1. Přemysl JANŮ[1], 2. Petr BÍLÝ[2]

University of Defence (1), University of Defence (2)
ORCID: 1.0000-0002-5837-9557; 2.0009-0004-3196-1645

doi:10.15199/48.2024.04.26

An access system for small family buildings

Abstract. *The article is devoted to the complete design of an access device for small objects, which is integrated into an electronic security system. Fully functional device is implemented in a family recreation facility, which is situated in the cottage area. The article analyses the object and determines a basic project threat. Based on this analysis, the mentioned system is thoroughly designed. The designed and assembled system is completely installed in the building and its correct functionality is verified*

Streszczenie. *Artykuł poświęcony jest kompletnemu projektowi urządzenia dostępu do małych przedmiotów, które jest zintegrowane z elektronicznym systemem bezpieczeństwa. W pełni funkcjonalne urządzenie zaimplementowane jest w obiekcie wypoczynku rodzinnego, który znajduje się na terenie domku. W artykule dokonano analizy obiektu i określono podstawowe zagrożenie projektowe. Na podstawie tej analizy wspomniany system jest szczegółowo projektowany. Zaprojektowany i zmontowany system jest całkowicie instalowany w budynku i sprawdzana jest jego poprawność działania. (**System dostępu do małych budynków rodzinnych)***

Keywords: access system, electronic security system, basic project threat, microprocessor system.
Słowa kluczowe: system dostępu, elektroniczny system zabezpieczeń, podstawowe zagrożenie projektu, system mikroprocesorowy.

Introduction

Access systems have been used for a relatively long time, mainly in commercial area and state institutions, where they help to prevent the entry of unauthorized persons, they help to separate areas requiring security or classified areas from each other. They also ensure the registration of persons who have entered into a building or certain area within it and also enable the recording of persons who have attempted to enter into the area without authorization. Access systems are particularly important in areas where increased security is needed for access by people, for example nuclear power plants.

In general, access systems consist of one or more access points. The access point ensures an identification of a person. The identification element can be entering a password, a numeric code using a keyboard, reading an identification token, such as a magnetic card, a barcode card, a chip card using a reader, or some of a biometric information, such as a fingerprint using a sensor, or their combination to increase the security of an area. Authentication is then performed in a main control unit, which contains a database of persons authorized to enter. Thus, the information read from the sensor or the entered data is compared with the values in the database. If this information matches an item in the database, authorization is done and the person is granted to access. Otherwise, the person is rejected. In the case of autonomous access systems, this is performed directly at the access point, otherwise the identification data can be provided remotely to a central control and service workplace, where authentication and authorization is carried out. This provision of identification information can be done using some serial bus, usually RS 485 or Ethernet. Another possibility is use of a wireless technology, for example radio transmission at a certain frequency, WiFi standard or GSM network. The access point also contains an actuator that ensures the entry of authorized person into the area. Actuators can include, for example, an electromagnetic door opener, a turnstile, a barrier and an electric motor for opening a door or gate. The last and very important device is a power system, which must be backed up. These systems are usually integrated with attendance systems, electronic security systems, electronic fire systems and camera systems [1-4].

Certain demands are placed on these systems, which depend on the influence of the environment and electromagnetic effect, when so-called environmental class is determined [1-4]. Furthermore, the so-called access levels of the system are determined, when it is specified who can intervene into the given system [1-4]. This will increase the security of the area. The economic demands also depends on the complexity of the system and these requirements.

At the beginning of implementation of access systems, the technologies used were not yet at such a high level, they were less available and expensive, and therefore the whole system was relatively economically demanding. Therefore, these systems were implemented only into the objects that required the highest level of security. With the development of sensor technology, microprocessor systems, digital signal processing and the possibility of effective long-distance transmission of information, the individual components of access systems have become more affordable and therefore not so economically demanding. For this reason, it is possible to install these systems even in less important objects from the point of view of critical infrastructure. Today, they are relatively easily available even to natural persons. This article is dedicated to the design of such an access system and is the result of a diploma thesis.

The access system, which is described in detail in this article, was designed for a recreational facility (cottage). For security reasons, the exact location of the object is not mentioned. The cottage is located at the foot of a gently rising hill and is surrounded on three sides by neighbouring buildings, between which there is no perimeter protection in the form of a fence. It is located on the perimeter of the entire cottage colony. The fourth side of the plot is formed by a mesh fence, behind which there is an unpaved access road along the entire width of the plot along a third-class road. The location situation of the object is illustrated in Fig. 1, which is a photo provided by an amateur drone. Fig. 2 shows the location of the object in the cottage area using an aerial map. Regarding the layout of the building, it is the cottage with three floors. The lowest floor is only a cellar for storing tools and harvest from a garden and has a separate entrance. The other two floors are accessible via stairs and have only one main entrance. As for other fillings of the building openings, in addition to the entrance door, on the first floor there is a door to the balcony and windows along the entire length of the wall, and in the attic, a pair of windows are located on two opposite walls of the gable of the building. The access system is designed and subsequently installed precisely for the two highest floors to

the entrance hall, and therefore only the first floor of the building is taken into account. For a better imagination, the layout of the object for the installation of the proposed access system is shown in Fig. 3.

Fig. 1. Location of the object – unmanned vehicle

When designing a system of this nature, it is necessary to take into account all possible risks that may have a negative effect on the protected interest. First of all, it is necessary to find out the protected assets and the operating conditions of the object. In this case, an end user installs the system in order to increase the level of security and prevent access to the protected object by unauthorized persons, rather due to the violation of privacy. The object contains only equipment of the cottage. Only TV and coffee machine can be considered as the most valuable. No valuables, cash, jewellery, paintings or other valuable works are stored in the building. The building is visited only by the owner and his family, and only on weekends, so the building is without supervision and security for almost whole week, therefore it requires the installation of an access system connected to an electronic security system with remote signalling of the entrance to the building. If it is necessary to process the design of an access system connected to an electronic security system, first it is necessary to identify and then evaluate real threats for the appropriate level of security. It is given that the threat must be relevant in the certain place and time, and also that the threat exists only when its bearer exists, as the case may be if there is no person who is capable or not interested in implementing the threat, the threat cannot be taken as real. Theft and burglary, robbery, intentional damage of assets and vandalism can be considered threats that actually threaten the selected object at a given place and time. As a bearer of the threat, it is possible to designate an ordinary criminal without special equipment, a small criminal group, and an enraged or envious resident or neighbour in the cottage colony. This is a list of threat actors with external position. As this is a recreational facility that is visited only by a close family circle, it is not relevant to consider the bearer of the threat with an inside position.

The more detailed description of the relevant threat actors is presented in [5]. The next step is to determine the probability of the threat being realized. This can be discovered, for example, based on historical data. When using crime maps in the given area in the period from 1st January 2010 to 31st March 2023, a total of 16 crimes were detected, of which seven were not clarified. In six, a probable perpetrator was identified and three were not recognized as a crime, but a misdemeanour. The more detailed characteristic and description of crimes are given in [5]. During determining the probability of the threat being realized, it is necessary to specify whether the bearer of the threat exists, has the ability to carry out the threat, and whether the threat has been implemented in the past. Furthermore, in combination with historical data, it is necessary to determine the probability of the realization of the threat.

Fig. 2. Location of the object – aerial map

It was analysed that the probability of threat realization was for theft and burglary high, for robbery low and for intentional assets damage low.

Fig. 3. Layout of the object

The next step in designing the right access system connected to an electronic security system is to determine the severity of the consequences. This is very important to determine the level of risk and specify the basic project threat, according to which the entire system is designed and must adapt to it. The severity of the consequences can be described verbally by creating a scale of the severity of the consequences, for example from a minor consequence to a catastrophic consequence, and adding a verbal description of the consequence to each level. For the above-mentioned object, it is possible to determine the severity of the consequences in the following way. Non-serious consequence – realization of a threat that could lead to damage or theft of property with a damage of 3,000 CZK. Marginal consequence – realization of a threat that could lead to damage or theft of property with a damage of 8,000 CZK. Serious consequence - realization of a threat that could lead to damage or theft of property with a damage of 15,000 CZK. Critical consequence – realization of a threat that could lead to damage or theft of property with a damage of 25,000 CZK and personal injury. Catastrophic consequence – realization of a threat that

could lead to damage or theft of property with a damage of 50,000 CZK and to the death of persons.

Based on this analysis, the level of risk and the basic project threat were defined. The owner of the building requires an autonomous access system connected to an electronic security system that can withstand the threat that can occur with the highest probability, which, according to the historical data and processing of the analysis of the realization of the threat probability, is burglary. The basic project threat is then represented by Table. 1.

Table 1. The basic project threat

Threat bearer	An ordinary criminal without special equipment
Intent of attack	Theft of property
Motivation	Economic
Abilities	-
Number of persons	1
Armament	Cold weapon
Tools	Mechanical hand tools, accumulator tools
Transport	Motor vehicle
Knowledge	Very limited
Financial resources	Low
Supporting infrastructure	Very limited
Cooperation with insider	No
Willingness to kill/die	No/No

Design and implementation of the access system

Based on the previous analysis and determination of the basic project threat, an access system to the presented object was designed. The proposed system should meet all the requirements listed in the previous chapter. Thus, the proposed access system is intended for a small object for use in indoor spaces with a temperature ranging from +5 °C to 40 °C and a relative humidity of 75% without condensation, which corresponds to environmental class number 1. In the viewpoint of access levels, only person with successful authorization has a permission to enter into the system, which corresponds to system access level number 2. The block diagram of the designed and implemented access system is shown in Fig. 4.

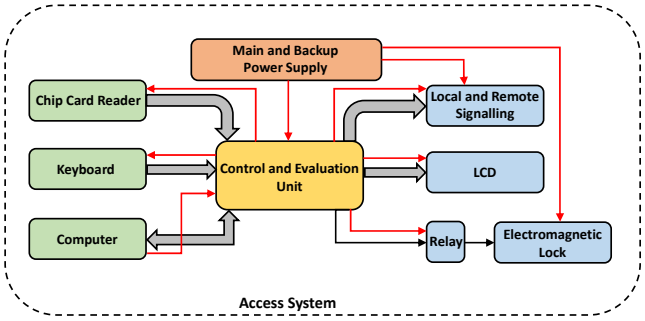

Fig. 4. The block of the designed access system

The core of the designed access system is the Control and evaluation unit. For this purpose, the Arduino Mega 2560 module [6] was chosen, which is equipped with a single-chip microprocessor ATmega2560 [7]. This module ensures the acquisition of data from the chip card or other token reader and the keyboard, performs a comparison with the user database, evaluates the situation and then allows or denies access and ensures the necessary signalling. This unit also supplies power to some system components. It allows voltages of 3.3 and 5 V. A module with circuit MFRC522 [8] integrated and an antenna was implemented as a chip card or other token reader. This device uses a radio frequency signal with a frequency of 13.56 MHz to communicate with the identification element and communicates with the Control and evaluation unit via the SPI serial bus.

It also allows communication via the I2C and UART bus. The power supply of this device is provided via the Control and evaluation unit. The value of the supply voltage is 3.3 V. A 4x4 matrix keyboard [9] is used as another identification device. This keyboard therefore consists of 16 buttons labelled 1 – 9, A B C D and two special characters *, #. These buttons can be freely configured.

For programming the Control and evaluation unit and also for its configuration, it is possible to use primarily a laptop with an installed development environment for programming the aforementioned microprocessor system. An electromagnetic lock [10] was used as an actuator that ensures entry into the building. This lock works with supply voltage of 12 V, therefore it is necessary to control it using the microprocessor system through a relay. An active piezoelectric buzzer [11], red and green LEDs were used for local signalling of the system status. An active piezoelectric buzzer signals by tone with frequency of 2400 Hz and for time of 1 s when a person is correctly authorized and door is unlocked. Incorrect authorization is signalled by a tone with a frequency of 500 Hz for 1 s. The red LED is activated when the door is locked and green LED when authorization is successful. The active piezoelectric buzzer and LEDs are controlled directly from the microprocessor system of the Control and evaluation unit.

LCD 1602 [12] with green backlight was used for direct display of status messages of the access system. This LCD allows two lines of sixteen characters to be displayed. To save the data pins of the microprocessor system, the LCD was also equipped with a converter that enables communication via the I2C serial bus. The LCD is powered directly from the microprocessor system. Remote signalling is solved by GPRS GSM module labelled SIM800L [13]. This device is able to make a phone call, send or receive SMS via connected microSIM. In the configuration of this system, it is intended only for sending short SMS. It communicates with the microprocessor system using UART. The supply voltage is recommended in the range of 3.7 - 4.2 V. Since it draws up to 2 A during initialization, it needs to be powered from an external DC source. A module with a microprocessor system does not allow such a high current.

The last and very important part of the designed access device is the power supply system. Since the proposed access system requires several different power supply voltages, it was necessary to design an appropriate source that can cover the supply of elements both 12 V and 5 V. The access system is also equipped with a backup source in the form of a lead-acid battery that needs to be charged with voltage of 13.8 V. All this is provided by the Main and backup power supply block. It is therefore necessary that it covers the power supply of the Control and evaluation unit and the components connected to it with a voltage of 5 V, the electromagnetic lock with a voltage of 12 V and the charging of the lead-acid battery with voltage of 13.8 V. For this reason, it was necessary to design a so-called multi-way power supply. The requirements for the main power supply were met by 65 W switched-mode power supply with output voltage of 18.5 V and maximum output current of 3.5 A. From this main power supply, the power for the microprocessor system, the GPRS GSM module, the electromagnetic lock and the charging of the backup battery are provided by adjustable DC/DC step-down converters [14], which make it possible to set the output voltage in the range of 1.25 – 32 V and provide an output current of up to 5 A. With these converters, the desired voltages of 5, 12

and 13.8 V is possible to be set. In the case of a distribution network power failure, it is necessary to keep the system in working order at all times, so it was important to include a backup source in the power system of the entire device. A Westinghouse WA12120 [15] lead-acid battery with a nominal voltage of 12 V was chosen for the designed access system. Due to its high level of quality and reliability, it is very suitable for this use. To increase the life of the battery, it was necessary to add a smart module for charging the battery marked XH-M604 [16] to the system, which ensures that the battery is not overcharged or undercharged. The battery charging module is equipped with a voltmeter that measures the voltage value of the connected battery. It controls the charging of the battery according to closing and opening voltage, which can be set using micro-switches on the module board. Connection of the module is very simple. The output voltage of 13.8 V from the DC/DC step/down converter is connected to the input and the lead-acid battery clamps marked BAT + and – is connected to the output. In order to ensure the power supply switch to the backup source in a case of a power failure, it was necessary to use an automatic power switch. In the designed system, the module marked YX850 [17] was implemented, which, in the case of a power failure, switches from the terminal for the main source to the terminal with the connected backup source using a built-in relay. During operation on the main power supply, the terminals for the battery fulfil the function of the output and thus the backup battery is being recharged via the smart charging module. The block diagram of the complete power supply system is represented by Fig. 5.

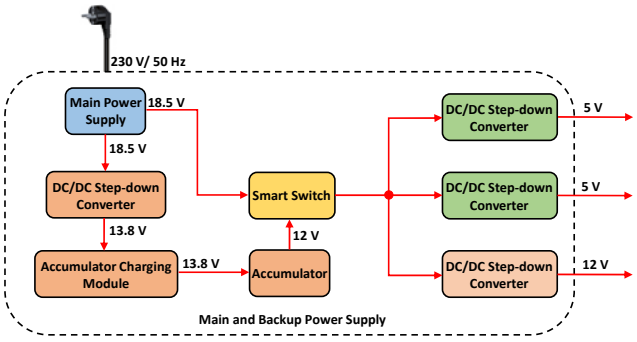

Fig. 5. Block diagram of the power supply system

Furthermore, it was necessary to integrate the designed access system with an electronic security system. The block diagram of the entire system is shown in Fig. 6.

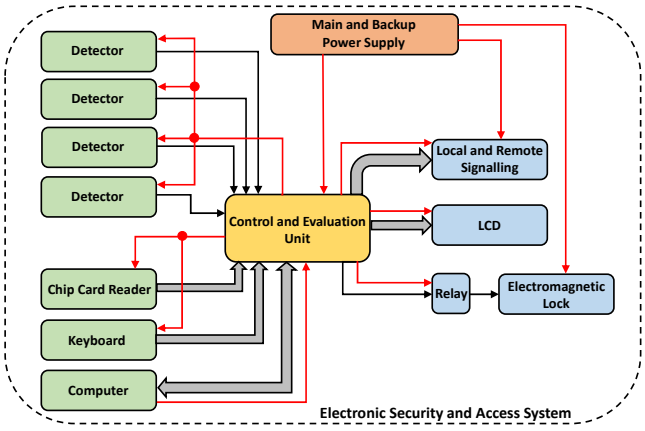

Fig. 6. Access system integrated into the electronic security system

The device was therefore combined with the detection part. It allows connection of four individual detectors or groups of detectors. The detectors are connected analogically to the Control and evaluation unit using a double-balanced loop for the maximum degree of security, thus to detect the highest number of states that can occur in the loop. The device is therefore able to evaluate the states: rest, alarm, sabotage by opening the detector cover, sabotage by cutting the detector's supply cable and sabotage by a short circuit at the input of the Control and evaluation unit. Various types can be imagined as detectors for casing protection systems, for example magnetic contacts, infrared barriers, microwave barriers and shock detectors. This can also include sensors for spatial protection, for example PIR and microwave sensors. The method of connecting of individual detectors to the Control and evaluation unit is determined by the diagram in Fig. 7.

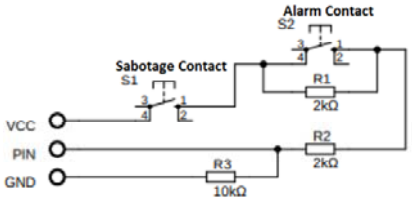

Fig. 7. Connection scheme of a detector to the Control and evaluation unit

The connection diagram of a detector to the Control and evaluation unit contains the detector's alarm contact, the detector's tamper contact, two balancing resistors with the value of 2 kΩ and one so-called pull-up resistor with the value of 10 kΩ. Terminals VCC and GND are power supply inputs, and the PIN clamp is used to connect to the input of the analogue-to-digital converter of the microprocessor system. The individual states are characterized by a certain resistance of the loop, which is proportional to the respective voltage and this is just measured using an analogue-to-digital converter. The power supply from the microprocessor system is used here, namely 5 V. When both contacts are closed, the state is rest. When the alarm contact is opened, alarm is indicated, thus this is the presence of an intruder. When the tamper contact is opened, removal of the detector cover is indicated, and in case of cutting the supply cable or a short circuit on the input terminals of the microprocessor system, sabotage is indicated.

Complete signalling consists of three parts. The first two, light signalling of the entrance to the building and acoustic signalling using a piezoelectric buzzer, are used by both the access system and the electronic security system. The light part realized by two LEDs signals the security status of the object. If the red LED is set, the system is armed, the detection part is in an active state and sends signals through the input circuits to the Control and evaluation unit. If the green LED is set, the system is disarmed, the detection part is out of order and does not detect status changes. The same is applied to the acoustic part, if the object is disarmed, the piezoelectric buzzer is out of operation and if the object is armed by placing an identification element on the reader, entering a numerical code and pressing the arming button, the piezoelectric buzzer is in an active mode and emits a sound of the appropriate frequency in the case of alarms. The third part of the signalling consists of four branches for four detection loops with four LEDs, when each of them is assigned to one of the states. As already mentioned, the double-balanced detection loop can detect four states, therefore a

corresponding colour is selected for each state, when green corresponding to the rest state, yellow to sabotage, red to alarm and blue to input short state. Another part of the signalling can also be considered the signalling using the LCD, on which the word disarmed is displayed during the disarming period, and when the object is armed, the individual detection loops and their state are depicted, for example, loop 1 is in an alarm state. This signalling is implemented using the same LCD that is used for the access system. It is also possible to send information about the individual states and behaviour of the system via short SMS by the GPRS GSM module.

The access system connected to the electronic security system is located in the building mentioned in the introduction chapter of this article. At the access point, there is the reader for cards or other tokens and the keyboard for entering an access code, which unlocks the door using the electromagnetic lock and unarms or arms the object. Inside the guarded building there are the Control and evaluation unit, local and remote signalling devices and a detection part. For a better imagination, the floor plan of the guarded building with distributed elements was created, which is shown in Fig. 8.

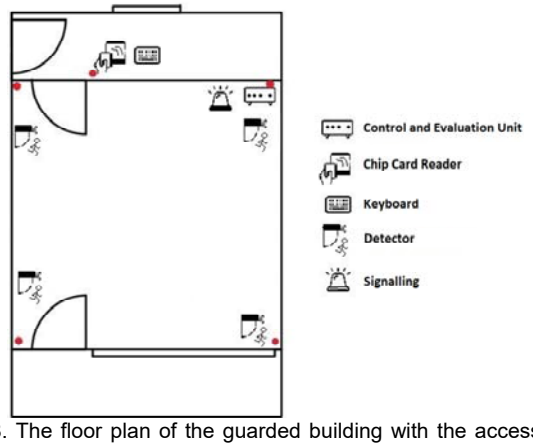

Fig. 8. The floor plan of the guarded building with the access and electronic security system

Algorithm at the microprocessor system

After assembling the complete system, the microprocessor of the Control and evaluation unit was programmed.

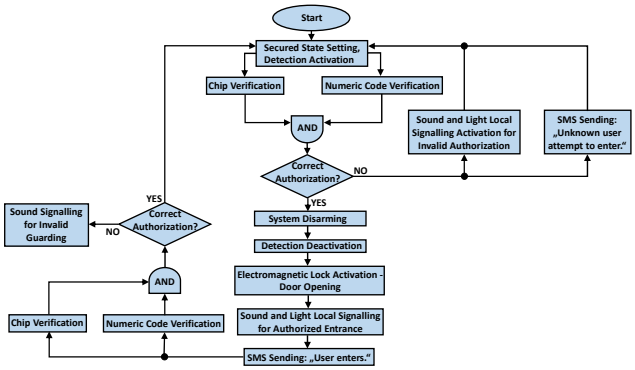

Fig. 9. Flowchart of the function of the access and electronic security system

The algorithm in the microprocessor system consists of three main parts, which is controlled by. In the first part, libraries are inserted, variables are defined and characterized, and various functions are set. In this program code, this part was used to insert all necessary libraries for the proper function of the system elements, and the phone numbers to which a text message is sent were also defined. The message options that can be sent have been set. The individual pins of elements were also specified, the layout of the keyboard was further characterized, a database of identification cards and users was created and an access code was set. In the second part, commands that are required to occur only once when the algorithm is run are inserted. The last part contains commands that are repeated over and over again. This includes checking of incoming signals from the input circuits until the condition for disarming the object changes. This condition stops everything, and until system is armed, the program continues. The detailed process, especially of the part that is constantly repeated, is represented by the flowchart in Fig. 9. The algorithm was developed and the microprocessor programmed in the Arduino IDE development environment, which uses the C programming language for microcontrollers.

Verification of the correct functionality of the entire system

When verifying the function of individual parts, both the hardware part and wiring, and the parts of the program that control these elements, it was necessary to power them. Since the individual elements are powered by different voltage values, it was essential to have the power supply system made first.

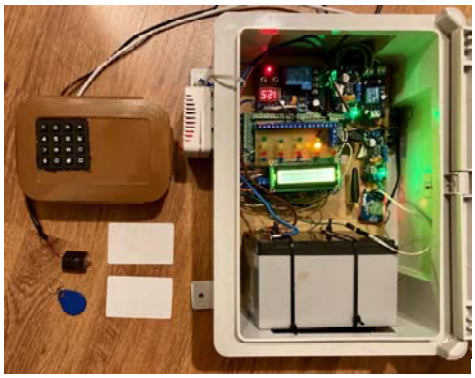

Fig. 10. Real appearance of the designed and tested system

It was necessary to test the functionality of each part stepwise, in order to avoid a situation where the system is made, it is non-functional and it is not possible to determine in a short time exactly, which part has a failure. This was the procedure for verifying the functionality of the access system. To verify the correct operation of the access system, the device was started. Initially, it was armed, which means, that the electromagnetic lock ensured that the door was closed and the detectors were activated. Subsequently, various identification cards were attached and an access code was entered. The system opened the electromagnetic lock and sent a text message about who entered into the object and disarmed the object only when known identification card was attached and the correct numeric code was entered. Otherwise, the system acoustically and visually signalled incorrect authorization of the user and sent a text message to the selected phone number that an unknown user tried to enter into the object. In this case, the system also remained completely armed. The real appearance of the entire system is shown in Fig. 10. To provide visual documentation, the access system was uninstalled and the individual components were arranged in close proximity to each other.

Conclusion

This paper presented a functional access system that was also integrated into an electronic security system. This system is designed to secure the entry of authorized persons into a small building. In this case, it is a small family holiday object in a cottage area.

In the article, an analysis of the area was carried out and the basic project threat was compiled. Based on this basic project threat, the entire system was designed. A chip card and entry of a numerical code was used as an identification element. A piezoelectric buzzer, LED and LCD were used to signal the status of the system and the secured object. A GPRS GSM module was applied for remote signalling of the system status. An electromagnetic lock was implemented to lock and unlock the object.

During the design of the entire device, it was necessary to pay attention to the thorough design of the power supply system, since it is the most important part. It ensures the reliable operation of the system. The device works with three supply voltage values. So it was essential to design a three-way power source that covers this and is also able to charge the backup battery.

Thanks to the integration into the electronic security system, the device also allows the connection of four groups of space intrusion detectors for the highest level of security.

To configure the entire system, it is necessary to use an external computer and reprogram the microprocessor system of the Control and evaluation unit. For the future improvement of this device, it would be possible to use data communication via the GPRS GSM module and display the status of the device and the object using a mobile application, or configure the entire system.

The work presented in this article was supported by the Czech Republic Ministry of Defence – University of Defence Development Program – "Conduction of Operations in Airspace".

***Authors**: Ing. Přemysl Janů, Ph.D., University of Defence, Faculty of Military Technology, Department of Aviation Technology, Kounicova 65, 662 10, Brno, E-mail: premysl.janu@unob.cz; Ing. Petr Bílý, University of Defence, Faculty of Military Technology, Department of Combat and Special Vehicles, Kounicova 65, 662 10, Brno, E-mail: pbily1998@gmail.com.*

REFERENCES

[1] M. L. Garcia, *The Design and Evaluation of Physical Protection systems*, 2nd ed. Burlington: Butterworth-Heinemann, 2008

[2] M. L. Garcia, *Vulnerability Assessment of Physical Protection Systems*, Burlington: Butterworth-Heinemann, 2006

[3] Jakubowski K., Paś J., Określenie parametrów eksploatacyjnych wybranych elektronicznych systemów bezpieczeństwa na podstawie procesu ich użytkowania w obiektach infrastruktury krytycznej, Przegląd Elektrotechniczny, 97 (2021), nr 10, 103-109

[4] Hatano T, Kani J., Maeda Y, Standardization and Technology Trends in Optical, Wireless and Virtualized Access Systems, IEICE Transactions on Communications, E102B (2019), nr 7, 1263-1269

[5] Mapa kriminality. *Kriminalita, policie cz* [online]. Praha: Policie České republiky, 2023 [cit. 2023-08-17]. Available from: https://kriminalita.policie.cz/

[6] Arduino Mega 2560 Rev3. *Arduino.cc* [online]. Arduino.cc, 2021 [cit. 2023-08-17]. Available from: https://store.arduino.cc/products/arduino-mega-2560-rev3?queryID=undefined

[7] Atmel ATmega640/V-1280/V-1281/V-2560/V-2561/V: 8-bit Atmel Microcontroller with 16/32/64KB In-System Programmable Flash. *Atmel* [online]. San Jose, USA: Atmel Corporation, 2014 [cit. 2023-08-17]. Available from: https://ww1.microchip.com/downloads/en/devicedoc/atmel-2549-8-bit-avr-microcontroller-atmega640-1280-1281-2560-2561_datasheet.pdf

[8] MFRC522. *NXP Semiconductors* [online]. Phoenix, Arizona, USA: NXP semiconductors, 2016 [cit. 2023-08-17]. Available from: https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf

[9] 4x4 matrix keyboard. *TIPA.EU* [online]. Opava, Czech Republic: TIPA.EU, 2023 [cit. 2023-08-17]. Available from: https://www.tipa.eu/en/4x4-matrix-keyboard/d-250903/

[10] Elektromagnetický zámek 12 VDC. *Dratek.cz* [online]. Havlíčkův Brod, Czech Republic: Dratek.cz, 2019 [cit. 2023-08-17]. Available from: https://dratek.cz/docs/produkty/1/1111/1579673300.pdf

[11] Piezo Buzzer. *Kailiec* [online]. Changzhou: Kailiec, 2017 [cit. 2023-08-17]. Available from: https://www.micro-buzzer.com/product/Piezo-Buzzer-HP1470X.html

[12] Liquid Crystal Displays (LCD) with Arduino. *Arduino.cc* [online]. Arduino.cc, 2023 [cit. 2023-08-17]. Available from: https://docs.arduino.cc/learn/electronics/lcd-displays

[13] Bezdrátový modul GSM GPRS SIM800L v2.0. *Dratek.cz* [online]. Havlíčkův Brod, Czech Republic: Dratek.cz, 2023 [cit. 2023-08-17]. Available from: https://dratek.cz/arduino/7569-bezdratovy-gsm-gprs-modul-sim800l-v2.0.html?gclid=EAIaIQobChMIv6qEiJrjgAMVkdF3Ch1v5w5cEAQYASABEgIKffD_BwE

[14] Modul DC/DC měnič step-down 1,25-32V/5A. *GME electronic* [online]. Prague, Czech Republic: GME electronic, 2023 [cit. 2023-08-17]. Available from: https://www.gme.cz/v/1508405/modul-dc-dc-menic-step-down-125-32v-5a

[15] Westinghouse WA12120. *GME electronic* [online]. Prague, Czech Republic: GME electronic, 2023 [cit. 2023-08-17]. Available from: https://img.gme.cz/files/eshop_data/eshop_data/1/540-508/czn.540-508.1.pdf

[16] XH-M604 Řídicí modul nabíječky baterií 6-60V. *Dratek.cz* [online]. Havlíčkův Brod, Czech Republic: Dratek.cz, 2022 [cit. 2023-08-17]. Available from: https://dratek.cz/docs/produkty/1/1702/1624863755.pdf

[17] YX850 Automatický přepínač napájení 5 - 48V. *Dratek.cz* [online]. Havlíčkův Brod, Czech Republic: Dratek.cz, 2023 [cit. 2023-08-17]. Available from: https://dratek.cz/arduino/74578-yx850-automaticky-prepinac-baterie.html