Intrusion detection sensors used by electronic security systems for critical facilities and infrastructures: a review

G. Yatman, S. Üzumcü, A. Pahsa & A. A. Mert
Department of Information and Security Technologies, HAVELSAN, Turkey

Abstract

This paper provides an introduction to the UFC 4-021-02 Electronic Security Systems Standard document prepared within the Unified Facilities Program of the U.S. Department of Defence, which is providing guidance to architects and engineers on how to plan and design electronic security systems for critical facilities and infrastructures. Then, this paper reviews the sensors, mainly the passive infrared-, seismic-, active infrared-, active ultrasonic-, microwave and fiber optic cable-sensors, that form the most frequently used sensors by an intrusion detection subsystem of electronic security systems for critical facilities and infrastructure protection. Lastly, this paper describes a generic perimeter electronic security system application with an unattended wireless sensor network (UWSN) and draws a conclusion by thoughts on other possible future sensor system developments.
Keywords: critical facility and infrastructure protection, electronic security systems, intrusion detection system, passive infrared sensor, seismic sensor, active infrared sensor, active ultrasonic sensor, microwave sensor, fiber optic cable sensor, unattended wireless sensor networks (UWSN).

1 Introduction

This paper provides brief information about smart sensor technologies used by the intrusion detection system, which is a subset of the electronic security system as described in Section 2 and shown in Figure 1, based on the UFC 4-021-02 Electronic Security Systems Standard Document. The unified facilities criteria (UFC) system is prescribed by MIL-STD 3007: Standard Practise for Unified

WIT Transactions on The Built Environment, Vol 151, © 2015 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE150121

Facilities Criteria and Unified Facilities Guide Specifications. The UFC 4-021-02 document is prepared within the Unified Facilities Program of the U.S. Department of Defense and is providing guidance to architects and engineers on how to plan and design electronic security systems. In Section 3, the most frequently used sensors by the intrusion detection system for critical facilities and infrastructure protection are reviewed, which are the passive infrared-, seismic-, active infrared-, active ultrasonic-, microwave and fiber optic cable-sensors. Then, in Section 4 a generic perimeter electronic security system application with unattended wireless sensor networks (UWSN) is described.

2 Electronic security system overview

Electronic security systems (ESS) are comprised mainly of access control systems (card readers, door contacts, etc.), closed circuit television (CCTV) system, intrusion detection systems (sensors), data transmission systems and operational control and command centers. ESS is part of an overall physical protection system. As shown in Figure 1, the overall physical protection system consists of civil engineering features of fences, gates, entry points, clear zones, and standoff distances; architectural issues of construction materials, barriers, doors, windows, and door hardware; structural issues of blast resistant protection; mechanical issues of heating, ventilation, and air conditioning (HVAC) protection and redundancy, electrical engineering issues of power redundancy and lighting systems, ESS, and operational considerations such as policy, procedures, and response times [1].

2.1 Detect, delay, and respond principle

Electronic security systems act mainly on the detect, delay, and respond principle where time between detection of an intrusion and response by security forces, which should be less than the time it takes for an intruder to reach his goal, is a key factor. For that reason, the ESS designer should plan and place certain intrusion time delaying obstacles like card readers or fences as shown in the example in Section 2.2, so that the security officers be able to gain enough response time to hinder the intruder trying to achieve his purpose, after receiving the intrusion alarm generated by the ESS.

2.2 Detect, delay and respond example.

Table 1 provides an example of the times related to each detect and delay option in Figure 2 [1]. The cumulative delay times shown in this example are estimated at slightly over eight and a half minutes. Assuming a security forces response time of eleven minutes, the sequence of events shown in Table 1 allows sufficient time for an adversary to achieve his purpose and/or damage the targeted asset [1].

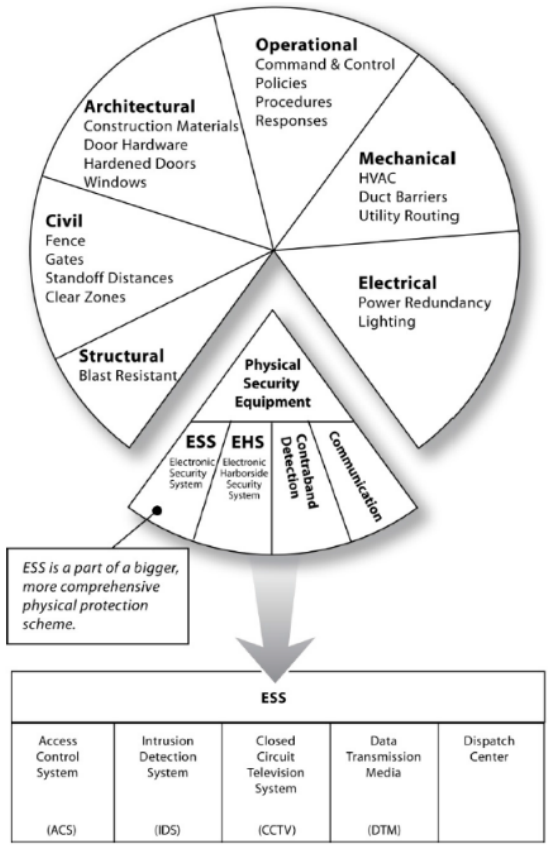

Figure 1: ESS as a part of a physical security system [1].

Table 1: Example breach events and delay time [1].

	Delay options	**Delay time**	**Detection options**
1	Climb fence	8–10 sec.	Perimeter fence detection system
2	Cross open ground (for example 600 feet)	10 feet/sec.	Microwave sensors
3	Breach building door or window or wall	1–2 min.	Door contacts or glass breakage sensor
4	Breach interior hardened door	2–4 min.	Door contacts
5	Work time in breached space	3 min.	Motion sensor
TOTAL DELAY TIME		**8 min 39 sec nominal for this example**	

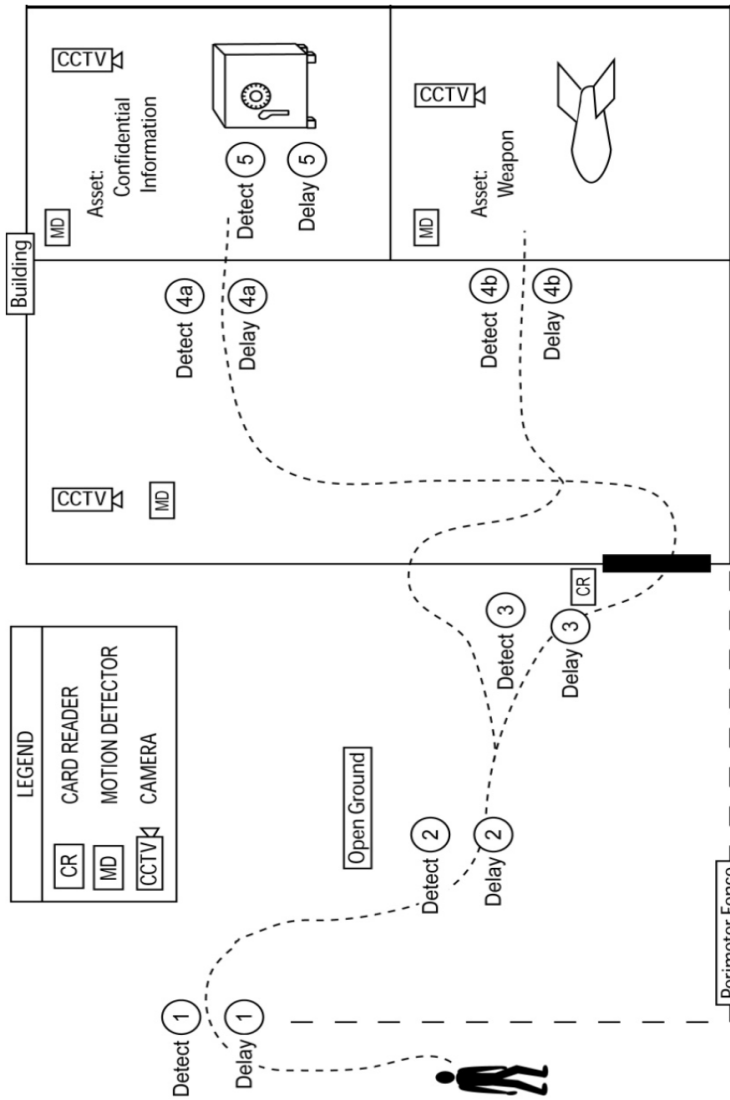

Figure 2: Example detect and delay options [1].

3 Intrusion detection system (IDS)

IDS is a subsystem of ESS as described in Section 2 of this document. The function of an IDS is to detect threatful/adversary intrusions. The detection of an intruder starts the "clock" on the detect, delay, respond timeline described previously.

The main components of an intrusion detection system are the following:

- Sensors detecting intrusion through sensing voice, vibration, motion and other physical and environmental events.
- A bidirectional data transmission media to transmit the signal of detection to a local and/or remote operational control and command center and for transmitting commands of operators to the field devices.
- Processors for automatic evaluation of the data received from sensors.
- Workstations with a user interface software for operators to monitor alarms actuated by the sensors.

In this section some of the most applied sensor types used by intrusion detection systems are presented.

3.1 Passive infrared motion (PIR) detectors

3.1.1 Detection principle

Infrared electromagnetic radiation is outside of the visible light spectrum and is emitted by all living beings and surrounding objects which can also be thought as radiated heat. The term passive for these kind of detectors refers to the fact that PIR devices are not generating any energy for detection purposes. Instead, they are only detecting the reflected heat from objects which are moving in their detection range.

Mirror or Fresnel lenses pool the rays of heat for maximum reception and transfer them onto a sensor made of pyroelectric (or thermoelectric) sensing materials. This sensing device generates a temporary electric potential when it detects a certain temperature difference which is caused by the object being warmer or colder than its environment and activates an alarm.

3.1.2 Application

Depending on the optics installed, PIR motion detectors are suitable for exterior (outdoor) and interior (indoor) surveillance.

3.1.3 Disadvantages and advantages

Structural elements inside detection area which are causing shadows are preventing detection or give rise to false alarms. The sensor is sensitive to weather. When body temperature and ambient temperature are the same, the sensor cannot differentiate and detect. Sudden temperature changes such as air turbulences or exhaust air from devices can create a moving object response which can activate false alarms.

The detectors can be easily installed. The detectors sensitivity can be adjusted. PIR sensors are very low on power consumption and thus suitable for battery powered applications.

3.1.4 Surveillance range

Depending on the type, the range may be approx. 100 m. The width of the surveillance area can be adjusted by suitable lenses or partial masking of the optical system (from <5° to >120°) [2].

3.2 Seismic sensors

3.2.1 Detection principle

In-ground seismic sensors also named as geophones detect seismic energy vibrations created in the ground by running, crawling or walking activities above its location. The seismic energy is converted by the sensors to electrical signals.

3.2.2 Application

Depending on the product, the detectors can be used for surveillance of paved, gravelled or asphalt surfaces as well as paths or grassland [2].

3.2.3 Disadvantages and advantages

The sensors sensitivity to low frequency signals is unsatisfactory. This fact leads to decrease of the detection range.

It is a hidden installation. It is suitable for surveillance of undulating terrain because the surveillance field can be aligned to the landscape. In-ground seismic sensors installed adjacent to the perimeter fence can provide additional detection capability for protection in case the vibration sensors mounted on the fence are bypassed by tunneling or careful climbing.

3.2.4 Surveillance range

One seismic sensor has a detection range of several meters per sensor. They can be cascaded to larger systems.

3.3 Infrared light barriers (active IR sensors)

3.3.1 Detection principle

Infrared (IR) light barriers are used for linear surveillance by IR light rays on straight perimeters where no ground undulations exist. This infrared sensor system is made of two basic units, a transmitter and a receiver. The transmitter, located at one end of the protection zone, generates a multiple frequency straight line beam to the receiver unit located at the opposite end of the zone thus an infrared “fence” is created between the transmitter and the receiver. Persons or objects interrupting the light ray between the units will be instantly detected.

3.3.2 Application

The area between transmitter and receiver needs to be clear of all obstacles/ obstructions that could interfere with the IR signal.

Typically, IR light barriers are used for surveillance in conjunction with wall, single/double fence or gate barriers.

When installed on roofs, these systems detect persons climbing over.

They can also be applied as a security curtain in front of objects to be protected. It is possible to install them on roofs to protect the crest.

3.3.3 Disadvantages and advantages

The surveillance range may be affected by weather conditions such as fog, heavy rain or severe sand/dust.

Their applications are manifold and can easily be retrofitted in existing security systems.

3.3.4 Surveillance range

Different systems with varying ranges are available.

The number of multiple barrier beam stretches, from individual transmitter-receiver pairs installed one above the other generally in posts, may differ.

The height of these barrier systems range from a few centimeters to several meters [2].

3.4 Active ultrasonic sensors

3.4.1 Detection principle

The active ultrasonic sensors are motion detecting devices that work similar to radar and sonar utilizing the Doppler principle.

They emit ultrasonic sound energy into a monitored area and reacts to a change in the reflected energy pattern.

3.4.2 Application

Ultrasonic sensors are installed typically on walls or ceilings. Ultrasonic sensors can be used together with passive infrared sensors to provide a greater probability of detection.

Because these sensor systems are dependent upon reflections, or echoes, from a moving intruder, clear line of sight between the sensor and the intruder are required so that energy can be transmitted to the intruder and reflected back with no obstructions in the way.

3.4.3 Disadvantages and advantages

Excessive air motion from a fan or an HVAC system can cause the sensor to trigger [3].

They are not affected from changes in the thermal environment. The ultrasonic sensor also can detect motion behind partial obstructions.

One of the key advantages of the ultrasonic sensor is the ability to calculate the distance to the object in motion [3].

3.4.4 Surveillance range

Ultrasonic sensors can be sensitive to slight motions at nearly twice the distance than PIR sensors. The overall detection range is comparable to that of a PIR sensor.

3.5 Microwave sensors

3.5.1 Detection principle
Microwave sensors are volumetric sensors and operate by radiating microwave energy into the protected area. They consist of physically separated transmission and reception units. Changes caused by intruders in the electromagnetic field between the transmitter and receiver are detected and lead to activation of alarms.

3.5.2 Application
Microwaves can be used to monitor both exterior areas and interior confined spaces, such as vaults, special storage areas, hallways and service passageways [4]. By exterior applications, microwave sensors are used for surveillance of wide areas or long stretches in open spaces or on top of roofs.

3.5.3 Disadvantages and advantages
The sensor is not suited for tight surveillance areas. Hills and depressions require special consideration as they may constitute surveillance loopholes [2]. Thus microwave signals pass through concrete and steel, special care is required when installing these sensors near roadways or adjacent buildings where nuisance alarms may occur due to reflected microwave patterns.

Detection is extremely reliable and weather insensitive.

3.5.4 Surveillance range
The radius of the elliptically extended surveillance area may be up to 15 m in the middle. It may be up to several hundred meters long.

3.6 Fiber optic cable sensor

3.6.1 Detection principle
Fiber optic cable sensors use light for transmission and detection. The cable sensor can be fastened to or installed on the fences or can be buried underground. They register disturbance at a barrier (e.g. fence) or in the ground. The fiber optic cable must be bent or disturbed in some way, to affect the wave guide of the light being transmitted and thereby signalling a disturbance [4]. Detection is a function of stress on the ground for buried applications or on the fence fabric by e.g. cutting or climbing over the fence for fence mounted cables.

3.6.2 Application
Fiber optic cable systems are suitable for surveillance of very long distances along e.g. fences or oil and gas pipelines.

3.6.3 Disadvantages and advantages
In some cases, considerable vibration caused by environmental impacts may cause false alarms.

The system is impervious to transient voltage and lightning strikes. It is suitable for retrofitting existing fences. Depending on the system, the fibre optic

sensor cable can also be used for transmission of communication data (e.g. video image data) [2].

3.6.4 Surveillance range

Depending on the product, these systems are suitable for distances up to 80 kilometers. The surveillance field of a cable is approx. one to two metres circumference around the cable routing [2]. Digital systems are able to localise alarms along the cable routing with an accuracy of several metres [2].

4 Description of a generic perimeter electronic security system application with unattended wireless sensor network (UWSN)

Today, closed circuit television (CCTV) systems are used by most of the security systems for critical facilities whereas the operation and maintenance costs of CCTV systems are high and the probability of preventing threats is low. Reasons are that these systems are dependent on the operators' recognition of potential threats through watching several screens with camera images in the operation center, and the cabling needs for the devices which is restricting the areas which can be monitored.

Recent advances in micro-electro-mechanical systems (MEMS) technology, wireless communications, and digital electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate untethered in short distances [5].

These sensor nodes together with wireless communication infrastructure and the operation center build up an electronic perimeter security system for critical facilities/infrastructures or borderlines which can be remote operated. Remote operated unattended wireless sensor network (UWSN) systems for protecting critical facilities and infrastructures in contrast to wired systems have advantages like cost effectiveness and the extension of area to be protected. Further advantages are the lower human live risk, long operation time without maintenance need, self-organizing capability, applicability to very large areas, endurance to tough environment and weather conditions.

The sensing units in the wireless area network (WAN) system don't only transmit the information collected from field, they also deliver information from other sensors through each other to collector units. Thus, a new sensor can be easily added to the network and even if a sensor is out of order due to a malfunction, the network structure can be reconstructed again according to the present condition. Another unique feature of sensor networks is the cooperative effort of sensor nodes [5]. Sensor nodes are fitted with an on-board processor. Instead of sending the raw data to the nodes responsible for the fusion, sensor nodes use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data [5].

The general structure of a generic perimeter electronic security system with UWSN application is shown in Figure 3. A command and control center software in this structure interprets and pre analyses the incoming data from the

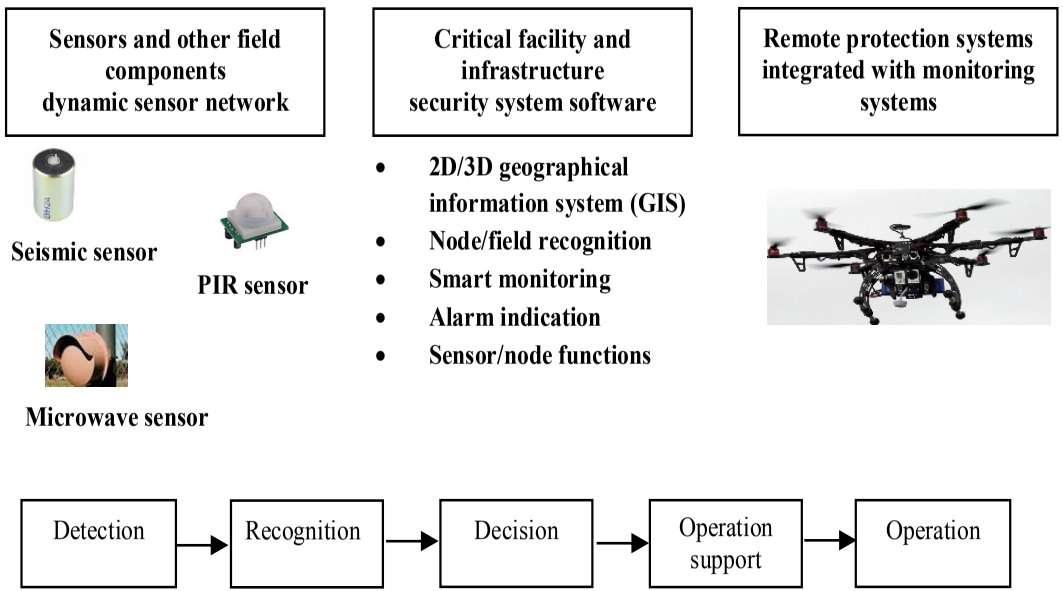

Figure 3: General block diagram of a critical facility/infrastructure electronic security system.

WIT Transactions on The Built Environment, Vol 151, © 2015 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)

smart and energy effective sensors comprising the WAN system, delivers the enquiries rapidly to the units to go into action, permits upon authorization remote operation of the sensors in the system, analyses data from past events and works in interaction with other systems like a unmanned vehicle drone which can be also added to the system for surveillance from air.

5 Conclusions and future directions

As discussed in the previous sections, various types of sensors operating in wireless mesh networks can build up highly effective smart security systems. These are state-of-the-art electronic security systems which have many advantages in contrast to wired classical systems as defined. New algorithms have also been developed for the application requirements of sensor networks.

These sensor network systems can be tailored to the optimum security systems required, by selecting the suitable sensors and other subsystem components according to the environmental, field and other conditions for the area to be protected. Important design criteria for electronic security systems are described by guiding standard documents like UFC 4-021-02.

Besides being used in security applications, it is foreseen that smart sensor systems will be placed everywhere in daily life in the near future. Personal health monitoring, training and coaching systems using wireless sensors are recently advertised by some of the leading electronic device companies. Wearable sensors of these systems are attached to the body and connected to a mobile or local data receiving and computing device with user software for tracking and showing performed activities, heart rates and other information required for monitoring.

Wireless sensor networks are going to be used in the health sector, for example by placing sensors in the homes of disabled patients for monitoring their health status remotely and continuously from hospitals. These systems can also be used for monitoring environmental pollution caused, for example, by industrial facilities, by placing relevant sensors in polluted sites for detecting the contaminants in water, soil or air. These and much more wireless sensor systems are now in front of our doors and are going to enter our lives soon.

References

[1] UFC 4-021-02, *Electronic Security Systems*, U.S. Department Of Defence, Unified Facilities Program, pp. 5–7, 2013
[2] VdS 3143, *Security Manual Perimeter*, Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV), pp. 31–38, 2012
[3] Hodges, L., *Ultrasonic and Passive Infrared Sensor Integration for Dual Technology User Detection Sensors*, Michigan State University, pp. 5–6, 2009
[4] National Criminal Justice Reference Service, *Perimeter Security Sensor Technologies Handbook*, Defense Advanced Research Projects Agency (DARPA) & The National Institute of Justice (NIJ), pp. 2–12 to 2–55, 1998
[5] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, *Wireless sensor networks: a survey*, Elsevier, Computer Networks 38, pp. 393–422, 2002