BRNO UNIVERSITY OF TECHNOLOGY
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ

DEPARTMENT OF FOREIGN LANGUAGES
ÚSTAV JAZYKŮ

ELECTRONIC SECURITY SYSTEMS
ELEKTRONICKÉ ZABEZPEČOVACÍ SYSTÉMY

BACHELOR'S THESIS
BAKALÁŘSKÁ PRÁCE

AUTHOR — **Dominik Tomek**
AUTOR PRÁCE

SUPERVISOR — **Mgr. Šárka Rujbrová**
VEDOUCÍ PRÁCE

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Angličtina v elektrotechnice a informatice**
Ústav jazyků

Student: Dominik Tomek ***ID:*** 173603
Ročník: 3 ***Akademický rok:*** 2016/17

NÁZEV TÉMATU:

Elektronické zabezpečovací systémy

POKYNY PRO VYPRACOVÁNÍ:

Vytvořte přehled moderních elektronických zabezpečovacích systémů, popište zakladní principy jejich fungování, uveďte, jaké jsou jejich výhody a nevýhody. Proveďte závěrečné shrnutí.

DOPORUČENÁ LITERATURA:

[1] Pearson, R. Electronic Security Systems. 1st ed. Burlington, MA: Butterworth-Heinemann, 2007.

[2] Garcia, M. L. Design and Evaluation of Physical Protection Systems. 2nd ed. Burlington, MA: Butterworth-Heinemann, 2008.

[3] Burda, K., Strašil, I. Zabezpečovací systémy. Brno: Vysoké učení technické v Brně, 2012.

[4] Lukáš, L. a kol. Bezpečnostní technologie, systémy a management I. Zlín: VeRBuM, 2011.

[5] Křeček, S. Příručka zabezpečovací techniky. Blatná: Blatenská tiskárna, 2003.

Termín zadání: 9.2.2017 ***Termín odevzdání:*** 2.6.2017

Vedoucí práce: Mgr. Šárka Rujbrová
Konzultant:

doc. PhDr. Milena Krhutová, Ph.D.
předseda oborové rady

ABSTRACT

The aim of this thesis is to give the reader basic understanding of the most common electronic security systems. The fundamental principles, characteristics and applications of modern electronic security systems used in homes and corporate environment are covered in this work. Moreover, it compares the security devices that are used in the systems and demonstrate their advantages and disadvantages. This work is suitable for students, individuals that want to start working in this field, or for those just interested in the topic.

KEYWORDS

Electronic security systems, physical security, access control, alarm systems, video surveillance systems

ABSTRAKT

Cílem této práce je seznámit čtenáře s nejběžněji používanými elektronickými zabezpečovacími systémy. Práce popisuje základní principy, vlastnosti a využití moderních elektronických zabezpečovacích systémů používaných v domácnostech a firmách. Dále práce porovnává jednotlivá zabezpečovací zařízení, která se v těchto systémech používají a uvádí jejich výhody a nevýhody. Tento dokument je vhodný pro studenty a osoby, které chtějí začít pracovat v tomto oboru nebo je tato problematika pouze zajímá.

KLÍČOVÁ SLOVA

Elektronické zabezpečovací systémy, fyzická bezpečnost, řízení přístupu, alarmové systémy, bezpečnostní kamerové systémy

TOMEK, D. *Elektronické zabezpečovací systémy*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav jazyků, 2016. 32 s. Bakalářská práce. Vedoucí práce: Mgr. Šárka Rujbrová. Odborný konzultant: doc. Ing. Karel Burda, CSc.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma Elektronické zabezpečovací systémy jsem vypracoval samostatně pod vedením vedoucího a odborného konzultanta bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne ....

(podpis autora)

ACKNOWLEDGMENT

I would like to thank my thesis supervisor Mgr. Šárka Rujbrová for her help and support while writing my bachelor thesis. I would also like to thank doc. Ing. Karel Burda, CSc. for his advice and consultancy.

CONTENTS

LIST OF FIGURES

INTRODUCTION

Security is one of the most important factors in our lives. We need security for our survival in society and we desire it for our well-being. Since we are creative beings we invented many security systems that help us achieve security. However, only in recent decades with the help of electricity we were able to design electronic security systems that can operate automatically and more reliably.

The electronic security systems are a substantial section in the field of physical security, next to the other security elements, such as guards, barriers and mechanical locks. Their primary function is to protect lives, property and information against criminals and natural hazards. Generally, an electronic security system is an electronic device or a set of devices operating together in order to provide a desired protection.

An example of the electronic security system is an electronic access control system which is the topic of the first chapter. The main focus of this chapter is on access control readers as the key electronic components of the systems. The second chapter covers electronic alarm systems which is furthermore divided into two subchapters, fire alarm systems and intrusion alarm systems. The fire alarm systems include two fundamental types of fire detectors, heat sensors and smoke sensors. Most of the intrusion alarm systems subchapter is focused on intrusion sensors since the sensors are the essential electronic elements of the systems. The final chapter primarily deals with different types of video surveillance systems. Each chapter begins with general information about the systems and then proceeds by describing each system in details.

1 ACCESS CONTROL SYSTEMS

The access control, also referred to as entry control, is one of the key elements of the physical security. Its main purpose is to limit the access for the authorized personnel only. The access can be limited for instance to a building, an area or a device containing some assets. In order to prevent an unauthorized person from entering, turnstiles or mantraps can be placed at the entrance as part of the access control system.

Mechanical keys and locks have been used for entry control for hundreds of years. However, they have some major drawbacks for which they are becoming obsolete. One of the disadvantages is that standard keys can be easily duplicated. Another disadvantage is that if a key is lost or stolen the lock must be rekeyed.

All these problems are solved with modern electronic access control systems. In case of an electronic access control system, the key represents a card, a PIN, or a biometric feature that are very difficult to duplicate. An electronic access control system can be easily configured without replacing any physical parts. Beside its main function, which is to allow only authorized personnel to enter, an electronic access control system can also be used to track the attendance of employees.

An electronic access control system for buildings commonly consists of five essential elements: an electric or magnetic lock, a door contact, a reader, an access control panel and a credential. The function of an electric or a magnetic lock is to release a door or open an entrance point if access is granted. The door contact detects whether the door is closed or opened. The reader reads an input credential which can be a card number, a PIN or a biometric pattern. The access control panel controls all the other elements. In addition to the five elements, an exit button can be added to the system to provide an option to request an exit.

The working principle of an electronic access control system differs based on the operation of the reader. The readers can be divided into four distinct categories:

- Non-intelligent readers
- Semi-intelligent readers

- Intelligent readers
- IP readers

In case of a non-intelligent reader, the reader just reads a credential and forwards it to an access control panel (see Figure 1). The access control panel compares the credential to an access control list and decides whether to grant or deny access. If the access is granted, the access control panel releases the lock.

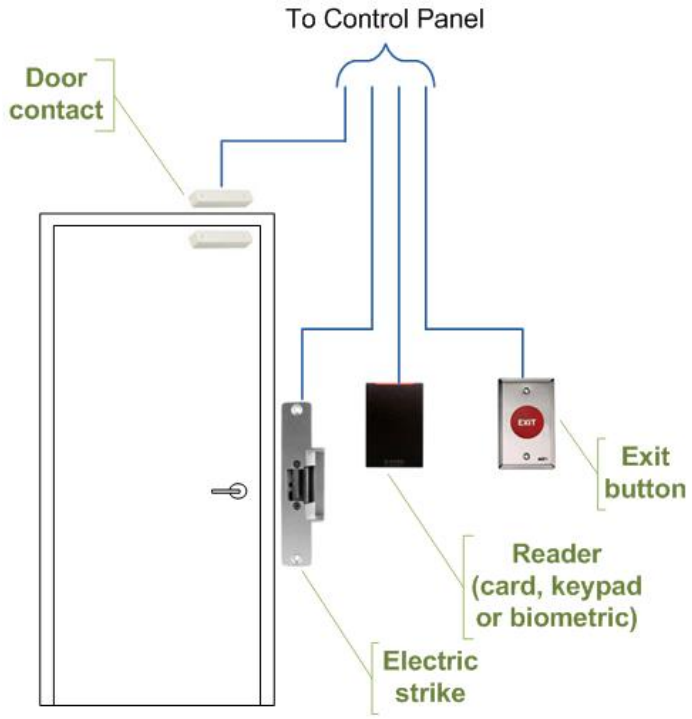

Figure 1 Access control system with a non-intelligent reader

The semi-intelligent reader is very similar to the non-intelligent readers. In addition to the non-intelligent reader, the semi-intelligent reader has the ability to control the lock. The reader sends the input credentials to the access control panel for verification. If the access control panel authorizes the access, the reader releases the lock.

The intelligent reader is able to make a decision without the access control panel. An access control list is stored in the reader. The access control list is regularly updated with the information from the access control panel. When a credential is inputted, the reader can grant the access and release the lock by itself (see Figure 2). The information about the access is sent to the access control panel for a record. If the intelligent reader has its

own power supply (battery), this type of reader can be very useful if there is a blackout or the connection to the access control panel is interrupted.

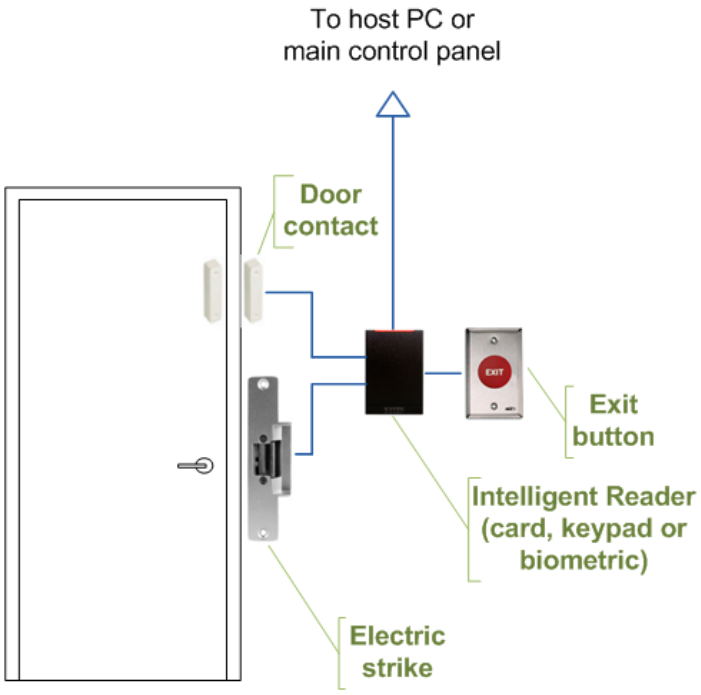

Figure 2 Access control system with an intelligent reader

The IP (internet protocol) reader is type of reader that can be connected to an existing computer network. This type of reader does not require to be connected to an access control panel because it is able to operate by itself. A computer connected to the network can be used to manage the IP reader. The inputted credential is processed by the reader and if the reader grants access, it sends a signal to release the lock. The IP readers usually have a battery to operate during a power outage. Some of the modern IP readers also support PoE (Power over Ethernet), this allows the readers to be powered using the Ethernet cable which is used for communication in the network without the need for a separate power cable.

1.1 Access Control Readers

An access control reader is a key electronic element of any access control system. There are many types of access control readers available nowadays. The appropriate reader

should be chosen based on the specific environment, costs, level of security required, and preferences of the users.

The access control readers can be classified by the credentials being inputted. In order to verify a person, it can be used something the person physically has (e.g. a card), something the person knows (e.g. a PIN) or something the person is i.e. a biometric measurement (e.g. a fingerprint). Therefore, the reader can be either a card reader, PIN reader or a biometric reader.

1.1.1 Card Readers

Card readers use a physical object which stores a unique credential number in digital form to establish identity of an individual. The object is commonly a card but it can also be in the form of a key fob. It can also differ in distance in which it communicates with the reader. Nevertheless, most of the cards are contactless nowadays. The card readers are easy to use but they have also many disadvantages. A physical card can be easily lost, damaged, stolen or passed on to an unauthorized person. This is not only a security risk, but it can be very costly as well. Two most common types of cards used for access control today are proximity cards and contact-less smart cards.

The proximity cards use the radio frequency at 125kHz for their operation. They can be either passive or active. However, most of the proximity cards used nowadays are passive. The passive cards have a capacitor built-in which charges using radio frequency energy generated by the card reader. The energy activates a chip inside the card which sends stored data to the reader. The active cards are in addition equipped with a long-life battery. The advantage of the active cards is that they can communicate with the reader at greater distance. Even though the proximity cards are resistant to most environmental issues, such as rain and frost, they can be damaged by high levels of electromagnetic fields. The proximity cards are used for example in parking areas. In this case, the gate opens as soon as the driver reaches a specific distance from the gate.

The contact-less smart cards are similar to proximity cards. However, they use radio frequency at 13.56 mHz and they are capable of storing more data and processing it. The benefit of this technology is that one card can be used for multiple purposes.

1.1.2 PIN Readers

This type of reader uses a PIN (personal identification number) which is typed on a keypad to verify identity of an individual. The PIN is typically a 4-6-digit number. The PIN reader can be more secure than the card readers if used properly because there is no physical object that could be stolen or lost. However, even the PIN reader is not a perfect access control solution.

The most common problem with PIN readers is that the authorized person might forget or pass the PIN required for the entry to an unauthorized person. The PIN can also be observed while typing or guessed if it is too easy and common (e.g. 1234) or if it relates to a publicly known information about the person, such as a birthday or a phone number. In order to reduce the risk of guessing the PIN some systems are configured to allow only a limited number of attempts per a time period. Another problem might occur if the authorized person writes the PIN on a piece of paper. This can be a serious security threat for the organization. In order to avoid such problems proper security training of the staff using the PIN reader should be held.

1.1.3 Biometric Readers

The biometric readers recognize specific features of the human body that are unique to an individual and compare them against templates stored in a database. If a match is found, the access is granted. Although the biometric readers are generally considered as more secure and easier to use than PIN and card readers because there is nothing the person has to remember or wear, in areas where high level of security is not the primary concern and fast throughput is required a card reader might be a more effective solution. Since some of the biometric readers are not always perfectly precise, it is worth considering a system with two or more step verification to increase overall security of the system. For example, systems with a fingerprint and PIN reader are commonly installed.

When we consider the precision of the biometric reader, two types of errors may occur. Either the access granted to a person that does not have the valid credential, which is called false accept. This may happen when the precision of the reader is configured to a very low value. The second type is false reject, which means that access was rejected to a person with a valid credential and it may be caused when precision of the reader is set

to a very high value. Although the false accept might be absolutely unacceptable for some institutions, the precision cannot be too high because the other scenario could occur which might be undesirable as well. Therefore, this trade-off should be balanced based on the security requirements.

There are many types of biometric readers nowadays. One of the most common is a fingerprint reader which detects unique patterns of a fingerprint (see Figure 3). Most of the readers use fingerprint ridge endings and bifurcations for the verification. The major benefits of the fingerprint readers are that they are relatively inexpensive and precise. One of the main drawbacks of a fingerprint reader is that its use is highly unhygienic especially if many people are using the same device. Another disadvantage of using a fingerprint reader is that there might be a problem with the reading if the finger is damaged or dirty. This problem might be overcome by scanning multiple fingers. In order to avoid bypassing the system with a synthetic finger, some readers measure the temperature to verify that the finger belongs to a living being.

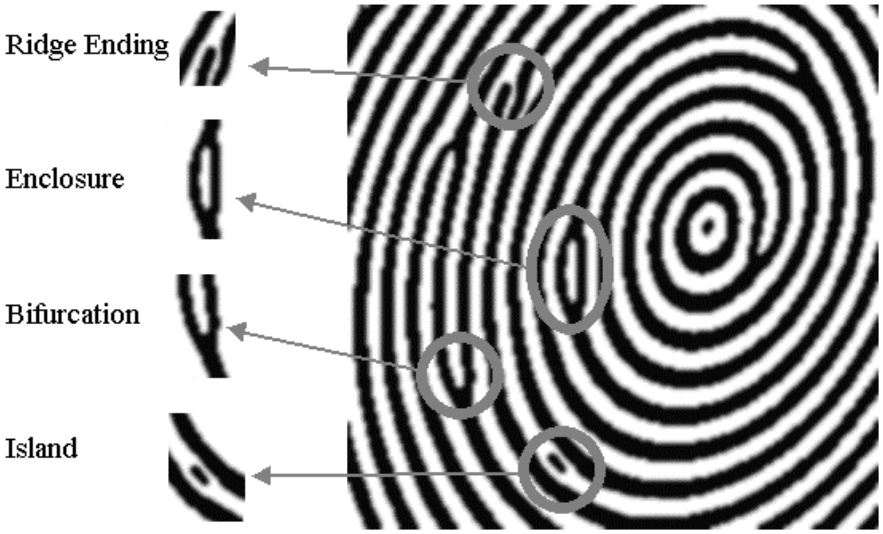

Figure 3 Ridge characteristics of a fingerprint

Similarly to the finger, palm of a hand can also be used for access verification. A palm reader scans the palm of a hand for distinct characteristics unique to an individual. Disadvantages of the palm reader are that it takes a lot of space and as the fingerprint reader it is highly unhygienic and it might have some problem with the reading if the palm is damaged of dirty.

Another type of reader that requires a hand for verification is a hand geometry reader (see Figure 4). This reader scans geometrics of a hand, such as proportions of the hand, curvature, fingers' widths and lengths. It is based on a 3D picture of the hand using a camera and a mirror.

Figure 4 Access control system with a hand geometry reader

Another type of biometric readers are facial readers. The facial readers have a camera built-in to capture an image of a face. In order to verify identity, the readers detect distinguishing facial characteristics. Most of them use especially characteristics that are relatively fixed over long period of time, such as cheekbones, the distance between the eyes, and upper outlines of eye sockets. The camera can also be used to take a picture of the person and keep it for a record. The key strength of this reader lies in its very convenient usability because there is no physical contact with the device. These readers are suitable even for a dusty or dirty working environment where other types of readers could cause problems. The face recognition is also used in video surveillance systems which are covered in the chapter 3. Some of the early readers could be bypassed using a photo of an authorized individual. One way to solve this problem is by adding another camera to create a three-dimensional image of the face.

Less common and relatively expensive is an iris reader which scans unique patterns in the iris of an eye. It can measure pits, striations and furrows of the iris. The reader is equipped with a black and white high resolution camera that takes a picture of the iris for identification.

The retina of the eye can also be used as biometrics for identity verification. This technology uses infrared scanning to obtain the vascular pattern.

Relatively new and fast growing concept in the field of access control is behavioral biometrics. As the name suggests, it measures specific behavioral characteristics to establish identity of an individual. Since the actions we perform are unique in a certain pattern, we can measure them to create a template which can be then used for the identification.

Some examples of behavioral characteristics are keystroke dynamics and cursor movements. The main benefit of using these behavioral patterns for verification is that they usually do not require any additional hardware which makes the technology more affordable than conventional readers. If a keyboard, a mouse, or a touchpad is present, the only thing needed is a software that processes and evaluates the behavioral characteristics. Another advantage of such behavioral verification is that it may run even without the knowledge of the individual being scanned. As the result, the authorized individual is not being distracted and the attacker might not be aware of the security system. For instance, keystroke dynamics verification can be used as another security layer in combination with a PIN verification.

Another example of behavioral biometrics is a signature verification reader. Since the signature of individuals is unique it can be used for authentication as well. The reader is equipped with a sensitive tablet or a sensitive pen which measures signature writing parameters, such as shape, motion, speed, and pressure.

Voice can also be used as biometric feature for identification. Speech measurements, such as waveform envelope, relative amplitude spectrum, voice pitch period, and resonant frequencies of the vocal tract are used for verification of identity. The major advantage of this method is that it can be used remotely without any additional hardware, for example over an existing telephone line. However, voice recognition is currently not considered as reliable and should be used only for low level security applications.

Furthermore, there might be a problem with the verification if the voice changes due to sickness.

Biometrics is a booming field in the security industry. Some of the new methods to establish identity are readers that recognize vein patterns of an eye and readers using heartbeat.

For facilities where high level of security is required, multi-biometric systems are a great solution to improve security. Multi-biometric systems consist of multiple biometric readers for authentication. An example of a multi-biometric system is a reader with fingerprint and facial recognition.

2 ALARM SYSTEMS

An alarm system is a set of interconnected devices used to protect property or lives by providing a response to a danger, such as fire break out or thief intrusion. The response of the system can be either warning the residents about the hazard or triggering an action that will solve it, such as automatic fire suppression. The electronic alarm systems covered in this chapter are used for home as well as corporate applications.

The main components of a typical alarm system are a control panel, sensors, alerting devices and a keypad. The control panel is the central element that communicates with all the components in the system. The connection with the control panel is either wired or wireless. The sensors detect a specific predefined activity that leads to an alarm situation, such as glass breakage or sudden rise of temperature, and report it to the control panel. The alerting devices, such as bells, sirens and flashing lights can be activated by the control panel and serve to warn the residents about an emergency. An additional effect of the alerting devices in the case of an intrusion alarm systems might be to scare off the intruder which could force the intruder to cancel the intrusion. The keypad is a device which allows the user to manage the alarm system.

Two most common alarm systems are fire alarm systems and intrusion alarm systems. They can be used individually or some complex alarm systems include both the fire and intrusion protection. The presence of these systems can be optionally accompanied by a video surveillance system to ensure that a backup security protection is present in case of alarm system failure or to enhance the overall security of the system.

2.1 Fire Alarm Systems

Fire alarm systems are used to detect and react to a fire when it breaks out in a facility. The fire can be typically caused for instance by an electronic device failure, faulty wiring or carelessly discarded lighted ends of cigarettes. The fire alarm systems are used in almost all types of buildings, especially in areas with high likelihood of fire, such as restaurants, warehouses and industrial buildings.

The basic working principle of a fire alarm system is a straightforward step-by-step process. When a fire occurs, the sensors automatically detect it and inform the control panel. If the sensors do not detect the fire, the control panel can be informed using a manual call point or a pull station. The control panel then reacts to the situation by triggering the alarming or fire extinguishing devices, usually both if they are present. In order to detect the fire, smoke or heat sensors are typically used.

2.1.1 Smoke Sensors

Two most common smoke sensors are photoelectric smoke detectors and ionization smoke detectors. Photoelectric smoke detector can be either light scattering or light obscuration type. In both cases, there is a light source (Light-Emitting Diode) and a light sensitive device (photosensitive diode).

The working principle of a light scattering type of photoelectric sensor is based on reflection of the light by combustion particles to the light sensitive device (see Figure 5). As the number of particles increases, more light is reflected. If enough light hits the detector, the current starts to flow which will trigger an alarm.

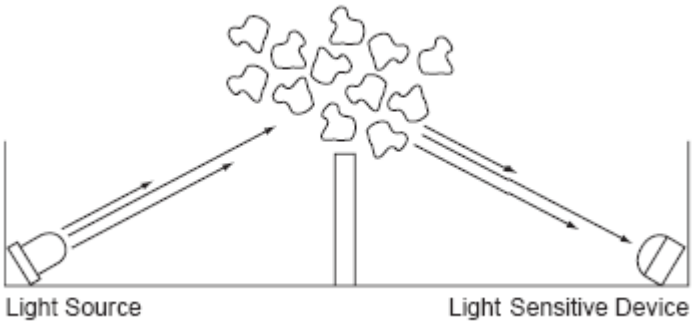

Figure 5 Light scattering photoelectric sensor reader

The light obscuration type of photoelectric sensor is similar, only the fundamental working principle is opposite. This time the devices face each other (see Figure 6). The alarm condition occurs when the current decrease on the receiver which is caused by particles of combustion entering the chamber and blocking the light to pass through.

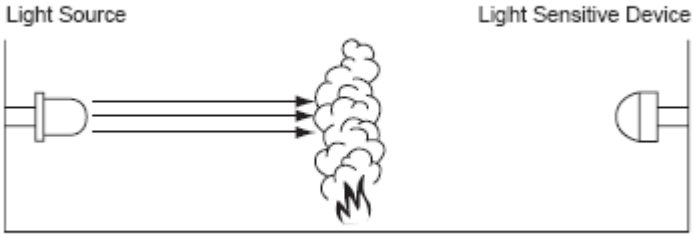

Figure 6 Light obscuration photoelectric sensor

The ionization smoke detector is composed of two charged plates and a small radioactive element that emits ions into the air (see Figure 7). The ions are attracted to the plates which causes the current to flow. This flow is reduced when smoke particles enter the chamber because they attach themselves to the ions. If the current flow drops under a certain level, an alarm is triggered.

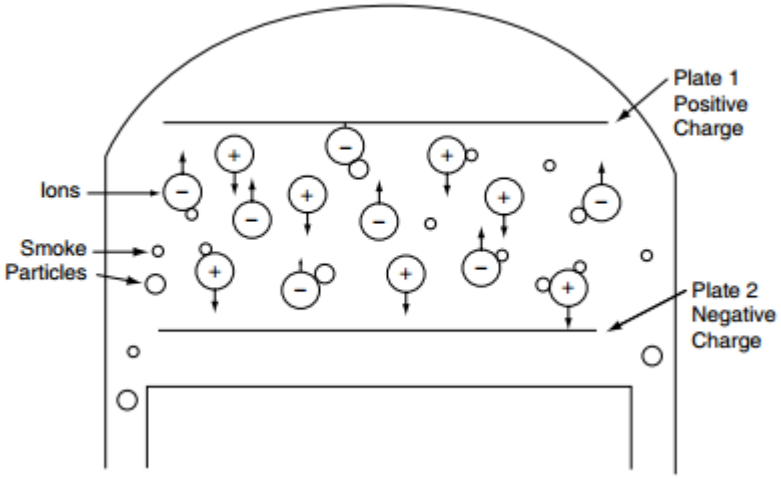

Figure 7 Ionization smoke detector

2.1.2 Heat Sensors

Heat sensors are used to detect a high temperature or sudden rise in temperature. They are suitable for places where smoke is present on regular basis but it is not fire related (e.g. kitchen). The heat sensor can be fixed temperature detector, rate-of-rise heat detector, or both in one device.

The fixed temperature type of detector triggers an alarm when the temperature exceeds a value which is typically 135 °F (57 °C). The sensor contains a spring that places tension on a plunger (see Figure 8). The plunger is held in place using a solder which melts at a fixed temperature. When the solder is melted, the plunger is pushed by the spring to connect the alarm contacts which turns the alarm on. Since the solder is melted after its operation it cannot be reused and must be replaced.

The other type of heat sensor is rate-of-rise heat detector which can react more quickly than the fixed temperature detector and does not have to be replaced after its usage. Here the contacts initiating the alarm can be connected by a diafram (see Figure 8). The diafram is swelled if the temperature in the chamber rises faster than the vent will allow the air to escape.

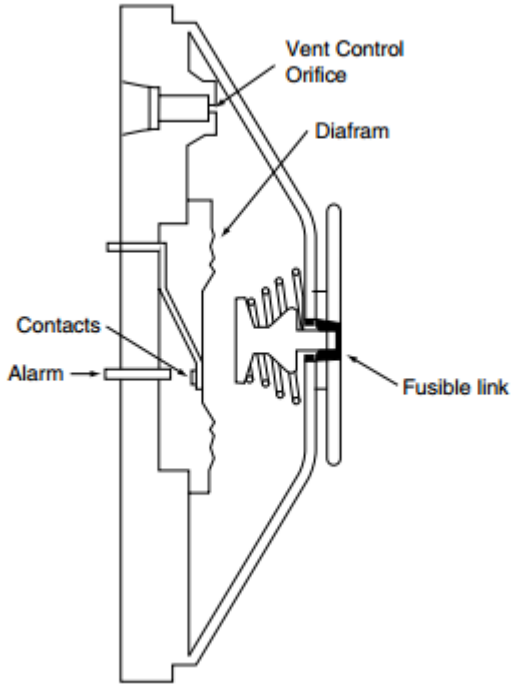

Figure 8 Fixed temperature and rate-of-rise heat sensor

2.2 Intrusion Alarm Systems

The aim of an intrusion alarm system is to trigger an alarm when an intrusion occurs. These systems are primarily used in high level security buildings to protect valuable assets

that could be potentially stolen, for instance in banks, galleries or jewelry stores. Another use of these systems is common in houses and commercial buildings located in high criminal rate areas.

An electronic intrusion alarm system works by detecting an intruder using a sensor, typically a motion sensor or a door/window sensor. The sensor then informs the control panel which triggers the alarming devices (e.g. bells, horns, sirens, speakers, sounders, strobe lights). In addition, some control panels can also be configured to send a notification about the intrusion to the owner or police. In some places security video cameras are installed to verify the intrusion before security personnel are deployed.

2.2.1 Intrusion Sensors

Intrusion sensors are devices used in intrusion alarm systems to detect presence of an intruder. The presence can be detected as changes in the environment caused by the intruder. There are many types of intrusion sensors, they may differ in the environment that operate, event that activates them and technology they use. This chapter covers both interior and exterior sensors.

According to Garcia (2007) the electronic intrusion sensors can be classified based on the following characteristics:

- passive or active
- covert or visible
- line-of-sight or terrain-following
- volumetric or line detection
- application

Passive sensors differ from the active sensors in the way they use energy for detection. The passive sensors use energy emitted directly by the intruder (e.g. heat, sound or mechanical energy) or a change of energy in the environment triggered by the presence of the intruder (e.g. a change in electric or magnetic field). Active sensors on the other hand have a transmitter which transmit an energy to a receiver. The receiver detects the intruder by a change in the transmitted energy caused by the intruder. Infrared, microwave, and other radio frequency devices are used for this purpose. The main advantage of the passive sensors is that they are more difficult to detect by the intruder

because they do not emit any energy. However, the active sensors are generally more reliable because the signal is stronger. Active sensors should not be used in areas with some explosive materials because the emitted energy could potentially initiate an explosion.

Covert sensors are hidden while the visible sensors are in plain view. The covert sensors can be hidden for example in the ground which makes them for the intruder harder to detect. But on the other hand, when the sensor is visible it may prevent the intruder from acting. Hidden sensors do not affect the appearance of the environment but they are usually more complicated to install and maintain than the visible ones.

Line-of-sight (LOS) sensors are capable of detecting only when there is an unobstructed path between the transmitter and receiver. Therefore, the terrain must be either flat or adjusted. On the other hand, terrain-following sensors achieve the same detection result on any terrain.

Volumetric sensors use a volume of space to detect an intrusion. This volume is typically difficult to identify. On the contrary, line detection sensors use a very narrow area for the detection (e.g. fence, wall, door, window) which is generally easier to identify.

From the applicational point of view, sensors can be classified according to the physical space where they operate. In case of exterior sensors, it can be ground, a fence or freestanding on a support in free space. While interior sensors detect either penetration of the boundary to an area or motion within the area.

Boundary-penetration vibration sensors are passive line sensors that detect vibration frequencies of a surface caused by sudden impact on the surface. An example of this type of sensors is a glass-break sensor which detects the vibration frequencies when the glass is broken. These sensors can be either visible or hidden.

Electromechanical sensors are characterized as passive, visible, line sensors. They are typically used on doors or windows. Most of these sensors use a magnetic switch. When a door is closed, magnetic field closes the switch. This type of sensors triggers an alarm when a magnetic switch opens which can be caused for example by opening a door by an intruder.

Infrasonic sensors are passive sensors that are capable of detecting pressure changes in the volume in which they operate. For example, this change in pressure can be caused by opening or closing a door. These sensors are suitable for areas which are not accessed on regular basis.

Ultrasonic sensors are visible, active, volumetric type of sensors which uses acoustic spectrum usually in the frequency range between 19 and 40 kHz. The sensors detect a change in the signal received from the signal transmitted (see Figure 9). This change is caused by an object moving in the detection zone.

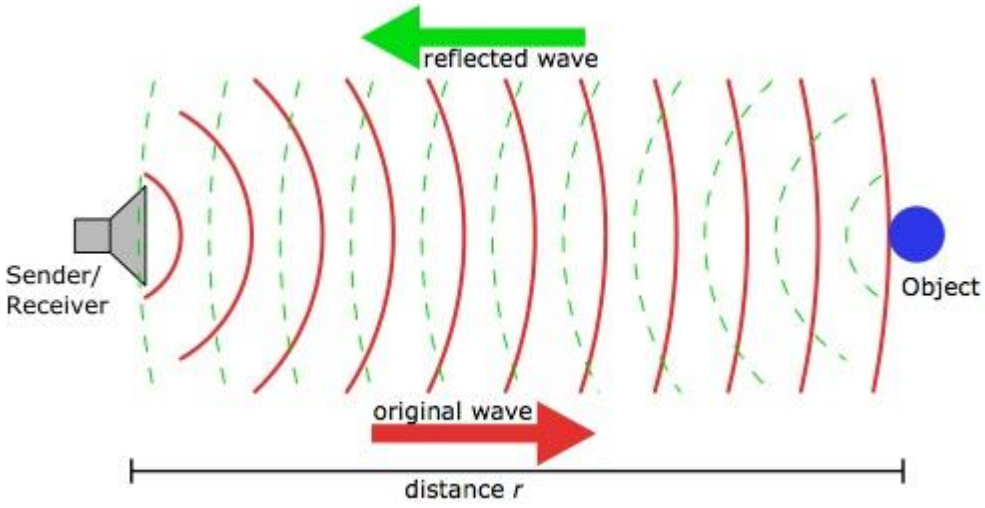

Figure 9 The working principle of an ultrasonic sensor

Active sonic sensors are visible, volumetric sensors working in the acoustic spectrum at frequencies of 500-1000 Hz. This type of sensors can achieve very good reflections because of the low frequency.

Passive sonic sensors are volumetric, covert sensors that operate by using a microphone that listen to the sounds in the area. The alarm is triggered if the sound parameters correspond to an intrusion.

Interior pressure sensors are passive, covert line detectors, often in the form of mats hidden underneath an object. These sensors trigger an alarm when an amount of pressure makes electrical contact over the metal strips inside the device.

Exterior pressure or seismic sensors are one of the types of sensors that are buried in

the ground. They are passive, covert, terrain-following sensors. These sensors are capable of detecting an intruder who walks, runs, or jumps on the ground. They do it by responding to disturbances of the soil, such as vibrations or change in pressure. Typically, the pressure sensors can sense lower frequency pressure waves while the seismic sensors detect higher frequency vibration.

Magnetic field sensors are another type of sensors that are buried in the ground, also belonging to the category of passive, covert, and terrain-following sensors. They work by reacting to a change in the magnetic field. This change can be caused by any ferromagnetic object, for example a vehicle or a weapon. It means that this type of sensors is not able to detect an intruder who is not equipped with any metal object. They are most commonly used to detect vehicles.

Another type of sensors buried in the ground are ported coaxial cable sensors, also known as leaky coax or radiating cable sensors. These sensors are active, covert, and terrain-following sensors. They detect a motion of an object with a high conductivity or high dielectric constant near the cables. The object might be for instance the human body or a metal vehicle.

Fiber-optic cable sensors are passive line sensors. Outdoor sensors are buried in the ground and usually woven into a grid. This type of sensor uses optical fibers, transparent fibers from glass or plastic, through which the light passes. These fibers are very sensitive to a change in shape. When an intruder steps on the ground above the fiber, the fiber bends which activates an alarm.

Fence-disturbance sensors are fence-associated sensors, usually installed on a security fence with chain-link mesh. They are passive, visible, terrain-following type of sensors. In order to detect an intruder, the sensors respond to disturbances of the fence, such as climbing or cutting on the fence. Transducers, such as switches, electromechanical transducers, geophones, strain-sensitive cables, fiber-optic cables, or electric cables are used to detect the movement or vibration of the fence.

Sensor fences categorize as passive, visible, terrain-following sensors. Their main purpose is to detect an intruder climbing or cutting on the fence. These sensor fences are composed of transducer elements which detect a deflection of wires on the fence.

Exterior electric field or capacitance sensors are active, visible, terrain-following

sensors. These sensors can be either freestanding or associated with a security fence. The working principle of this type of sensors is based on detecting a change in capacitive coupling among a set of wires attached to a fence. The wires are electrically isolated from the fence. The detection area of electric field sensors extends up to 1m beyond the wires. The electric field sensors require proper electrical grounding to avoid nuisance alarms. Both types of sensors are susceptible to rain, lightning, fence motion, and small animals.

Active infrared (IR) sensors are active, visible line sensors. The sensors operate by transmitting an IR beam emitted by diode to the receiver (see Figure 10). If the beam is broken the alarm is raised. In order to increase security, multiple-beam sensors are used because they are not as easy to bypass as single-beam sensors. The beam can be reflected using mirrors to form more complex patterns. Nuisance alarm can be caused by reduced atmospheric visibility (e.g. fog, snow, rain) or vegetation, such as grass.

Passive infrared (PIR) sensors detect thermal energy emitted by the human body. They work best when the background has much different temperature than the intruder. These detectors can sense an intruder moving through the detector field of view as well as large objects that generate heat, such as vehicles. The sensors are used for both interior and exterior applications.

Capacitance proximity sensors are covert line, active sensors that can detect an intruder approaching or touching a metal object.

Bistatic microwave sensors are classified as active, visible, volumetric type of sensors. The detection system is composed of two microwave antennas. One is the transmitter and the other is the receiver of microwave energy (see Figure 10). It detects changes in the transmitted microwave beam which is caused by an intruder moving in the area between the antennas. Vegetation in the area should not be higher than 1-2 inches to avoid nuisance alarms.

Monostatic microwave sensors, on the other hand, use only single antenna which acts as the transmitter and receiver at the same time. They work by detecting changes in the reflected microwave energy caused by an intruder entering the detection zone. Monostatic microwave sensors are primarily used for interior application. The fundamental working principle is similar to the principle of ultrasonic sensor (see Figure 9).

Another way to detect an intruder is using a video motion detector (VMD). The video motion detector is a passive sensor which can be used indoor as well as outdoor. The sensor processes the video signal from a video camera to detect an intruder. It senses changes in the video brightness level. However, this type of sensors requires enough light for its operation.

Some of the detectors used in practice are dual technology which means that they use two different technologies to detect the same action, a common example is a motion detector with combination of infrared and microwave technology (see Figure 10). This provides additional layer of security as both technologies complement each other and significantly helps to avoid nuisance alarms.

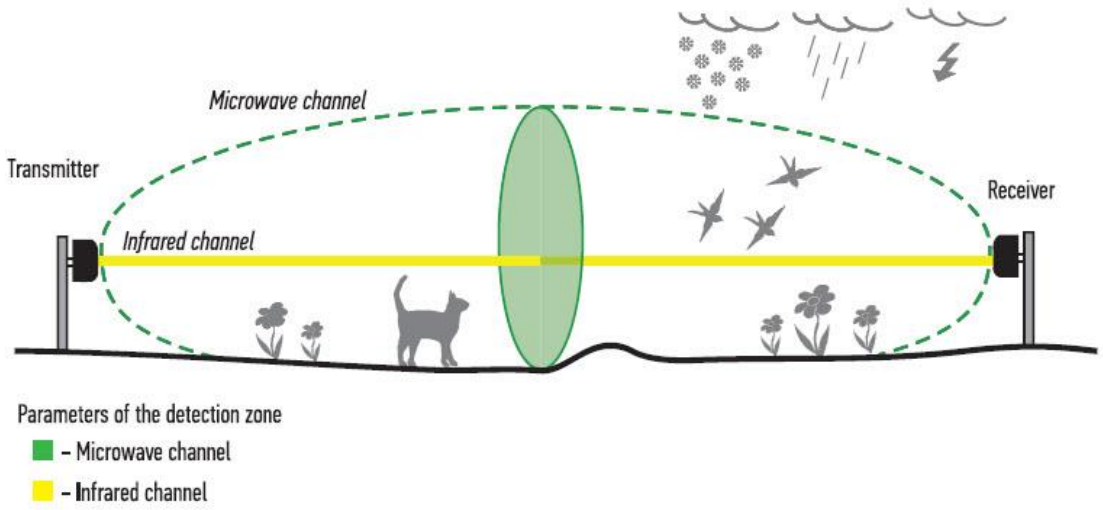

Figure 10 Dual technology (bistatic microwave and active infrared) sensor

It is a good idea, especially in case of the exterior sensors, to use a video camera that monitors the area in order to inspect for an intrusion without the need to go there in case of an alarm situation. The security cameras are discussed in details in the next chapter.

3 VIDEO SURVEILLANCE SYSTEMS

Video surveillance plays an important role in the physical security. A video surveillance system, also known as a CCTV (closed-circuit television), is a combination of hardware and software to monitor an area. In the physical security, the main purpose of the video surveillance systems is to prevent and record criminal activities or other types of hazards, such as natural or technical accidents. Besides, the video surveillance systems can also be used as a video baby monitor or to keep an eye on an elderly family member or a pet. The security surveillance systems are primarily used in places with high concentration of people, such as airports and rail stations, or in facilities that require high level of security, such as military bases and banks.

A video surveillance system can be installed individually or it might be combined with some other security system, such as access control or alarm system, to provide an additional layer of security. For example, an advanced video surveillance system equipped with a face recognition system can also serve as an access control system.

The video is either monitored in real-time or it is recorded and stored for a later use or both simultaneously. In case of a real-time video surveillance, the video is usually watched by an operator who can immediately respond to an undesirable activity. Some of the modern video surveillance systems are able to detect a suspicious activity even without any human intervention and notify a security person or trigger an alarm. If the video is stored for a record, it can be accessed later to prove an evidence to the police.

Since the recorded videos usually require a large amount of storage space, especially in surveillance systems consisting of many video cameras recording high quality videos, some of the video cameras have the ability to record video only in a specified time of the day or only if an action is detected which can significantly save the storage space.

Since there is a growing use of surveillance systems, privacy is becoming a big issue. Surveillance systems should not be installed in places where certain degree of privacy is expected, such as toilets, bathrooms and bedrooms. In many cities around the world, the security cameras are placed on almost every corner to survey the citizens. The city of Chicago for example, has a large surveillance network with over 22,000 cameras which

makes the city the most surveilled city in the United States (Polygon, 2013). Some people accept the surveillance to be protected while others consider this as an invasion to their privacy and rally against it.

Besides its main purpose, which is to record a video, the video surveillance system can scare off potential criminals because they are less likely to commit a crime in an area that is being monitored. Specifically for this purpose, fake video cameras systems can be used. These cameras may look like real security cameras but they do not record anything because they have no video recording system. Their intention is only to provide a psychological feeling that the area is being watched. Their main benefit is that they are very affordable.

3.1 Security Cameras

The video cameras are devices that take large number of pictures per second which the human eye perceives as a continuous movie. The rate of pictures per second is called FPS (frames per second), the standard rate that is used is around 24-30 FPS. Some cameras operate at a lower rate which makes the video choppy but it can significantly save storage space.

There are many types of security cameras available nowadays. They differ in size, shape, parameters and features which all play a role in their application. One of the important parameters of video cameras is resolution which gives information about the quality, how detailed the recorded video will be. The resolution is usually given as the number of horizontal and vertical lines. This number is typically expressed in units of pixels.

The security video cameras can be divided by their design into three distinct categories: bullet cameras, box cameras and dome cameras.

The bullet cameras are commonly placed outside on a building or a pole (see Figure 11). Some of the bullet cameras can be rotated to monitor a specific location. This might be beneficial if the camera is pointing to a desired place, for example a cash register or a door. On the other hand, this function can be misused by a criminal who can rotate the camera to avoid detection.

Figure 11 Three bullet cameras on the corner of a building

The box camera (see Figure 12) requires lens which might come with the camera or it has to be bought separately. Box cameras are flexible because the lens can be easily replaced by lens with different parameters.

Figure 12 Box camera with lens connected

Another type is a camera placed in a dome (see Figure 13) which provides a few advantages over the bullet and box cameras. The dome camera cannot be rotated nor moved if mounted properly to the wall. If the camera is not visible through the dome, nobody can see the direction to which the camera is pointing. The dome also serves as a protection for the camera which is especially solid in case of vandal-proof cameras. The dome cameras are commonly used for in-door applications because they are usually smaller and they are not as much noticeable as the other types.

Figure 13 Dome camera in a rail station

The video cameras that have the ability to rotate and zoom are called PTZ (pan-tilt-zoom) cameras where panning refers to the horizontal movement and tilting to the vertical movement. There are also different variations of these cameras, such as only pan-tilt or only zoom cameras. The rotation and zoom of the camera can be controlled either manually by an operator of the video surveillance system or some of the more intelligent systems are able to focus on an object automatically.

Some of the video cameras are also capable of recording audio using a built-in microphone. This additional function might be beneficial because the surveillance system provides more information about the recorded situation. However, audio recording should be considered from the legal point of view because not everywhere is audio recording allowed, it may vary from region to region. In some countries or states, it might be for instance required to inform people that the audio is being recorded in the area.

The video camera should be suitable to the given light conditions. In order to record a video in low-light conditions, a special video cameras for this purpose should be used. An appropriate recording device for this situation is a video camera equipped with IR (infrared) lights which are turned on when light in the environment falls below a certain

level. The IR cameras use a specific spectrum of light which is heat. The resulting video can be for example only in shades of grey where black or white color represents the heat (see Figure 14). The infrared cameras can be hardly used to recognize a person but they are capable of recording a video even at night or in places where there is absolutely no light. If there is too much light on the other hand, a video camera with an auto iris is recommended. This feature allows the camera to automatically close the iris to limit the amount of light entering the camera when it is necessary, for example when the sun is shining directly to the camera in the morning.

Figure 14 Picture taken by an infrared camera

The video cameras are either wired or wireless, each type has its advantages and disadvantages that should be considered according to the required application. In comparison with the wireless cameras, the wired cameras are generally more reliable, the video quality is better and there is no time delay. The wireless cameras are on the other hand easier and more affordable to install because they do not require any cabling for the data transfer. It is important to understand that most of the wireless cameras are not completely wireless since they require a power adapter to operate. Some cameras can be powered by batteries but the batteries have to be regularly recharged or replaced by new ones. Furthermore, the wireless connection is not recommended from the security point of view because the wireless network could be potentially accessed by an intruder. The

wired cameras should be installed everywhere that it is possible and wireless cameras only in places where it is not possible to implement the wired cameras. It is common to install wired cameras in new buildings where the cables are hidden in the walls during the construction. However, in case of historical buildings, such as galleries, museums and churches, it might be a better solution to use wireless devices for structural and esthetical reasons.

Another important property of a security camera to consider is whether it is designed for indoor or outdoor use. The outdoor cameras differ from the indoor cameras in the way that they are waterproof and more robust to withstand even extreme weather conditions. Therefore, the indoor cameras should be used only in buildings with standard room conditions, such as houses, offices and retail stores. The video cameras for an indoor application should not be used in a harsh, dirty or wet environment, such as warehouses, barns and industrial buildings.

Based on the technology and operation, the security cameras can be generally divided into two main categories: analog cameras and IP cameras.

3.1.1 Analog Cameras

The analog cameras are older than IP cameras and their usage is steadily declining. An analog camera is a type of camera that records the video in an analog form. The analog signal is then usually transferred over a coaxial cable to a DVR (digital video recorder) or directly to a monitor (see Figure 15). The digital video recorder is a device that stores the recorded video in a digital form. Note: not every analog camera can be connected with other cameras to a single coaxial cable.

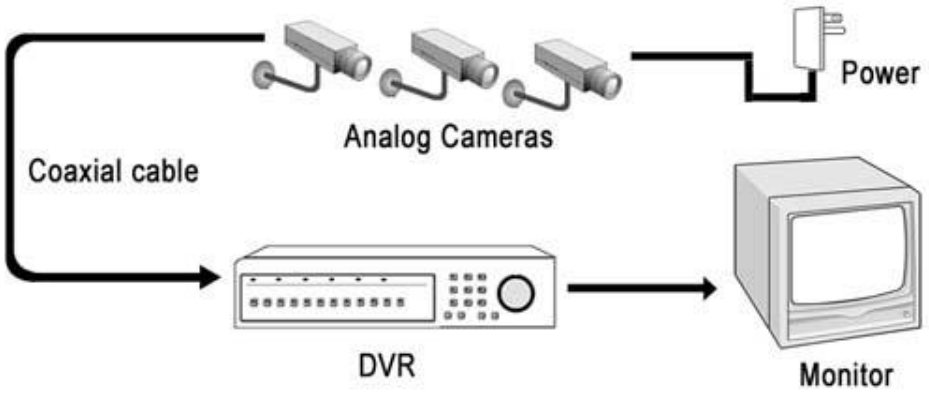

Figure 15 Analog video system with a digital video recorder

3.1.2 IP Cameras

IP cameras, also known as network cameras or netcams, are increasingly popular especially because they are capable of providing higher resolution than the analog cameras. The IP cameras are generally easier to install and require less hardware because they can be connected into the existing network infrastructure.

In an IP camera system, all data are processed digitally. The camera is called IP because it can be connected into an IP (internet protocol) network using a standard Ethernet cable or wirelessly. It is important to take into the account the bandwidth of the network because if there are many video cameras on the network recording in high resolution, it may significantly slow down the whole network. One of the solutions to avoid the network congestion is to use a separated network with its own switch dedicated only for the video cameras. In case of devices supporting PoE (Power over Ethernet), the camera can be powered directly by the Ethernet cable, therefore no power adapter is required.

When an IP camera is recording, the video is commonly sent to an NVR (network video recorder), where it is stored for later access. Alternatively, a standard PC with a video recording software can be used instead of a NVR device. If the video camera has an internal storage, no network video recorder is needed. In order to access a video stored on the camera or watch the live feed from the camera, the user only needs a computer connected to the same network (see Figure 16). If the switch is connected to the internet, it can be configured to allow access from the internet, then the user can access the camera

from anywhere in the world where there is an internet connection.

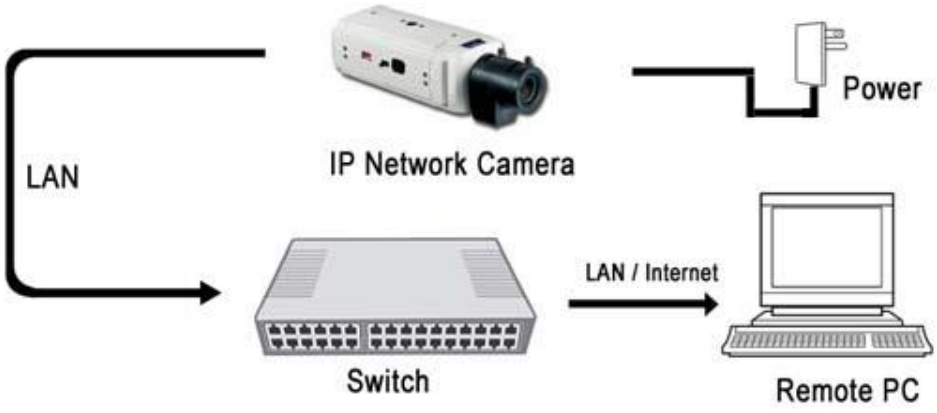

Figure 16 IP surveillence system with a network switch

CONCLUSION

The electronic security systems play a significant role in our modern world and should not be overlooked. Today, there are many kinds of electronic security systems with different parameters each for some specific purposes. The electronic security systems are being constantly improved to be more reliable and precise. But even the latest electronic security systems do not have to be sufficient when installed individually and should be combined with other security systems to ensure the highest security. The majority of the electronic security systems still require some human intervention, either to install and maintain the equipment or provide a response to the system.

The purpose of the security systems is to minimize the security threats as much as possible. In the real world, the potential security threat cannot always be completely avoided. In addition to the security, sometimes it is necessary to consider the budget for the security system. Even though, a more advanced technology might be available on the market if the company or individual does not have enough funds, they are not able to improve the security further more. On the contrary, sometimes the latest most advanced and expensive technology is not needed for the required level of security. The capabilities and quality of the security system should be balanced with the costs based on the specific security needs of the business or individual.

Since the costs of the electronic security systems are decreasing steadily, the fundamental systems are available to almost anyone and government agencies are applying them on a massive scale. However, privacy of individuals should always be respected and personal data intended for security purposes should not be sold or used in any other way without the permission of the individuals.

The importance of electronic security systems will probably grow in the near future because we are becoming increasingly dependent on technology. Even if the number of security incidents would decline significantly, there will still be a concern for security because the human behavior and nature are highly unpredictable.

BIBLIOGRAPHY

Access control. (n.d.). In *Wikipedia*. Retrieved November 1, 2016, from https://en.wikipedia.org/wiki/Access_control

Access Control. (2016, March 11). Retrieved November 5, 2016, from http://www.tech-faq.com/access-control.html

Agurwal, T. (n.d.). Importance and Classification of Electronic Security System. Retrieved November 5, 2016, from https://www.elprocus.com/electronic-security-system/

Baker, P. R., & Benny, D. J. (2013). *The complete guide to physical security*. Boca Raton, FL: CRC Press.

Basics of a Home Security System. (2016, January 5). Retrieved November 5, 2016, from https://www.electronichouse.com/home-security/anatomy-of-a-home-security-system/

Bloomberg. (2014, October 31). *Killing the Need for Passwords With Biometrics* [Video file]. Retrieved from https://www.youtube.com/watch?v=88Rjg8gM_DI

Closed-circuit television. (n.d.). In *Wikipedia*. Retrieved November 1, 2016, from https://en.wikipedia.org/wiki/Closed-circuit_television

CPNI UK. (2014, June 23). *Biometrics for Automatic Access Control Systems* [Video file]. Retrieved from https://www.youtube.com/watch?v=9zCBFnIJaQw

CPNI UK. (2014, June 23). *Perimeter CCTV* [Video file]. Retrieved from https://www.youtube.com/watch?v=qo_BlaWu8wk

CPNI UK. (2014, June 23). *Wireless Connectivity of Physical Security Systems* [Video file]. Retrieved from https://www.youtube.com/watch?v=60gE1i5_mVw

Eli the Computer Guy. (2012, February 12). *Introduction to Digital Surveillance Systems* [Video file]. Retrieved from https://www.youtube.com/watch?v=OY_fz16lPvE

Eli the Computer Guy. (2012, February 25). *Digital Surveillance Cameras* [Video file]. Retrieved from https://www.youtube.com/watch?v=OSeYmKkbrhI

Eli the Computer Guy. (2012, March 2). *IP Surveillance Cameras* [Video file]. Retrieved from https://www.youtube.com/watch?v=xW6ns3dmqDI

Eli the Computer Guy. (2012, March 16). *Digital Surveillance System Administration* [Video file]. Retrieved from https://www.youtube.com/watch?v=9XBTHkLJo1c

Eli the Computer Guy. (2013, October 11). *Biometric Access Systems Introduction* [Video file]. Retrieved from https://www.youtube.com/watch?v=Hr67YDPJzPY

eNCATechReport. (2014, November 25). *Biometrics Technology | Tech Report* [Video file]. Retrieved from https://www.youtube.com/watch?v=Vy2e_Zb0eoY

EnvisionSurveillance. (2013, June 5). *Facial Recognition vs fingerprint biometric Access Control* [Video file]. Retrieved from https://www.youtube.com/watch?v=Nws1Xitjl5M

Eureka Forbes. (2011, December 21). *Eurovigil : Intrusion alarm systems (wired and wireless)* [Video file]. Retrieved from https://www.youtube.com/watch?v=5eq9V6jg6b4

Fire alarm system. (n.d.). In *Wikipedia*. Retrieved November 1, 2016, from https://en.wikipedia.org/wiki/Fire_alarm_system

firesystemsltd. (2014, January 11). *Fire Alarm Detection Systems – In Action* [Video file]. Retrieved from https://www.youtube.com/watch?v=TLN_JcCkQVU

Garcia, M. L. (2007). *Design and Evaluation of Physical Protection Systems; Second Edition*. Butterworth-Heinemann.

Home Security and Surveillance System [PDF]. (n.d.). Retrieved from https://www.pearsonhighered.com/samplechapter/0789729377.pdf

HowStuffWorks. (2014, September 15). *TechStuff: Biometrics pt. 1* [Video file]. Retrieved from https://www.youtube.com/watch?v=-NcnbYEdqBk

HowStuffWorks. (2014, September 19). *TechStuff: Biometrics pt. 2* [Video file]. Retrieved from https://www.youtube.com/watch?v=3ndDL3Dq4WY

howtosurveillance. (2013, August 22). *Security Camera Types* [Video file]. Retrieved from https://www.youtube.com/watch?v=LVah8MduHnU

IP camera. (n.d.). In *Wikipedia*. Retrieved November 1, 2016, from https://en.wikipedia.org/wiki/IP_camera

IP reader. (n.d.). In *Wikipedia*. Retrieved November 1, 2016, from https://en.wikipedia.org/wiki/IP_reader

Mac Jorgensen. (2015, November 21). *Wired vs Wireless Security Cameras – Expert Advice* [Video file]. Retrieved from https://www.youtube.com/watch?v=u3ey8oDdzGI

MxInstaller. (2011, May 24). *IP Camera Training: How an IP camera system works* [Video file]. Retrieved from https://www.youtube.com/watch?v=79G4InvJX78

NeoRising Technologies. (2012, February 3). *Honeywell's access control solutions – security system* [Video file]. Retrieved from https://www.youtube.com/watch?v=jOE1PsbbSVA

Pearson, R. L. (2007). *Electronic security systems: A manager's guide to evaluating and selecting system solutions*. Retrieved from https://books.google.com

Physical security. (n.d.). In *Wikipedia*. Retrieved November 1, 2016, from https://en.wikipedia.org/wiki/Physical_security

Polygon. (2013, October 16). *Invasion: The Real-World Technology of Watch Dogs* [Video file]. Retrieved from https://www.youtube.com/watch?v=6UNIfv3ZNT0

Radio Parts. (2014, March 11). *CCTV training* [Video file]. Retrieved from https://youtu.be/0tEZrfn5iQM

Radio Parts. (2016, April 19). *Understanding CCTV Systems [15 Apr 2016]* [Video file]. Retrieved from https://www.youtube.com/watch?v=F01qz4Or20Y

Security alarm. (n.d.). In *Wikipedia*. Retrieved November 1, 2016, from https://en.wikipedia.org/wiki/Security_alarm

SecurityCameraKing.com. (2014, August 27). *Learn the Basics of Access Control in this Video: Access Control 101* [Video file]. Retrieved from https://youtu.be/XvR6ww7F54w

Siemens. (2012, September 24). *Wireless fire alarm system: SWING animation – how it works* [Video file]. Retrieved from https://www.youtube.com/watch?v=zEq5c-rmPu4

The Beginner's Guide to Security Cameras [PDF]. (2013). Retrieved from http://safewise.com/images/safewise/files/Beginners_Guide_to_Security_Cameras.pdf

The Evolution of Access Control Systems. (2014, June 19). Retrieved November 5, 2016, from http://securecomminc.com/2014/06/19/the-evolution-of-access-control-systems/

Tool Craze. (2015, September 30). *How to install a Surveillance System* [Video file]. Retrieved from https://www.youtube.com/watch?v=hoCUbAQ34_A

USPTOvideo. (2013, February 15). *Science of Innovation -- Biometrics* [Video file]. Retrieved from https://www.youtube.com/watch?v=IlThIvXn2Hk