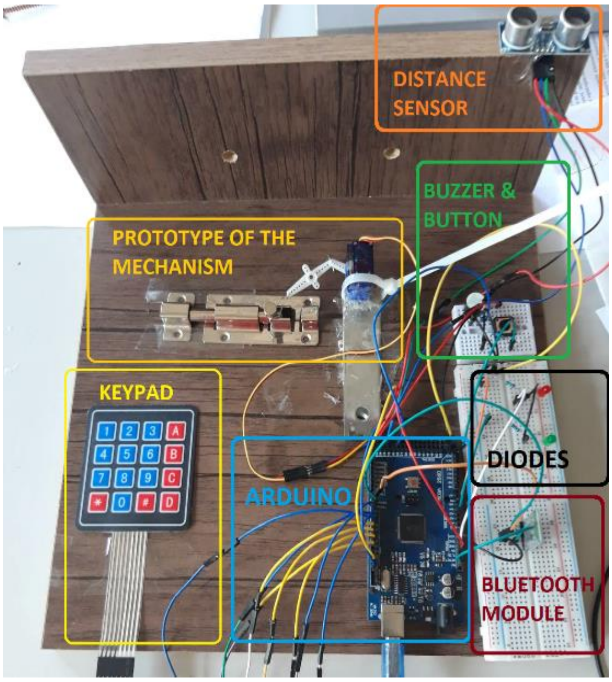

Fig. 7. Experimental model of the safety lock system

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.

Fig. 8. Display of the smartphone application interface over bluetooth connection

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 passwords. 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.

REFFERENCES

[1] Yugashini, I.; Vidhyasri, S.; Devi. K. G. (2013): Design and implementation of automated door accessing system with face recognition, *International Journal of Science and Modern Engineering* (IJISME), **1** (12), 10–13.

[2] Doh O.; Ha, I. (2015): A digital door lock system for the Internet of Things with improved security and usability, *Advanced Science and Technology Letters* Vol. **109**, pp. 33–38. http://dx.doi.org/10.14257/astl.2015.109.08

[3] Bhushan, P.; Vishal, M; Sagar, S.; Mayur, P.; Patole, U. R. (2918): Automatic door lock system using PIN on android phone, *International Research Journal of Engineering and Technology* (IRJET) Vol. **05**, Issue 11, pp 1007–1011. e-ISSN: 2395-0056.

[4] Goswami, S.; Choudhury, A.; Das, S.; Banerjee, T.; Ghosh, S. (2017): Automated password protected door lock system, *Advances in Industrial Engineering and Management*, Vol. **6**, No. 1, 48–52.

[5] Thoung, T. H.; Dr. Zin Ma Ma Myo (2019): Implementation of automatic door opening system with entry counter for university library, *International Journal of Trend in Scientific Research and Development* (IJTSRD), Vol. **3,** Issue 5, pp.1267–1269.

[6] Adiono, T.; Fuada, S.; Feranti Anindya, S.; Purwanda, I. G.; Fathany, M. Y. (2019): IoT-enabled door lock system, *International Journal of Advanced Computer Science and Applications* (IJACSA), Vol. **10**, No. 5. DOI: 10.14569/IJACSA.2019.0100556

[7] Lee H.-S.; Hsieh, L.-C. (2009): Innovative design of an automatic car-door opening system, *Proceedings of the IMECS 2009*, Vol. **II.** IMECS 2009, March 18–20, Hong Kong.

[8] Downs, S.; Pollo, A.; Bredemeier, E. (2018): Residential automatic door opener. Mechanical Engineering Design Project Class. 94.

[9] Allain, Rhett (2012): *Maximum Acceleration in the 100 m Dash*. WIRED SCIENCE, Aug. 31.

[10] Lee, J. (2008): *Usain Bolt 100 m 10-meter Splits and Speed Endurance*.