SUPERVISION AND CONTROL SYSTEMS USED IN THE MANAGEMENT OF FACILITIES

Constantin PRISTAVU[1]

Rezumat. *Securitatea este singurul concept care poate îndeplini cerințele de siguranță și stabilitate necesare bunei funcționări a sistemelor în condițiile actuale. Ca proces emergent, securitatea are ca obiectiv principal stabilitatea sistemelor. Practic, noțiunea de securitate poate fi asociată cu ideea de „fără pericol", chiar dacă pericolul în sine există, dar nu poate acționa împotriva sistemului protejat, iar noțiunea opusă de insecuritate poate fi asociată cu ideea de „prezență". În aceste condiții, fără îndeplinirea tuturor condițiilor de siguranță, poate acționa asupra sistemului, punandu-i in pericol securitatea.*

Abstract. *Security is the only concept that can meet the requirements of security and stability necessary for the proper functioning of systems in the current conditions. As an emerging process, security has as its main objective the stability of systems. Basically, the notion of security can be associated with the idea of "no danger", even if the danger itself exists, but it cannot act against the protected system, and the opposite notion of insecurity can be associated with the idea of "presence". Under these conditions, it can act on the system, endangering its security.*

Keywords: Risk, Assessment, Security, Burglary, Fire

1. Introduction

Here It is becoming increasingly clear that in our century security is becoming the pillar on which economic development and, indirectly, the well-being of the population is based. The range in which the issue of human safety needs to be addressed requires new approaches, new concepts and tools for both decision-making and action. If during the Cold War security was the main concern of the army, today it has become a consumer product that generates its own market, with specific procedures and quality standards.

According to the study, security services are traditionally requested by companies or private institutions that require security services. On the other hand, appealing to these types of companies is a consequence of public distrust of the authorities, especially the police and the judiciary, coupled with the general feeling that, in the event of events, the system can be manipulated if you know how to invest funds. resources and have adequate connections. In such an environment, the use of deterrents (security agents) is often perceived as a more effective way of

[1] CMP master student, University POLITEHNICA of Bucharest, Spl. Independentei 313, sector 6, ZipCode 060032, România. E-mail: cristipristavu55@gmail.com.

preventing crime. The perception that the state is unable to protect its citizens stimulates the demand for alternative means of security, which leads to the development of the private security sector [1], [2], [3], [4].

In this context, this document is dedicated to the study, understanding and design of systems that ensure the safety and security of people, their property and the safe conduct of all associated activities [5], [6].

2. Security systems

The main functions of a security system are determined by the main measures to be taken to protect targets, goods or persons:

• Prevention of intrusion of potential intruders in the protected area: fences, doors with locks, loud audible alarm.

• Restricting unauthorized access: codes, cards.

• Incident detection and monitoring: event identification, recording and archiving.

• Sending an alarm signal to the surveillance center and the intervention of specialized forces.

To perform these functions, devices, equipment and procedures have been developed that can function independently as a safety subsystem or in a combination of two or more subsystems [7], [8], [9].

The following are the main subsystems with their specific functions:

a) Fire detection, signaling and warning subsystem (FIRECLASS)

The main functions of the subsystem are [11], [12]:

• Fire detection based on signals from field sensors.

• Receiving signals from the field

• Local audible and / or optical alarms to alert people in the area

• Remote alarm and alert for intervention

• Control of automatic fire extinguishing systems where they are.

• Operator interface: system programming, configuration / reconfiguration.

• Save events for later analysis

As can be seen in Fig. 1, the main elements of a fire detection and warning system are:

• FIRECLASS fire station

• Fire siren

• Fire button

• Fun and temperature detector

• Batteries

• Cable connecting the elements [10], [13].

Fig. 1. Fire detection devices and warning system

b) Burglary detection and signaling subsystem (DSC PC4020)

The main functions of the subsystem are:

• Detection of attempts to enter protected areas

• Analysis of information to determine the type of event, the affected areas, as well as filtering errors (false positive)

• Local and remote acoustic and / or optical signaling

• Interface with the operator: programming, setting / dynamic reconfiguration (activation / deactivation of the zone according to the security plan)

• Save events for later analysis

Some elements that are part of the system (Fig.2.):

• PC4020 DSC control panel

• Motion detector

• Keyboard

• Magnetic contact

• Panic button

Fig. 2. Burglary detection system

c) Access Control Subsystem (IMPRO)

The main functions of the subsystem are:

• Restricting the access rights of people or vehicles by: using a PIN code, card, biometric features (fingerprint, weight, iris recognition, etc.).

• Detect and record events associated with access points, including date and time.

• Synthetic information based on the analysis of events for different periods (day, month, year or on demand at all times) by individuals or groups of individuals.

Elements such as: card reader, keyboard, electromagnet, etc., are part of the access control system (Fig. 3.)

Fig. 3. Door access control system

d) Closed Circuit Television Subsystem (HIKVISION)

It is the fastest growing and most efficient subsystem in the following areas:

• Retail

• Transport

• Education

• Industrial

• State institutions

• Health

• Banking and Finance

The main functions of the subsystem are:

• Capture images with a TV camera (fixed / mobile (pan-tilt-zoom / speed dome), black-and-white / color, with adjustable / unadjustable fixed parameters, visible or infrared, etc.).

• Transfer these images to their destination (analog signal, video signal, IP, TCP / IP signal or HD-SDI through different media: coaxial, UTP, or public networks).

• Management of received information using specialized equipment and programs for image processing, display, recording and archiving.

The main elements that are part of this subsystem are (Fig. 4):

• Video camera (indoor / outdoor)

• Video recorder

• Power source

• Monitor

• HDD

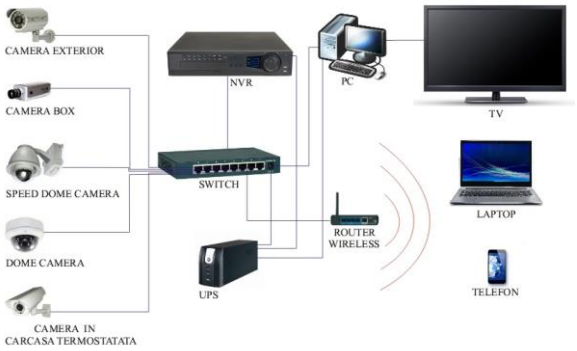

Fig. 4. Closed circuit television system

3. Integrated security systems

The analysis of the presented subsystems allows us to highlight the following:

• Each subsystem has specific functions and can operate independently.

• There are also general functions (for example, intrusion into a restricted area can be detected by a fence and an access control system).

• Most of the functions of the analyzed subsystems complement each other.

For small applications, security requirements may be covered by one or two subsystems.

However, there are applications whose importance is determined by the degree of security (airports, ports, defense), the importance of security values (banks, museums) or crowds (shopping malls, hospitals, educational institutions), and security and protection. the requirements are becoming more and more complex. In their case, an acceptable degree of protection can only be ensured when two or more of the subsystems presented are used.

However, without coordination between subsystems, the large amount of information provided cannot be optimally used and therefore the measures and actions to be taken will not have the expected effect.

Experience has shown that by integrating subsystems, their functions are improved and an efficient system is obtained.

The advantages of integrated systems are the following:

• increasing the efficiency and, indirectly, the level of protection;

• cost reduction;

• system flexibility;

• scalability.

Integrated systems may interact with other installations associated with the controlled target. For example, if a fire breaks out, hatches are opened and smoke outlets are turned on, and the access control subsystem opens its doors so that people can leave the safe areas. At the same time, the sound system broadcasts ads and guides people in accessible ways.

Compared to independent subsystems, as a direct consequence of integration, there are two additional requirements:

• the need to process a large amount of information taken from several subsystems;

• subsystem interconnection solution: physical support, procedures and communication protocols.

As a result, many companies (usually installers) have developed their own tools, hardware and software to integrate security devices.

4. Integrated systems management

The following requirements are imposed on an integrated security system: it must work in concert: the equipment that makes up the integrated system must be compatible with each other for optimal communication, use software that can handle a large amount of information and control subsystems; and their parameters in real time [14...20].

The CAVI software platform, used for unified monitoring and management of burglary, access control, fire detection and video surveillance systems, is a multi-user application that gives operators simultaneous access to the database with the following functions:

• Client-server structure (MS SQL Server);

• Unlimited number of burglary plants;

• Fire systems consisting of fire stations interconnected in the network;

Provides access to recorded video images using markers generated by alarm or access control events. Allows the video system to inspect any security-generated events.

The graphical interface allows you to create maps for convenient location of alarms. System component detectors are symbolized and located on field maps. Detector color indicates status: green - normal operation, yellow - technical malfunction, red - alarm, blue - off.

If an event occurs, the monitoring software will automatically display the alarm notification window and the corresponding map; Alarms are accompanied by an audible signal that stops when the alarm is confirmed by the operator in the monitoring window.

The program allows you to view event history, use various filters for alarms, technical issues, etc.) and generate reports (customizable by the operator or predefined in advance).

5. Implementing a security system in a banking institution

In order to implement a security system in a bank-specific location, the following important steps must be followed:

Physical security risk analysis is an assessment of the risks that may occur in a location depending on its specificity.

According to art. 66 of Law no. 333/2003, regarding the protection of objectives, goods, values and protection of persons, companies are obliged to perform a risk analysis on physical security.

Physical security risk analysis is, according to the legal provisions, a mandatory document for companies, which hold securities and assets, and which must ensure their protection. Specifically, this analysis is an assessment of the vulnerabilities that a company may have, so as to minimize possible risks.

The design of the security system makes the transition from an overview to a security system for a specific purpose.

"The project is drawn up in accordance with the provisions of art. 28, para. (7) of Law no. 333/2003, respectively, art. 5, para. (3) and art. 6 of Annex 7 to H.G. no. 301/2012. and includes details of execution and installation for each subsystem, technical data sheets of the equipment used, description of protected areas, lists of quantities and equipment used, technical reports, general data and general description of the works. "

Due to the high costs of implementing an integrated security system, it is necessary to adapt the existing system, or partially replace it, in order to be able to control it remotely.

In order to be interconnected and integrated in a dispatcher, the subsystems presented above required the additional installation of several classic monitoring elements (magnetic contacts, relays and signaling LEDs). This rudimentary but efficient solution led to solving the customer's problem, without having to make a major investment by replacing the entire system.

Monitoring and dispatching - implementation of a modern and innovative concept, able to operate autonomously - integration of solutions in a single system capable of ensuring the highest degree of safety and comfort.

In order to maximize the benefits of burglar alarms, detection systems, fire and various other physical and parametric operations (temperature, pressure, current, water, etc.), it is necessary to take action as soon as possible by the persons responsible for the removal. the cause of the action. As you can see, this is a chain of detection - communication - dispatcher - communication - end customer.

Without making too many technical statements about this chain, I will try to address the end user, ie the beneficiary, who needs to be aware of the needs of physical security and understand that choosing a short-medium-long-term security strategy can leads to significant financial savings, but more than that, the physical

security of goods and people. Therefore, in order to achieve this goal as effectively as possible, it is necessary to monitor and dispatch, ie surveillance and interference with alarm events with the assistance of experts and legal representatives, as well as control measures aimed at ensuring the security of assets and persons specified in the contract. This is to increase the speed of response and to limit or even eliminate the loss.

The first more sophisticated electronic systems operated with audible and visual signals without the involvement of a special brigade or specially designated personnel, often making their effectiveness questionable. In most cases, local alarms generated by the alarm system were rejected or confirmed after a long time, which was not guaranteed to work well or significantly reduced sabotage attempts. For this reason, long-term monitoring and intervention have increased the efficiency of the alarm system and ensured its installation. Gradually, monitoring and sending alarm systems became more and more important as they proved to be effective. Thanks to modern communications, the dispatcher is able to monitor a large number of systems anywhere in real time.

The monitoring process is based in principle on the following three components:

• Hardware components, such as: ethernet communication device, server, special protocol receiver, power supply, telephone modem, GSM, RADIO, GPRS, etc.;

• Software components, such as: central control station special programs, operating systems, connection programs and other automation programs;

• Human resources are represented on the one hand by specialized personnel who make specific decisions after the event at the dispatching console, which cannot be automated, and on the other hand by technicians who ensure the uninterrupted operation of all installed equipment.

Monitoring means, first of all, regular surveillance of the system and the reception of all events on a console. A combination of alarm systems - the dispatcher checks himself in a short time and transmits to the dispatcher any damage, sabotage, power outages and low battery capacity. In the event of a connection between the alarm system and the dispatcher or other faults, the persons authorized to remedy them will be notified immediately [20…26]. Advanced dispatching programs can automatically execute various command instructions, so today they can process more than 1,000 events per minute. In addition, the significant reduction in customer dispatching costs has made it possible to purchase such services at a very reasonable price, given the importance of maintaining a secure atmosphere.

The benefits of connecting to a monitoring dispatcher are innumerable, and unlike existing applications on mobile phones, it gives you extra protection and fast response speed:

• A monitoring dispatcher is never in a meeting, unable to answer the call.

• A monitoring dispatcher is not behind the wheel and is constantly on the road.

• A monitoring dispatcher is never in a place with no signal or low signal or in a tunnel.

• A monitoring dispatcher is never carrying shopping bags in his hands.

• A monitoring dispatcher does not turn off his handsets at night.

• A monitoring dispatcher periodically checks the equipment.

• A monitoring dispatcher never takes the phone to play Angry Birds.

• A monitoring dispatcher never runs out of battery power.

• A monitoring dispatcher always hears the alarm, because he never holds the phone in his coat pocket.

• A monitoring dispatcher never turns off the phone during a movie.

• A monitoring dispatcher hears all the time and is not disturbed by the noises that cover the notification sounds.

• A monitoring dispatcher rigorously organizes the history of events for a case analysis.

• A monitoring dispatcher calls the intervention team much faster.

And don't forget that unwanted events take place on Saturdays, Sundays, holidays, parties and holidays.

6. Conclusions

The paper presents both the functions of the security system and the components of each subsystem, as well as the steps that must be taken in the implementation of the system.

What makes this work unique from other articles is the CAVI platform, which has the ability to integrate complex infrastructures of security systems, security systems, BMS systems, IT infrastructure, or GPS systems, for a very large number of locations, with the ability to integrate any IoT device into a network that is easily scalable and works from any infrastructure such as SaaS, Cloud or its own infrastructure on virtual or physical servers.

Smart CAVI started as its own security information and migrated to a complete IoT platform, unique in the world, which integrates various sensors and devices, with built-in and customizable modules such as: building management, business intelligence, ERP, infrastructure management and others.

Compared to any other competing software currently available in the world (Genetech, Milestone, Azitrend, UltraVision, Alvis, Hikvision IVMS4200 and some proprietary software from Honeywell, General Electric and others), CAVI takes over all security streams and signals from to components of different vendors, filter them and then cross-reference the result with business, financial and even meteorological data to provide an overview of the entire security-related process (including financial and budgetary information related to those processes).

R E F E R E N C E S

[1] Adrian Roșca, 2012 - Security Systems Designer Course Manual, Security System.

[2]https://lege5.ro/Gratuit/gm4teobsge/legea-nr-333-2003-privind-paza-obiectivelor-bunurilor-valorilor-si-protectia-persoanelor?pid=67283088#p-67283088

[3] Silviu Clep, 2012 - Security Systems Designer Course Manual, Designing Alarm Detection Equipment Monitoring Systems.

[4] Aurel Catrinoiu, 2012 - Course manual Security Systems Designer, Security Systems Designer, Knowledge of Incident Legislation.

[5] Cristian Șoricuț, 2012 - Course manual Designer Security systems, Technical regulations: Fire detection and alarm installations design principle.

[6] Laurențiu Popescu, 2012 - Course Manual Designer Security Systems, Burglar Security Systems and Perimeter Protection.

[7] Viorel Tuleș, 2012-2,2012 - Security Systems Designer Course Manual, Introductory Notions: Designer Access Control Course.

[8] Viorel Tuleș, 2012-1, 2012 - Course Manual Designer Security Systems, Introductory Notions: Closed Circuit Television Systems.

[9] Viorel Tuleș, 2012-3, 2012 - Security Systems Designer Course Manual, Design Course: Closed Circuit Television Systems.

[10] Daniel Popescu, 2012 - Security Systems Designer Course Manual, General rules for low current installations.

[11] Alexandru Fanea, 2009 - Doctoral thesis: Contributions to the efficient management of thermal energy processes. Supervised order and process diagnosis.

[12] Ciubotaru B, Fanea A, 2005-1,2005 - Fault diagnosis for alarm management in industrial processes, Proceedings of IMACS 2005.

[13] Ciubotaru B, Fanea A, 2005-2,2005 - Fault diagnosis in industrial processes, Proceedings of IMAACA 2005.

[14] Condur G, Ciubotaru B, Fanea A, 2009 - Alarm Management and Diagnosis in Industrial Facilities, CIFA, Bucharest.

[15] Chow EY, Wilsky AS, 1984-Analytical Redundancy and the Design of Robust Failure Detection Systems, IEEE Trans. On Automatic Control Vol.

[16] Åslund J, Biteus J, Frisk E, Krysander M and Nielsen L, 2005– A systematic inclusion of diagnostic performance in fault tree analysis, Proceedings IFAC 16th Triennial World Congress.

[17] Papadopoulos Y, Grante C, Grunske L and Kaiser B, 2005- Continuous Assessment of Designs & Re-use in Model-based Safety Analysis, Proceedings IFAC 16th Triennial World Congress.

[18] Lupu C, Petrescu C, Alexandru M, Mateescu M, Popescu D, 2004 - Industrial process management systems, Ed. Printech.

[19] Tertişco M, Popescu D, Jora B, 1984 - Continuous industrial automation, Politehnica Publishing House.

[20] Tertişco M, Popescu D, Jora B, Russ I, 1991- Continuous industrial automation, Didactic and Pedagogical Publishing House, Bucharest.

[21] Isermann R, 1997 - Supervision, fault-detection and fault-diagnosis methods - an introduction, Control Engineering.

[22] Isermann R, 2006 - Fault-Diagnosis Systems, Springer-Verlag Berlin Heidelberg.

[23] http://www.jsu.edu/police/docs/Schoolsafety.pdf

[24]https://web.archive.org/web/20180128055910/http://airef.org/wp-content/uploads/2014/06/BurglarSurveyStudyFinalReport.pdf

[25] https://www.safewise.com/home-security-faq/how-do-security-systems-work/

[26] Computer Engineering An Approach A Reliable Approach to Computer Science.