POSSIBILITIES OF USING MODERN ACCESS CONTROL SYSTEMS FOR THE PURPOSES OF RESEARCH AND TEACHING AT UNIVERSITY

Filip Lenko¹, Andrej Veľas²

Abstract: This article discusses the position of access control systems in the field of intruder systems, its benefits and wide-ranging use in the academic environment. This article points out the potential of access control systems and motivates further research in the field of alarm systems and their integration. As part of the dissertation a project for an access control system was submitted, which enabled the purchase and implementation of an access control system for the teaching laboratory at the Faculty of Security Engineering. The installed access control system serves not only as security for the selected laboratory, but also as a teaching aid, which is used in teaching and thus increases the practical competencies of students. The system is also accessible to students, who can create methodological procedures for its testing and subsequently test them. Such measurements are then used in solving students' final diploma and dissertation theses. Approximately 50 students use the access control system during the academic year. The contribution and aim of the paper is to point out the use of the implemented system in the academic environment and its impact on the improvement of teaching. The conclusion of the article consists of the benefits resulting from the implementation of the access control system at the Faculty of Security Engineering and recommendations for its further use.

UDC Classification: 378, **DOI:** <https://doi.org/10.12955/pss.v1.62>

Keywords: access control, education, training, safety.

Introduction

Current trends and the rise of modern technologies bring informatization more and more often into everyday life. As part of this process, a number of useful and practical solutions have been created that make users comfortable and simplify their lives. While the field of digitization and technical development has experienced an enormous boom in recent years, so has the field of security.

In the area of security of buildings and public spaces, the level of security can be increased by intruder systems. Under intruder systems, it is possible to imagine a wide range of electrical systems, the aim of which is to guarantee the protection of the protected interest. Typical representatives of intruder systems are alarm security systems, CCTV systems, fire alarm systems and access control systems (Halaj et al., 2018).

The researchers of the Faculty of Security Engineering have been dealing with intruder systems for a long time, and at present they have also begun to focus on the area of access control systems. Access control systems can interconnect all areas of intruder systems and their operation also includes mechanical means of restraint, which is why they need to be given great attention. The area of access control systems is being explored on a small scale despite these facts.

The Faculty of Security Engineering teaches subjects such as intruder systems, electrical security systems and access control systems. The lecturers try to provide students with as much information as possible in this area. An access control system from Entry was installed in the laboratory for a better approach to access control systems and the practical training of students – more advantages are stated in figure 1. The System contains a controller, magnetic locks and two biometric readers, which also have RFID readers (Boroš et al., 2018).

This article deals with the use of access control systems not only in terms of security but also their use in the academic environment and seeks the position of access control systems in the field of intruder alarm systems. The main goal of the paper is to point out the use and benefits of the implemented access control system for the practical teaching of subjects and its wide use in the academic environment.

Access control systems

Access control systems can be generally defined as electronic systems whose task is to control the entry into or exit from a protected object or room. Their aim is to allow an authorized person to enter the protected area and to prevent an unauthorized person from entering the protected area. For this activity, access control systems use elements of an electrical alarm system in combination with elements of mechanical security. Depending on the level of security, they are often combined with the staff in the

¹ University of Žilina, Slovakia, Faculty of security engineering, Department of security management, filip.lenko@fbi.uniza.sk

² University of Žilina, Slovakia, Faculty of security engineering, Department of security management, andrej.velas@fbi.uniza.sk

monitoring center. Most access control systems also function as part of an object alarm system. For this reason, we can say that access control systems are an integral part of the whole alarm intruder system (Loveček et al., 2018).

The design and architecture of the system is specific to each object and adapts to the requirements of the owner, the specifics of the secured object and the required level of security. Access systems are manufactured in many designs according to their purpose and degree of security (Veľas et al., 2019).

Simple systems consist of only one reader directly in which the decision module is located together with the user database. Such systems are advantageous for simple security applications where a high degree of security is not required and the value of the interest is not high. Such a system is advantageous in securing one or two rooms within a building, or for controlling one entrance to a building. However, if it is necessary to provide more rooms, it is advantageous to choose another type of system architecture. A typical architecture contains the following components: access readers - these are located at the entrances to the secured rooms, control unit - it is connected to access readers and other extensions, mechanical security devices - electronic locks, door closers, sensors, power supplies and more (Kutaj et al., 2017). The capacity of the control unit is often a problem. The most frequently manufactured control units can control 4 to 8 doors, if we need to control more doors, it is necessary to expand the system with another control unit and access readers, which must be interconnected. With very large systems, the control units can be connected via a computer network and their register or database can be stored on a computer server (Mariš et al., 2020).

A typical principle of operation of an access control system is: a person requesting access to a protected area must prove his identity at the access point. There are several ways to prove your identity. A person's knowledge, most often a code – either a PIN or a password, a method of ownership, i.e. a token - can be used to prove their identity - for example an NFC tag, an RFID card or a property using biometric methods, for example fingerprint, iris, retina and more for identification (Norman, 2017). The access reader reads the data and sends it to the control unit for comparison. The control unit then compares the data obtained with the data in its registers. If it finds a match, the control unit allows this person to enter by releasing the electric or magnetic lock or releasing the turnstile. The control unit writes the request to memory. If the submitted identification sample has not been found in the register, the system must not release the entry and thus prevent the entry of an unauthorized person and indicate this attempt (Lenko & Veľas, 2019).

The so-called soft elements also enter the whole system. As soft elements we can mark system users - authorized persons for entry and system administrators (Norman, 2017). The reliability of the access control system can be assumed on the basis of its parameters, the methods used for identification, security levels, etc., we can say that the system is almost ideal, but soft elements are the risk. If an authorized user provides a PIN code or access token to a third party, they can enter the protected area and the system will not detect that there is an unauthorized person in the secured area (Jain, 2016). For these reasons, it is necessary to have security policies in place within the organization's security system that must be followed by authorized persons (Halaj et al., 2018).

Position of access control system in the field of alarm systems

Access control systems have their position within the overall system of protection of buildings and alarm systems. Unlike alarm security systems, the area of access control systems also includes mechanical security means, e.g. turnstiles, security passages, electric locks, magnetic locks and other devices. The access control system is often connected to an alarm security system. If an unauthorized user tries to get through the access point, the system signals such action and if he manages to overcome the access point, the access control system can trigger an alarm condition in the alarm security system, in other words it can serve as an active component of the alarm security system (Loveček et al., 2018).

Another system with which it cooperates is an electric fire alarm system. In the event that a fire alarm condition is declared, all access points that serve as escape routes must not be blocked and allow persons to leave the protected area. A number of access readers of access control systems are supplemented by the so-called pressure signaling, when pressure is created by the intruder on a person who is allowed to enter. The pressure signaling function of the access control system can be described as an emergency system resp. for the emergency call system, which also fall under the area of alarm systems. Another

example is the so-called safety capsules. The security capsule system combines camera systems, biometric systems and mechanical restraint systems (Lenko & Veľas, 2019).

We can conclude that the access control system can be connected to almost all types of intruder alarm systems and mechanical restraints and can be described as an interdisciplinary system. The access control system offers a high degree of integration with other alarm systems as well as the possibility of connecting a large number of different technologies.

Implementation of access control systems at the Faculty of Security Engineering

Figure 1: Benefits of implemented access control system

As part of the solution of the student's dissertation and the practical part of teaching the subject Access control systems at the Faculty of Security Engineering in Žilina, it was necessary to expand the current equipment of the faculty with an access control system. A project was developed to procure the access control system. After a broader analysis of the possibilities, the project also included other possibilities of using this system within the Faculty of Safety Engineering. The institutional grant project was subsequently financed by the faculty itself and some results of its solution are as follows:

- Access control system used to control access to the laboratory:
 By implementing an access system to the laboratory and classrooms, it is possible to allow access to the authorized persons most often by teachers on the basis of their biometric data. As the laboratories have the equipment, so far the keys to these rooms are issued at the gatehouse. The system allows you to grant access to authorized persons, but also to set time filters, i.e. to determine at what time the authorized person will have access to the room. The advantage is simple control and registration of authorized persons in the rooms and it is also possible to connect the access control system to the alarm system, which would indicate an unauthorized attempt to enter the room.
- Access control system serving as a study aid:
 A very significant benefit of the installed access control system is its use in the teaching process as a teaching aid. As part of their studies, students regularly come into contact with one of the systems whose applications they are learning about. Within the subjects Electrical Security Systems and Access Control Systems, students in laboratory teaching work with the access system, its software interface, learn how to connect, configure, etc. (Boroš et al., 2018). This knowledge then serves students in the design of security systems in the project documentation. Students within the subject of Access control systems must prepare a seminar project. Part of the students do their project on theoretical level and another part do it in the practical area. In the practical seminar project, their task in biometric systems is to determine the parameters FAR and FRR based on measurement according to the prescribed methodology. Implemented readers

are combined, which allows students in their seminar project to measure and determine the reliability of the RFID system.

- Records of students' attendance at laboratory exercises:
Before the start of the course, the presence of all students in the laboratory exercises is verified. This activity is lengthy, performed manually, and sometimes may not be relevant. All students of the University of Žilina in Žilina have European Student Passes - ISIC, which the access reader can read. Experimental registration of students was performed using an RFID reader, where each student attached his ISIC card to the reader while entering the room. Subsequently, a list of students present at the laboratory exercise was created, which can be exported from the access system software. As part of the student record, a measurement was also made regarding the preferences between RFID and biometric technology. Students were given the opportunity to prove their presence in class through RFID technology or a fingerprint. Almost 80% of students chose the option of a fingerprint, they justified it with user friendliness, and it is easier according to them.
- Aid in solving practical parts of final theses and testing:
The installed access control system as well as other systems that are used within the Faculty of Security Engineering in teaching can be used by students to test or verify the functionality of the system in specific conditions. The results of measurements and the acquired knowledge are further applied in the solution of practical parts of diploma and dissertation theses. The practical conclusions then create benefits for the final work and better prepare students for subsequent practice. The practical part of the final theses is focused on access control systems and is similar to a seminar project that students do as part of their studies. Students create their own procedures for testing access control systems as part of the final theses. The aim is to find out whether the FAR and FRR values for biometrics are the same for other measurement procedures. Another challenge for students is to identify the possibilities of overcoming biometric systems. To overcome them, they try to use various methods and tools.
- Publication of test results and comparison of different access control systems:
Access control systems belong to the field of intruder alarm systems. The team of the Department of Security Management has long been dealing with the area of alarm systems in its scientific research activities. In general, a large number of researchers and authors do not deal with access control systems, so we decided to pay more attention to the issue of access control systems. Several experimental measurements are planned for the next period, the results of which will then be published in scientific publications and conferences and thus help to expand the field of knowledge about access systems.

Users of the access control system at the Faculty of Security Engineering

The main users of the project outputs are staff and PhD students who test the components of intruder alarm systems and students who will use the proposed system for experimental testing and as a teaching aid. The results of experimental testing will be further used in the final works and competition works.

We can also assume the acquisition of new contacts or new connections to companies engaged in the production and installation of security systems, the result of which will be the connection of studies with practice (Šoltés et al., 2018).

Another benefit is the acquisition of new knowledge about access control systems usable in their design and thus increase the level of security of protected objects.

Non-certified testing of access control systems

Testing begins by verifying the complex functionality of access control systems. The functionality of the system, control of electric locks, backup power supply of the system, user friendliness, data recording into the device memory, their export and safety of component connection are comprehensively verified.

Subsequently, we approach the main measurements, which are more sophisticated. They consist mainly in testing access readers. For RFID readers, the most common test is the so-called capacitive test of the reader (Sichkar, 2018). The test is performed using a device that contains several RFID cards and gradually adds them to the reader. By increasing the frequency of adding cards to the reader, it is possible to find its limits. The result of such a test is to find out how many cards it can read correctly in a specified

time interval and how many times the reader has read the card incorrectly. The most important result is to find out if the system has accepted a card that is not registered in the system. In practice, due to incorrect card recognition, the system may allow unauthorized entry. In the measurement of RFID systems, such an error is very rare, current RFID systems are very reliable, but their disadvantage is that the data from the RFID or NFC card can be stolen.

For these reasons, we focus more on biometric-based access readers. Testing of biometric readers can be divided into two areas. One area of testing overcoming systems by different procedures. Silicone castings and fingerprints on adhesive tape are most often used for fingerprints. With a face identification system, a photograph can be submitted to the camera. These tests do not prescribe the relevant technical standards, but provide a much more comprehensive view of the level of security of biometric systems.

The second area of measurement and assessment of biometric readers are their parameters FAR and FRR - False rejection rate and False acceptance rate. Measuring these characteristics is more demanding than with RFID readers. The measurement on the fingerprint readers consists in applying the fingerprint to the reader in a specified number of repetitions, for example 100. During the measurement of the FAR parameter, all persons proving their identity must be unauthorized. During the measurement of the FRR parameter, these persons must be authorized, ie their fingerprint is stored in the system memory. During the measurement, the FAR records how many times the fingerprint of an unauthorized person has been accepted. During the FRR measurement, we record how many times the entry of an authorized person was not allowed. After the measurement, the individual parameters are calculated using the following formulas (Rak, 2008):

$$FAR = \frac{N_{FA}}{N_{IIA}} \qquad FRR = \frac{N_{FR}}{N_{EIA}}$$

N_{FA} – Number of false acceptances

N_{IIA} – Number of attempts by unauthorized persons to identify

N_{FR} – Number of false rejections

N_{EIA} – Number of attempts by authorized persons to verification

Importance of testing components of access control systems

Testing of components of access control systems consists in measuring and testing the defined properties of the components and subsequent comparison with the technical documentation provided by the manufacturer of the tested system. We divide the components of access control systems into four classes according to the relevant technical standards. The classification into a specific class, i.e. the degree of security, depends on the results of the component tests. The measurement is performed in an authorized testing laboratory.

Non-certified tests consist in verifying the technical parameters defined by the manufacturer in the technical documentation and subsequently verifying the correct classification of the components into classes and grades. This allows organizations to perform tests during component development with an access control system without the need to spend funds on the entire certification process. All they have to do is test the product we have already tested in an authorized laboratory.

The benefits of tests and measurements that are not certified, i.e. not prescribed by technical standards, make it possible to examine the shortcomings of the components of access control systems. These results can then be published at professional conferences.

Conclusion

This article determines the position of access control systems within a comprehensive system of alarm systems. It is important to point out the interconnection of access control systems to other alarm systems. At present, access control systems do not have a high position among alarm systems, they are only considered to be a part of them. Access control systems are often unbeatable in their security applications, but mechanical restraints or incorrect selection and installation fail.

This article points out that the implementation of the access control system at the Faculty of Security Engineering has not only increased the level of laboratory security but mainly contributes to increasing the practical competencies of students and makes the study more attractive for students.

As part of the study, students can design their own procedures for measuring and testing various parameters of access control systems such as the characteristics of FAR and FRR. Students can explore transmission paths and communication between components. The results of experimental measurements are further used in the final work of students.

From previous measurements, we have found that 80% of system users prefer biometric identification - fingerprint over RFID cards. This was justified by the user-friendliness of the biometric system, so there is no need to carry any token or RFID card. It is also interesting to use entry control systems as an attendance system for students for laboratory exercises. The attendance system is currently used only by employees for arrival and departure from work, but we have also managed to use the access control system as an electronic record of the presence of students at a specific laboratory exercise. In the future, it is possible to make such records using a camera system and compare individual methods.

By performed measurements on biometric and RFID systems, we often verify the values given by the manufacturers, if we follow the methodology given by the relevant technical standard. However, biometric systems can be overcome in simulated conditions by their own procedures. These findings are very valuable for manufacturers of access readers and access control systems.

The field of access control systems is on the rise, but few authors discuss this area. This fact gives opportunities and motivation for researchers to research in a given topic.

Acknowledgment

This article was supported by the Internal Grant Scheme of Faculty of Security Engineering, University of Zilina from the grant No. 201907.

References

- Beqqal, M. E. (2017). Access Control System in Campus Combining RFID and Biometric Based Smart Card Technologies. *Europe and MENA Cooperation Advances in Information and Communication Technologies* (pp. pp. 599-569). Cham: Springer.
- Boroš, M., Kutaj, M., Mariš, L., & Veľas, A. (2018). INTED 2018 Proceedings. *Development of security at the local level through practical students training* (pp. 725-729). Valencia, Spain: INTED2018.
- Boroš, M., Veľas, A., Kampová, K., & Loveček, T. (2018). 10th International Conference on Education and New Learning Technologies. *Creation of final works as part of the dual education of university graduates* (pp. 6710-6713). Palma, Spain: EDULEARN18.
- Dragan, S. K. (2020). Expert Systems with Applications, vol. 143. *A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities*, pp. 1-27.
- Halaj, M., Kutaj, M., & Boroš, M. (2018). CBU International Conference Proceedings. *The organization's safety culture, its indicators and its measurement capabilities* (pp. 595-600). Prague: CBU Research Institute.
- Jain, K. A. (2016, August 1). 50 years of biometric research: Accomplishments, challenges and opportunities. *Pattern Recognition Letters*, vol. 79, pp. pp. 80-105.
- Kutaj, M., & Boroš, M. (2017). Innovations in science and education, CBU international conference proceedings. *Development of a new generation of magnetic contact based on hall-effect sensor* (pp. 1154-1158). Prague: Central Bohemia University.
- Lenko, F., & Veľas, A. (2019, 9 15). Alarm systems and their use in municipalities. *Košická bezpečnostná revue*, pp. 41-46.
- Loveček, T., Mariš, L., & Šiser, A. (2018). *Plánovanie a projektovanie systémov ochrany objektov. [Planning and design of building protection systems.]*. Žilina: EDIS.
- Mariš, L., Loveček, T., & Zeegers, M. (2020). Security of Infrastructure Systems: Infrastructure Security Assessment. In D. Rehak, A. Bernatik, Z. Dvorak, & M. Hromada, *Safety and Security Issues in Technical Infrastructures* (pp. 353-382). Hershey, PA: IGI Global.
- Norman, L. T. (2017). *Electronic access control. Second edition*. Chippenham: Butterworth-Heinemann, ELSEVIER.
- Rak, R. M. (2008). *Biometrie a identita človeka ve forenzních a komerčních aplikacích*. Praha: Grada Publishing.
- Ross, N. P. (2020). *Protecting controlled unclassified information in nonfederal systems and organizations*. USA: NIST.
- Sichkar, V. N. (2018). Fingerprint Identification as Access Control System. *International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)* (pp. pp. 1-4). Moscow: IEEE, 345 E 47TH ST, NEW YORK, NY 10017 USA.
- Šoltés, V., Kubás, J., & Repková Štofková, K. (2018). INTED2018 Proceedings. *Motivation of students in education in the field of security management* (pp. 9331-9337). Valencia, Spain: INTED2018.
- Veľas, A., & Boroš, M. (2019). *Intruder alarms*. Žilina: EDIS.
- Veľas, A., Boroš, M., & Lošonczi, P. (2018). *Testovanie detekčnej schopnosti vybraných komponentov poplachových systémov. [Testing the detection capability of selected components of alarm systems]*. Žilina: EDIS.