Security design of selected soft targets

Ondřej Zimek^{1*}

¹ Tomas Bata University in Zlín, Faculty of Applied Informatics, Nad Stráněmi 4511, 760 05 Zlín, Czech Republic.

Abstract This article is focused on security design of selected Soft Targets. For this purpose, the kindergartens were chosen as Soft Targets. One of the reasons for this selection was the fact that some kindergartens were attacked recently. Considering that every kindergarten is unique, the design of security is solved by recommendations form. The recommendations were focused on the combination of three main security categories. Especially the Intruder Alarm System was described in detail.

1 Introduction

It could be said that terrorism is widespread around the world. [1] In recent years, the number of terrorist attacks in the EU has been increasing. More than half of these attacks have been focused on so-called soft targets. [2]

Kindergartens are the places where little children spend their time, and everybody supposed that they are safe here. Unfortunately, they do not avoid attacks. It proves the attack, which happened in the last year in China. About 15 children have been injured by a knife attack at a kindergarten. Furthermore, a man who planned to attack the kindergarten was arrested in France this year. For these reasons, the aim of this study is a security design of the kindergartens.

1.1 Soft Targets

We can define the Soft targets as places with a high concentration of people and low or no security measures against terrorism. For example:

- school facilities,
- shopping malls
- libraries, cinemas,
- restaurants,
- train and bus stations,
- sports stadiums,
- Etc. [2,3,4]

A risk analysis is a necessary tool to determine the security level of an object. For example, the risk analysis could be carried out by the Ministry of Interior of the Czech Republic methodology. This methodology is called "Basics of Soft Targets Protection Guidelines of the Czech Republic". The methodology describes a procedure for assessing the risks of a soft target. For the risk analysis, it distinguishes a few basic parameters – Performing an attack, Place of attack, Time of Attack, Likelihood, Impact and Degree of threat. In the first

column ‘Performing an attack’ there are presented possible ways of performing an attack like Knife attack, Bomb attack, Attack by car or assassination. In the second column, there are two different kinds of places of attack - In front of or inside the building. Time of attack determines whether the attack happens during the Daily working time or Event for invited. The Total Likelihood is calculated as the sum of Accessibility, Obstacles, and Desirability. The Total Impact Value is calculated as the sum of Damage to Building, Threat to Lives, Impact on Community, and Economic Losses. Finally, the Degree of Threat is determined as the product of Total Likelihood and Total Impact. Based on this methodology, the degree of Threat is calculated. Additionally, an acceptable level of risk is determined. Unacceptable risks could be reduced to acceptable levels by mechanical devices or electronic devices. [5]

Fig. 1 Targets of terrorist attacks in Europe (1998-2014) [5].

Figure 1 shows targets of terrorist attacks in Europe in years 1998-2014. As can be seen, the most frequent targets of terrorist attacks are soft targets with a share of 53% of the total attacks. It is possible that this trend will continue in the future. According to this preliminary study, it is needed to secure these places.

* Corresponding author: zimek@utb.cz

1.2 Intruder alarm system

The Intruder Alarm System (IAS) is becoming one of the most important parts of the electronic part of each modern house. The system protects the possession and the life of the owner, and it is a part of the technical security which replaced the physical security. The physical security in the form of the real person is not reliable, and it is very economically inefficient to employ a person as physical security. According to the [6] 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%. Due to these problems, technical security with the alarm systems is nowadays prevalent.

The system can be combined with other systems such as fire system or with the smart house system. Intruder Alarm System with the combination of the smart house can be defined as an Integrated Alarm System. According to the author [7] A smart home is one that incorporates advanced automation systems in order to provide its inhabitants, the sophisticated monitoring and control facilities over various functions. For example, a smart home may have automated facilities for controlling lights, fans, air conditioners, temperature, multimedia systems such as home theatre systems etc., security, window, door operations, curtains and many other functions. In this case, the Intruder Alarm System is the main system which controls other devices. Very often The Intruder Alarm System is integrated with the Fire Alarm System.

Every Intruder Alarm System should consist of main components which can detect the intrusion into the protected object or area. The system also should be able to evaluate and process the incoming alarm signal from alarm detector, and the system must cause a reasonable response to the signal. According to mentioned information, every Intruder Alarm System should consist of following components: Control and Indicating Equipment, Alarm detectors.

The Control and Indicating Equipment is the main part of the whole system. It periodically scans the inputs where the detectors are connected. The mainboard usually consists of the microcontroller which controls the whole system. To this microcontroller is also connected others chips which are responsible for the other communication such as Ethernet connection, Global Position System or programming USB port. Commercially made mainboard usually has the interface to the second board where other chip is responsible for the communication between connected detectors. The customer can have different requirements for the number of connected detectors. That's the reason why commercially made mainboards have separated board for the detectors. The author [8] stated that Each CIE must be manufactured according to the standard EN 50131-3: Control and indicating equipment.

There are many alarm detectors on the market. The detectors can be divided according to its application to many categories. Each category has a different usage in the alarm systems. Each detector must be connected to the CIE.

The digital connection is usually provided using a common bus for several detectors. Each detector has a unique address which is saved in the CIE. This address is also saved in the detector. The biggest advantage of the digital connection is that several detectors can be connected into one buss. The analogue connection is much more complicated. The analogue connection is based on the voltage loop where several detectors are connected in one loop. The difference between detector is ensured by the resistor which has a different value for each detector. This difference is evaluated by the CIE.

The detectors have several states which must be evaluated by the CIE. These states are Idle, Alarm, Failure, Short-circuit, and the Antimasking. According to [7] Anti-masking is a motion ability to detect if an intruder has attempted to defeat the detector by blocking it with a material that blocks infrared energy, such as paper, tape, film, or spray. When the detector is triggered, it automatically sent the signal to the CIE.

Every CIE must have the Uninterruptible Power Supply (UPS) to ensure flawless operation even when a power failure occurs. This event can be caused intentionally by the intruder. The capacity of the UPS must be dimensioned to power CIE and connected detectors during the power failure powered. This time is specified in the standard EN 50131-6 Power Supply Units. There are several durations according to the Degree of Security; However, the minimal time is 12 hours.

2 Control and indicating equipment

The main-board is composed of the microcontroller which has 256kB Program Space, 4 UARTs, 14 PWM, 16 Analog Inputs, 54 Digital I/O ports. This system is responsible for the whole system, and it has the highest rights in the system. There is also an Ethernet communication interface. This communication is established by the W500 which is used in the Arduino Ethernet board. Ethernet board makes possible to link the data with a router through an IP address that is within the range of addresses unused. Thus, it was possible to incorporate features in the prototype server that allow the user to manipulate the system from anywhere as long as access to the Internet or a local area network is obtained.

The main board also has pinheads which can be used to connect standard Arduino boards. In this case, the GSM board is mounted on the main-board. Author [10] mentioned that the GSM board is based on the controller SIM900 by SIMCOM. It supports GSM/GPRS standards and operates at the frequencies of 850, 900, 1,800 and 1,900 MHz. The shield can be connected directly to the board of Arduino Uno by a set of pins mounted at the bottom of the printed circuit board.

The can be connected to the USB hub which can be used for the programming, or it can also be used for the direct communication with the connected computer. In the corner is situated the power connected to the 12 V/DC. On the left side of the board are situated state signals for the Ethernet chip. These signals are

representing the current state of the Ethernet communication. On the top is placed standard pinhead for the Arduino boards. Any of the standard Arduino boards can be used as an extension of the current system. The board also consist of headers which can be used to connect other devices. Connected devices should communicate via the serial interface, which is implemented on the main board. The board has USB hub which allows to connect up to four devices by one cable placed on the side of the board.

2.1 Communication interface

It means that only detectors which are connected by the analogue loop can be connected to this board. Board provides 16 independent loops, and each loop can hold up to three detectors. This makes it possible to connect 48 analogue detectors to the Zone-Board. This number is sufficient for most households.

Each loop can be programmed independently using standard modes such as Normally Closed (NO), End of Line (EOL), Double End of Line (DEOL) and Advanced Technology Zone (ATZ). Each mode comes with some advantages and some disadvantages. The most used mode in the analogue loops is the ATZ mode which has the biggest possible number of connected detectors in one loop, and it is still possible to distinguish between each detector in the loop. This function is caused by using different values of the resistors which are bypassing each detector. The connection between the Zone-Board and the Main-board is established using the serial interface.

The mode consists of three independent detectors. When commercially made alarm detector detect the intruder, it activates the switch which is bypassed by the resistor. This cause that the resistor in the loop is changed according to the activated detector. This change can be measured by the CIE. Each detector has different value; it causes that resistors can be distinguished from each other by the CIE. A special resistor is added at the end of the loop. This resistor allows for distinguish between the idle and the sabotage state. The previous study [9] found that this concept can be extended by using the logarithmic scale of the resistors to increase the maximal possible states up to 12 to one loop.

2.2 Smart integration

As mentioned before, Designed CIE should be able to communicate with other devices which can be in the common household. The author [8] The Integrated Alarm Systems are defined as systems having a one or more common devices at least one of which is an alarm application. Integration can be divided into the Hardware and Software. For purposes of this research, the Software integration was chosen. The author [8] also mentioned that “software integration methods are based on linking separate applications via a communication bus, and their control, management, visualization is providing software products, which are installed on an external computer or at unattended control centers equipped with the

necessary software.” Each external device can be connected to designed CIE via the Ethernet connection which is situated on the side of the Main-board.

The system can also be extended by the Arduino relay module. This module can be used as a hardware integration to control other connected electronic devices. The author [8] also mentioned that the hardware integration also includes the use of automation systems (eg. intelligent wiring system), which in addition to standard control of technologies for buildings (lighting, heating, air conditioning, blinds, irrigation, sound, etc.) offers the ability to connect security devices (detectors, hold-up devices, control and indicating equipment IAS etc.).

Zone-Board only detects the intruder by the connected alarm detectors. The alarm message is then sent to the Main-Board which the evaluates the received message. The final alarm triggering depends on the internal conditions in the program. These conditions are based on the zones, time, and the arming. All information must be imported into the system, and it should be changed by the user. The system also consists of the Ethernet connection which allows creating the web sides. The setting can be changed by the user, or it can be changed by the certificated person via the Ethernet connection. The Ethernet connection can also be used for transmitting the alarm message to the Alarm Receiving Center (ARC).

3 The design of security for the kindergartens

For reduce the risk to an acceptable level, it is necessary to secure the kindergarten. As can be seen in figure 2, security could be separated into three main categories. The best option of security is to compound all these categories.

To ensure physical security may be used private security services or trained employees. It is appropriate to prepare procedure “Response in a crisis situation” for employees. The employees should be trained in the procedure.

It is appropriate to use the IAS elements, in the category of electronic devices. Especially, elements for perimeter and building shell should be used. For example, magnetic detectors, glass break detectors or motion detectors. It is advisable to connect these elements to ARC, which will evaluate and respond to any alarms. A good choice is also to install an access system.

CCTV must not be forgotten. For passive use, CCTV can be installed as a recording device or deterrent element. For active use, CCTV can be installed as a device for online monitoring. Software like a detect suspicious behavior or facial recognition is very suitable.

Fig. 2 Combination of security categories.

Finally, the last category of security is mechanical devices. Security doors that reduce the possibility of unauthorized entry can be used to secure kindergarten. Furthermore, it is advisable to install bullet resistant windows or foils. In the case of the small budget, security foils can be installed.

Conclusion

This paper deals with the fact that most of the terrorist attacks that occurred in Europe were aimed at so-called Soft Targets. Moreover, some attacks were focused on kindergartens recently. Therefore, the design of security for the kindergartens was performed. Considering that every kindergarten is unique, the design of security is solved by recommendations form. The recommendations were focused on the combination of three main security categories - Security personnel, Electronic devices, and Mechanical devices. Especially the IAS was described in detail. One of the challenges for future research is to develop some new security technologies.

Acknowledgement: This work was supported by the Internal Grant Agency of Tomas Bata University under the project No. IGA/FAI/2019/003.

References

1. M. Zineddin & L. Sherwood, WIT TTBE, (2013)
2. P. Beňová, Š. Hošková - Mayerová, J. Navrátil, JSSI (2019)
3. D. Lapkova, L. Kotek and L. Kralik, 29TH DAAAM (2018)
4. L. Figuli, Z. Kubíková and M. Ivančo, IDCS 17(1-A), (2019)
5. Z. Kalvach, G. (2016)
6. L. Jiang, Ch. Jun, M. Jun. 9th Int. Conf. on Measur. Tech. and Mech. Aut. (2017)
7. Chen, Song-Shyong, Luke K. Wang, Wei-Hsuan Li, and Wen-Ping Chen. ICAMSE, (2016)
8. J. Valouch. App. Mech. and Mat. (2015)

9. M. Shariqsuhail, G. Viswanathareddy, G. Rambabu, C. V. R. Dharmasavarni, and V. K. Mittal. ICACCI, (2016)
10. M. Pospisilik, T. Smekal, M. Adamek, P. Neumann, T. Dulik. MATEC Web of Conf. (2016)