Ondrej ZIMEK[1], Vaclav MACH[1], Jan VALOUCH[1], Milan ADAMEK[1], Martin HROMADA[1]

Tomas Bata University in Zlín, Faculty of Applied Informatics, Department of Security Engineering (1)

doi:10.15199/48.2020.04.05

Integrated Alarm System with the Access System for Kindergartens

Abstract. Abstract*. The aim of this article is to design the Integrated Alarm System for the Kindergartens which can handle Alarm, Access and Attendance application by a common system. A similar system is not available on the market yet and there are an opportunity and interest for integrated systems. This article is focused on the kindergartens as a soft target where also Access and Attendance system is needed. Due to this demand, the new concept of the Integrated Alarm System was designed. The main-board consists of three independent microcontrollers where each microcontroller is responsible for one application. The Attendance and Alarm part are prepared for the components which are using the bus connection by the RS-232 or RS-485. The system also has an Ethernet and GPRS interface for outside communication and connection. Each part of the system and the schematic part come with a detailed explanation of the components.*

Streszczenie. *W artykule zaprezentowano projekt systemu alarmowego stosowanego w ogródkach dziecięcych. System zabezpicza teren przed wejściem osób niepożądanych.* ***Zintegrowany system alarmowy zabezpieczający szkolny ogród dziecięcy przed obecnością osób niepożądanych.***

Keywords: Technical Security, Control and Indicating Equipment, Soft Target, Kindergarten
Słowa kluczowe: System alarmowy, niepożadane wejscie, ogód dziecięcy

Introduction

The concept of soft targets is slowly becoming known to the public. The reason is that recent terrorist attacks have been targeted at these places. The soft targets could be defined as crowded places that have very low or no security solutions against terrorist attacks. [1] Soft targets are not all crowded places and there are three main categories of crowded places; Critical Infrastructure, Soft Targets and Hard Targets

Fig. 1 Crowded places [2]

The difference between these categories is safety solutions. The security of the critical infrastructure is solved by laws and documents of government. A fuel store is, for example, a critical infrastructure element. On the other hand, hard targets are places with very high safety solutions. A nuclear power plant is one of a representative of hard targets. The remaining objects A and E are not marked as crowded places because the concentration of people in these places is at a low level. [2,3]

Soft targets (sector C) are part of a group of targets called crowded places (sectors B + C + D). In addition to soft targets, there is an important category of critical infrastructure elements (sectors A + B) that have certain security specificities and are dealt with by specific legislation. Furthermore, even the part of critical infrastructure elements that gather a greater number of people (sector B) is not among the soft targets. Sector D is the group of targets where the public gathers (ie crowded places) but, unlike soft targets, they have security against violent attacks. Sector E then shows well-secured, often non-public environments with few people. These two groups (sectors D + E) are systematically engaged by the security community according to specific legal regulations, we call it hard targets. Sector A is a critical infrastructure with no more public.

A representative of soft targets:

- School facilities,
- Train and bus stations,
- Libraries and Cinemas,
- Sport halls,
- Entertainment venues,
- Religious sites,

A kindergarten could be defined as the soft target by definition. Kindergartens are places with a high concentration of children, and lots of people believe that their children are safe there. Schools mean children. Children are associated with extreme vulnerability while at the same time they represent one of the most precious assets of each society. That is why attacks against schools are perceived as the most tragic ones. In the past, schools have been targeted by terrorists but also by students themselves, which calls for a multifaceted security approach.

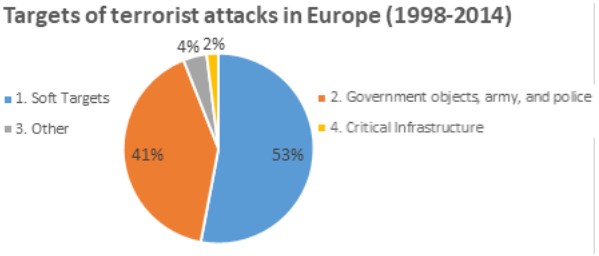

Fig. 2 Targets of terrorist attacks in Europe (1998-2014) [1]

Previous figure shows targets of terrorism in Europe that happen in years 1998-2018. As can be seen, the most attractive targets were the soft targets with a share of more than half of all attacks. According to the author [2] the most common modus operandi were knife attack. The most serious attack happened in China in 2010. Seven children and two adults have been killed and 11 children have been injured. The attacker, 48-year-old man, attacked by a cleaver. There are three possibilities to protect kindergarteners or soft targets; Security Personnel, Mechanical Devices and Electronic Devices. The electronic devices have been chosen for this research. [1] Before installation any security measures against terrorism, it is appropriate to perform a risk analysis.

The author [1] mentioned that the IAS should serve primarily for detection of perimeter intrusion or unauthorized entry into a building or area. The system should be divided into several areas and offer a wide range of possible uses. For example: motion detectors, open door and window

sensors, glass break sensors, fence climbing detectors. In all these devices, the alarm output should be connected to a local CIE which can sent the alarm message by SMS to a mobile device or sent out to the Alarm Receiving Center which provides central dispatching services, including storage of selected data from secured premises, as well as remote surveillance and control.

Entry and attendance control systems primarily provide data for the payroll office but at the same time can be used to make entry of unauthorized persons more difficult or to hinder unauthorized access within the building. Doors and walk-ins operating on chips, cards or biometric recognition can efficiently prevent criminal behavior and vandalism, however, it needs to be said that they do not provide sufficient protection in case of an active attack. [4]

Intruder Alarm System

Every Intruder Alarm System is a part of the technical security which should protect the life, health and the possession of the owner. The main element of the system is electronic system instead of person. According to the author [5] when a person stares at a screen for more than 20 minutes, his attention drops by 30%; and for periods over an hour, this drop can reach 70%. It means that real person is not very reliable, and the electronic device is used. The reaction of the system can be also more precise and quicker than a person can be.

This article is focused on the conjunction of the IAS and the access system which must follow the ČSN CLC/TS 50398 standard. The Integrated Alarm System is any system having one or more common devices where at least one of them is an alarm application. This type of the connection is call the Integrated Alarm System. [7]

There are two possible variants of the connection. The first one represents a combination of two or more single-purpose systems. Dedicated applications are connected to a common optional device that is not required by the standard. The connection is realized using an additional transmission line. Dedicated devices are connected to the common complementary device via an additional transmission line. The device which is required by the standard in the alarm application must not be affected by any other dedicated or optional system in any operating condition. The second type represents a combination of two dedicated systems which has a common device at least for one of the applications. The used device must follow the standard. represents a combination of multiple alarm or non-alarm systems. These systems use common devices and transmission lines. Failure of any application in the system can impact the integrity of the device required by the standard. It means that the integrity of the required device can be affected. [6]

Every Intruder Alarm System usually consists of several components like Control and Indication Equipment, Alarm detectors. communication interface and the power supply. The main components of the system is the CIE. This device periodically scans connected detectors and evaluates incoming information. The detectors can transmit only basic states like Serenity, Alarm, Failure, and Sabotage. Serenity and Alarm. [8] The CIE must react to the states according to the current schedule in the system. The system must trigger alarm when detector is activated and the system is secured.

The potential intruder must be detected in the protected room or area. Detectors can be divided into several types according to place. These types are light-sensitive (Passive Infra-Red), sound-sensitive (Microwave) contact-sensitive (Magnetic contact) or vibration-sensitive (Glass-break). Each category is suitable for different purpose and location.

The other aspect is the environment, where detectors are placed. Detectors can also be divided into the outdoor and indoor according to the environment. Used component must be able to work correctly in a given environment. The expected environments are indoor, indoor general, outdoor protected, and outdoor general. Each environment has its own description of possible conditions.

One of the used components must be a part that provides power supply in case of power failure. Due to the information, the used component must be able to accept 230 V input voltage, store backup voltage in a lead battery and provide stable 12 V output voltage. The UPS must be dimensioned according to the number of connected devices.

Access system

The Access system is electronic system which protects some place or area against the unauthorized entry. It is usually connected with the movement monitoring systems, and it can be used as addition component to the Intruder Alarm Systems or Closed-circuit Television. The access permission to the user or person is given by the system according to the current time scheduled timetable. The system can approve or reject the access after success identification. The advanced systems can monitor the movement of the user in several zones and flexibly changes the access rights.

The access system can be extended by the attendance system which can identify the person movement through several zones, and based on the time, this information can be used for the calculation of working time. Every access system consists of several components like power supply, main unit, card reader, input device, communication interface, identification chip, and evaluating software. There is also standardization for the access systems called ČSN EN 60839-11-1 Alarm and electronic security systems - Part 11-1: Electronic access control systems - System and components requirements. [9

Before the main design of the access system, each object must be evaluated for the level of the classification. The standard uses four types of the classification from 1 (low risk) up to 4 (high risk). This classification is based on the value of property, and the types of potential attack. The classification is the following.

1. Low risk - Organizational resources, protection of low value assets, where the potential intruder has little skill, little knowledge of access control systems, identification tools and IT technologies, little money for attack.
2. Low to Moderate risk - Organizational resources, asset protection of low and medium value where the potential intruder has intermediate skills and knowledge of access control systems, identification means and IT technologies, small to medium funding for attack.
3. Moderate to High risk - Less organizational resources, protection of high value commercial resources where the potential intruder has great skill, little knowledge of access control systems, identification means and IT technologies, medium funding for attack.
4. High risk - Very high value or critical infrastructure commercial assets where the potential intruder has very high skill and knowledge of access control systems, identification tools and IT technologies, great financial resources for attack. [9]

Different situation needs different classification of the identification due to the degree of the security. According to this problem, the identification classes were created. The class expresses the connection between the zone and the authorized user. The system must have in all entrance

unambiguous identification of the person. There are five classes of the identification.
Identification Class 0 - no direct identification. Based on simple access request without user identity (button, contact, motion detector, etc.)
Identification Class 1 - information stored in memory. Based on passwords, personal identification numbers, etc.
Identification Class 2 - identification element or biometrics. Based on identification elements, cards, physical keys, fingerprints, etc.
Identification Class 3 - Identification element or biometrics together with information stored in memory. Based on the use of a combination of identification element or biometrics and information stored in memory. [10,11]

Requirements for the Integrated Alarm System

This chapter consists of all requirements for the Integrated Alarm System. The System should be constructed like other commercially made IAS according to the mentioned standards, and all detectors on the market should be connectable to the system. The system should also consist of the Access and Attendance System controlled by the software. The function and should be controlled remotely via the Ethernet connection. In the final design should be placed an Uninterruptable Power Supply in case of power failure. All requirements are listed in this chapter and the actual design with the schematic is listed in the following chapter.

The first part of the requirements is focused on the Intruder Alarm System which is the most important component of the system. The main components of the alarm part must the microcontroller which is focused only on the evaluation of the information obtained from connected detectors. This part should be able to communicated with the digital and with the analog alarm detectors. The system should be able to cover up to 128 connected devices. [12]

The second part is focused on the Access System. This part should be able to communicate with the common contact and contactless card readers used for the authentication is access systems. There should be placed a removable memory card for the access and attendance system. Both parts should have access to the communication interface via the Ethernet and the GPRS modules. Designed system should be placed in steel box with the Uninterruptible Power Supply backed up by the battery.

Integrated Alarm System for Kindergartens

This chapter consists of the schematic part with an explanation based on the previous chapter and standardization. The designed system should be placed on a single Printed Circuit Board. Only the UPS with the battery will be placed separately inside of the steel box. The block schema of system can be found in following figure.

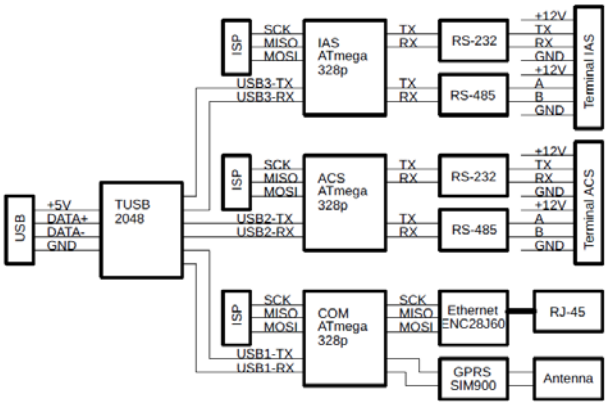

Fig. 3 Block schema of the designed system

Schematic part for the Alarm and Access Applications

Both parts of the system are driven by the single microcontroller ATmega328P which has enough power to manage all connected devices and other communication. The IAS part should handle up to 128 detectors connected by the serial bus called RS232 and RS485. This protocols are very often by all manufacturers on the market. However, this interface is not supported by the used microcontroller. Due to this problem, an external convertor from the Universal Asynchronous Receiver Transmitter (UART) to RS232 and RS485 protocol was placed. The schematic of the MAX-232 and MAX-485 can be found in the following figure.

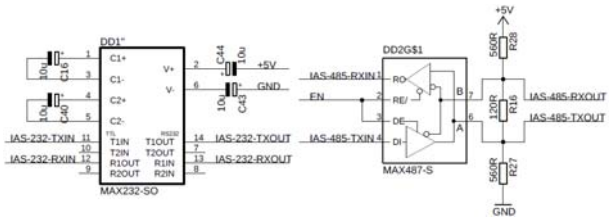

Fig. 4 Schematic part of the RS-232 and RS-485

Each microcontroller has the same setting like power supply +5V, frequency 16 MHz, UART communication and also the SPI interface in form of the pinhead on the board. The external communication is done by the USB interface using the USB hub called TUSB2046 which can be found in the following figure.

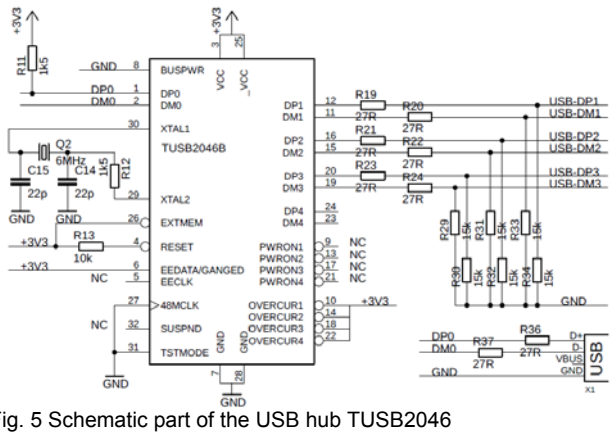

Fig. 5 Schematic part of the USB hub TUSB2046

The Ethernet and GPRS Communication

The external communication via the Ethernet is done using a single chip called ENC28J60 which is powerful enough to establish reliable Ethernet interface. In this case, the chip is connected to the ATmega328P via the SPI. The part of the physical Ethernet connection is done using two pairs of pins for transmitting and receiving data. However, the signal must be galvanically isolated from the physical connection using a special Ethernet magnetic transformers. These transformers can be placed separately on the board or it can be placed in the Ethernet connector. In this case, the transformers are placed in the connector. There are also additional electronic parts between the ENC28J60 and the Ethernet connector which helps with the electromagnetic stability. The schematic part can be found in the following figure.

The ENC28J60 has very easy and structured library for programming basic implementations like web server which is the main purpose of this part in the system. This server can be used or the remote control of the system using the internet and it can be used as s transmitting part of the alarm signal to the Alarm Receiving Center (ARC). The

biggest advantage is that the chip uses its own power and it is not dependent on the power and the time of the PC.
The other external interface of this system is GPRS communication which is done using the SIM900. This chip is very often used for additional communication using the wireless method. The connection between the chip and the ATmega328P is also very easy via the classical UART.

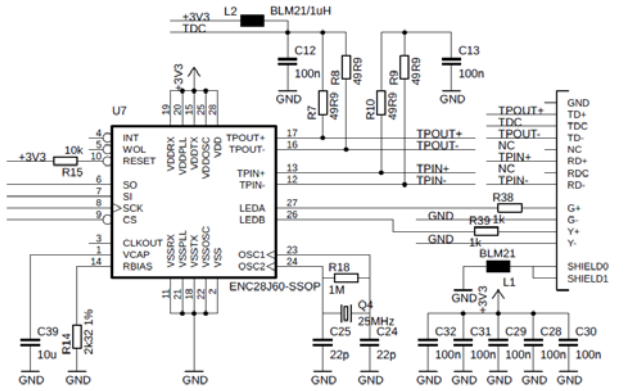

Figure 6 Schematic part of the Ethernet communication using the ENC28J60

The SIM900 need the Subscriber Identification Module (SIM) card for the communication with the closest base station. The SIM connector is ready for the classical size and it is placed on the top side of the board. The biggest advantage of this chip is the programming which is done using the AT-commands. It means that the program sends the exact command with parameters which will be executed. All incoming data must be requested without any external interrupt. This part can be used for the remote communication and it can be used for the transmitting the alarm message to the ARC as well. The wireless communication must have the antenna connector. In this case, the RSMA connector for the GPRS communication was used and placed on the edge of the board. The schematic part can be found of the following figure.

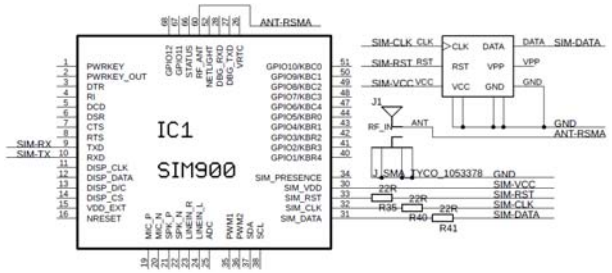

Fig. 7 Schematic part of the Ethernet communication.

Final Design of the Integrated Alarm System for the Kindergartens

The whole system was designed as common IAS on the market which can fit is quite compact casing with other components. The PCB has very compact dimensions without any excessing part over the edge. The terminals for the connecting IAS and ACS components are the most important connectors. Both terminals are situated on the side in the middle of the edge for easy access. As mentioned before, both terminal consists of serial interfaces RS-232 and RS485 for each system. There are also pins for the power supply for the connected devices. The final design of the Integrated Alarm System for the kindergartens can be found in the following figure.

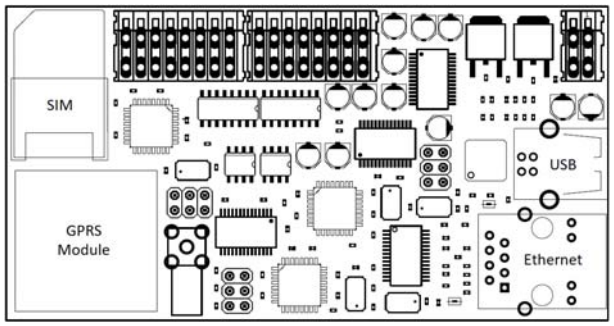

Fig. 8 Final design of the Integrated Alarm System for the Kindergartens

There are also terminal for the external communication like USB, Ethernet and the GPRS antenna. The USB and the Ethernet connectors can be placed through the casing to enable passing external cables without opening the casing. There is the terminal for the external antenna because the antenna is unable for working in the steel casing. Usually the external antenna is placed out of the steel casing. In the corner of the PCB is also the power supply for the system and for the external devices.

As mentioned before, this system can be used for the managing Alarm, Access and Attendance system independently of each other. Each system has its own microcontroller and external communication. System can use all common alarm, access and attendance devices which communicates via the RS-232 or RS-485. Each system can handle up to 128 independent devices like detectors or card readers. Both systems can use common external interface like USB, Ethernet and GPRS. The system can be managed by the program which can run on common PC with the USB or Ethernet. The final PCB should be placed in the special steel box with the UPS.

Conclusion

This article is focused on the soft targets namely Kindergartens which are part of school facilities and the main goal is to design the Intruder Alarm System for this type of facility. The design combines the common Intruder Alarm System with the Access System into one independent system. This combination is very often appraised by the personal due to the reduction of the complexity. The access system also provides better management and the surveillance not only of the visitors but also of the children which are in the facility.

The designed device is composed of two independent parts each for one application. Both parts share the common external communication interface such as USB, Ethernet and the GPRS. Each part also has separate internal communication interfaces where all needed alarm of access components can be connected. The system can handle all common devices on the market due to the standardization. All electrical schematics of all part are described and composed according to the current standardization for present application. The final product can handle up to 128 alarm components and 128 access components and it should be placed inside of the independent steel box witch the UPS.

The main board can be easily managed and programmed remotely from the PC or other device due to the external communication. The external communication can be also used as an interface connected to the ARC in case of the alarm is triggered. Further research can be focused of the sophisticated program which can manage all needed function of the real-time operating system.

Acknowledgement

This work was supported by the Internal Grant Agency of Tomas Bata University under the project No. IGA/FAI/2020/003.

Authors

Ing. Ondrej Zimek, Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stráněmi 4511, 760 05 Zlín Czech Republic, E-mail: zimek@utb.cz,

Ing. Vaclav Mach, Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stráněmi 4511,760 05 Zlín Czech Republic, E-mail: v2mach@utb.cz,

Ing. Jan Valouch, Ph.D., Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stráněmi 4511, 760 05 Zlín Czech Republic, E-mail: valouch@utb.cz,

doc. Mgr. Milan Adámek, Ph.D., Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stráněmi 4511, 760 05 Zlín Czech Republic, E-mail: adamek@utb.cz,

doc. Ing. Martin Hromada, Ph.D., Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stráněmi 4511, 760 05 Zlín Czech Republic, E-mail: hromada@utb.cz.

REFERENCES

[1] Kalvach, Zdeněk et al. Basics of Soft Targets Protection: Guidelines. Soft Targets Protection Institute. Prague 2016.

[2] Lapková, Dora, Lukáš Kotek: Možnosti ochrany měkkých cílů, Fakulta bezpečnostného inžinierstva, Žilinská univerzita, ISBN 978-80-554-1398-3

[3] Fagel, Michael J. a Jennifer L. Hesterman, ed. Soft targets and crisis management: what emergency planners and security professionals need to know. Boca Raton: CRC Press, Taylor & Francis Group, 2017. ISBN 978-1-4987-5632-7.

[4] Benova, Hoskova-Mayerova, Navratil. Terrorist Attacks on Selected Soft Targets. Journal of Security and Sustainability Issues, 2019. doi.org/10.9770/jssi.2019.8.3(13)

[5] Landa, Jiang, Chu Jun, and Miao Jun. Implementation of a Remote Real-Time Surveillance Security System for Intruder Detection. 9th International Conference on Measuring Technology and Mechatronics Automation, (2017). doi:10.1109/icmtma.2017.0032.

[6] KIM, Seung Hyun, Su Chang LIM and Do Yeon KIM. Intelligent intrusion detection system featuring a virtual fence, active intruder detection, classification, tracking, and action recognition. Annals of Nuclear Energy. 2018, 112, 845-855. DOI: 10.1016/j.anucene.2017.11.026. ISSN 03064549

[7] Valouch, Jan. The Proposal of Methodology for Evaluating the Effectiveness of Alarm Systems. Applied Mechanics and Materials (2015). doi:10.4028/www.scientific.net/amm.736.183.

[8] Hanacek, Adam and Martin Sysel. The Methods of Testing and Possibility to Overcome the Protection against Sabotage of Analog Intrusion Alarm Systems. Intelligent Systems in Cybernetics and Automation Theory, (2015). DOI: 10.1007/978-3-319-18503-3_12. ISBN 978-3-319-18502-6.

[9] CSN EN 60839-11-1. Alarm and electronic security systems - Part 11-1: Electronic access control systems - System and components requirements. 1 Prague: The Office for Standards, Metrology and Testing, 2014.

[10] NORMAN, Thomas L. Electronic access control. Waltham, MA: Butterworth-Heinemann, 2012. ISBN 9780123820280.

[11] JUAN, He, Luo GUANG-YI and Zeng LI-JUAN. Intelligent Access Control System Based on RFID. International Conference on Mechanical, Electronic and Information Technology (ICMEIT 2018) [online]. Shanghai, 2018, 2018, 341-343, ISBN: 978-1-60595-548-3.

[12] Belbergui, Chaimaa, Najib Elkamoun and Rachid Hilal. Spatial and Temporal Organization Based Access Control for Wireless Network as a Component of Security Requirements. Wireless Personal Communications. 2017, 97(3), 4587-4619. DOI: 10.1007/s11277-017-4740-z. ISSN 0929-6212.