Volume XXI, 40 – No.1, 2019, DOI: 10.35116/aa.2019.0008

ELECTRONIC SYSTEM OF AIRPORT SECURITY

Radoslav ŠULEJ*, Jozef GALANDA, František ADAMČÍK
Technical university of Kosice, Faculty of Aeronautics, Rampova 7, 041 21 Kosice
Martin JEZNÝ
Airport Košice, a.s., 041 75 Kosice
**Corresponding author.* E-mail: radoslav.sulej@tuke.sk

Abstract. Priorities of on electronic airport security system involve timely information on unauthorized penetration or an attempt of entering the airport areas. Visible positioning of some of the system components is to divert potential perpetrators from attempting to penetrate airport facilities by way of signalling such events and also serving as a means of prevention.

Keywords: airport security; electronic system; security system

1. INTRODUCTION

The system of electronic airport security, further only EAS, is made up of components capable of protecting the areas of concern from break in. It is capable of automatically or human factor assisted relaying the required information to person or personnel in charge. For the purpose of identifying unauthorized Access into the protected area or just attempting it, is monitored employing detectors capable of recognizing movements, breaking glasses, opening doors or even attempts of sabotage.

The control element of the entire EAS system is a switching centre capable of evaluating the alarm state responses received from the separate detectors and subsequently transferring in via a communication system information for the user on penetration of the object. Integral part of the switchboard is a back-up source tasked with ensuring functionality of the EAS in case of power cut. Control of the switching centre is ensured by control elements that may involve a keyboard, remote control but latest models also involve mobile phones with the appropriate applications.

EAS can also be coupled to a centralized system of monitoring, alarm receiving centre, mobile phone sending the necessary information directly to police, private security agency of other predefined locations. Currently EAS makes uses a database system enabling complementing or extending the system even at a later date in future. Another advantage is in the addressability of the EAS components whereby the staff in charge is provided exact information as to which detector has raised the alarm, which module went out of operation and further information of use.

2. SECURITY SYSTEM

Any security system is made up of its separate but mutually interconnected parts with communication established among them. The security system can be understood as a set of elements of physical protection, technical equipment and elements of organization- and mode-related arrangements, see Figure 1. The set of the separate elements makes up a system of protection frequently termed as an integrated security system in which the individual elements of protection are combined thus providing optimum safety for the concrete object or interest to be protected [1].

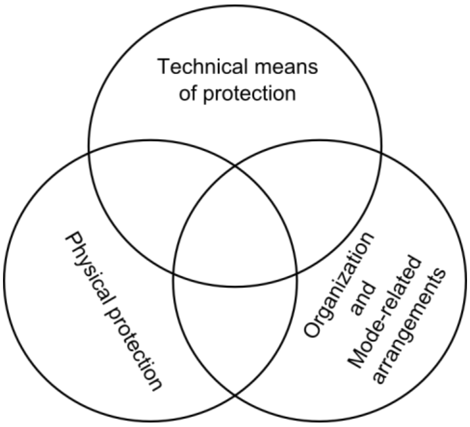
Technical means of protection
Physical protection
Organization and Mode-related arrangements

Figure 1 Security system [1]

In relation to providing protection for an interest, the system is defined as a set of technical and organizational arrangements that always must be placed between the threats and the object of threat. The set is made up of a combination of means for standard, mode-related, technical and physical protection termed as security system [1].

From technical point of view, the security system represents a system of electrical, electronic, mechanical or other components making up a firm installed barrier, which prevents a person from entering or leaving a protected object. It also protects against driving in or out the object under protection. The barrier cannot be overcome without professional expertise or physical force [1].

3. BASIC FORMS OF PROTECTION

The security system is made up of several independent and mutually interconnected sub-systems. Currently the following classification of the forms (subsystems) of protection applies [1]:

- Mode-based protection,
- Physical protection,
- Technical protection.

Mode-based protection is a set of administrative measures and procedures tasked with the introduction of a certain system into the operation of individual employees and guests in the protected objects with the aim of improving security in the object under protection along with providing other forms of protection. It is a system of organizational and administrative measures taken to define motion of persons within a protected object, area and its vicinity, as well as ensure flow of information related to the security of the object in question [1].

Physical protection is understood as the physical presence of a person within the protected area, at the place of interest to be guarded. It also involve ground patrolling, guarding, operating the EAS and also exercising direct control and supervision over activities mentioned [1].

Technical protection is a relatively simple and inexpensive form of object security. More or less, it offers preventive function, consequently, though combination with physical protection is recommended [1].

3.1. Potentials of using the EAS in view of area-based applications

In terms of the object security, the area-based applications of the EAS can be classified as follows [1]:

- Perimeter protection
- Cladding protection
- Area protection,

- Object protection.

Perimeter protection - signalling penetration of the object perimeter understood the frontier of the object represented by a protective barrier, i.e. a fence [1].

Cladding protection – signalling disruption of the object´s cladding, these of either vertical or horizontal building structures (walls, floors, ceilings). In this case the object is understood as a single building under construction, either the whole or defined set of its rooms [1].

Area protection – signalling violation of internal areas of an object defined by vertical and horizontal building structures. The perpetrator is assumed to have penetrated the object and is moving within its area where detectors have been installed around the assets to be protected [1].

Object protection – signalling immediate presence of the perpetrator at the object of protection or unauthorized handling with the object protected. [1]

4. MAJOR TASKS OF THE EAC

Any security system is made up of its separate but mutually interconnected parts with communication established among them. The security system can be understood as a set of elements of physical protection, technical equipment and elements of organization- and mode-related arrangements, see Fig.1. The set of the separate elements makes up a system of protection frequently termed as an integrated security system in which the individual elements of protection are combined thus providing optimum safety for the concrete object or interest to be protected [1].

4.1. Alarm signalling

Depending on the actual mode of operation, the EAS must ensure signalling of the alarm on having received signal from a violated detector, emergency reporter or elements of protection against sabotage. Alarm must also be signalled in cases as follows [2]:

- short circuit of the signal conductors or some of the conductors running between the switching centre and the equipment linked to it (detectors, control equipment, signalling components),
- unauthorized handling and intervention into the switching centre or system components.

Signalling of the alarm must be acoustic at least, whereas optical signalling is also recommended. In case of using optical signalling, it should be kept on until de-activated by the servicing staff. The purpose of optical signalling is to enable identification of the place of alarm status.

4.2. Failure signalling

EAS should ensure fail signalling in the following cases [2]:

- power cut from the main source,
- power cut from the back-up source,
- drop in battery capacity,
- communication failure among the components of transfer and signalling,
- communication failure with the detectors.

4.3. Status indication

Using means of indication, the EAS should indicate [2]:

- State of alarm,
- State of failure,
- State of safety loops On or Off,
- State of detectors,

- State of transition from actual mode to other mode of operation (for example from mode of guarding into standby mode).

The switching centre should feature elements of indication installed directly on the control equipment to ensure indication of the states as above.

4.4. Sabotage detection

Sabotage detection must be featured by all EAS components, expect from emergency indicators. It must be active in both modes of EAS operation, i.-e. while guarding or when on standby. The control equipment that might affect the functionality of the EAS are designed for use in the interiors of guarded objects and must include means of preventing replacement of such and equipment as a whole, or its part or signals running between the equipment and the switching centre [2].

4.5. Protecting the EAS against sabotage

Components contained in he EAS involve equipment that limit Access into its internal elements so as to prevent them from changing their setting or putting them out of operation. Protection against sabotage may take different forms and depends on the location of the EAS (in the exterior or interior of the area to be protected).

Requirements set for protection against sabotage:

- all the clips and control elements must be secured against unlawful access,
- claddings must be sufficiently resistant to mechanical damages so as to prevent unauthorized access to the internal elements of the system without visible traces of damage to cladding or raising the sabotage alarm,
- access to internal equipment as parts of the EACS must be designed so that special tools are needed so as to enable access to them.

4.6. Entry into the events memory

Entry into the memory is necessary for feedback checks as well as for securing events that have taken part for a period of time.

Events entered into the memory [2]:

- identity of the user at programing,
- states of guarding/standby,
- switching On/Off protection,
- alarm status of emergency,
- identification of the zone in emergency,
- alarm status of violation,
- identification of the zone of break-in,
- state of sabotage,
- identification of the individual detector of violation,
- zone, detector of break-in or the emergency indicator blocked,
- zone, detector of break-in or emergency indicator switched off,
- failure of the detector,
- failure of the emergency indicator,
- failure of the back-up power source,
- failure of the main power source,
- failure of the warning equipment,
- other failures,
- detector raising alarm as first,
- requirements to change the battery,
- change in date and time,

- change in specific settings,
- completing/deleting users.

The means of the memory serving for mandatory recording of the events must be protected against accidental or purposeful deletion of the events.

5. CONCLUSION

At the present time technical protection along with physical protection are rated among the most frequently used forms of protection and depending on the intervention capability of the latter are considered as the most reliable ones. The components employed will also determine whether the security system will belong to the most difficult ones to overcome or not.

EAS provides sufficient protection of objects, but despite of it, it is recommended to be combined with mechanical barriers of protection (farrowing rails, locks and latches), camera systems, electronic fire signalling, all of them realising to the level of safety and security.

ACKNOWLEDGEMENT

This work was supported by the Slovak Research and Development Agency under the contract No. APVV-15-0527.

References

[1] Veľas, A.: Elektrické zabezpečovacie systémy. Žilina: EDIS – vydavateľstvo ŽU, 2010. ISBN 978-80-554-0224-6. Available at: http://fsi.uniza.sk/kbm/wp-content/uploads/2013/12/Velas_EZS.pdf.

[2] STN EN 50131-1 (33 4591) Poplachové systémy – Elektrické zabezpečovacie a tiesňové poplachové systémy.