Scholars Journal of Engineering and Technology (SJET)
Abbreviated Key Title: Sch. J. Eng. Tech.
©Scholars Academic and Scientific Publisher
A Unit of Scholars Academic and Scientific Society, India
www.saspublishers.com

ISSN 2347-9523 (Print)
ISSN 2321-435X (Online)

IoT Physical Access Control System

Olena Starkova[1*], Kostiantyn Herasymenko[1], Yekatierina Babailova[2]
[1]Department of Information Technologies, Taras Shevchenko National University of Kyiv, Ukraine
[2]Department of Radio Engineering, National Technical University of Ukraine, “Igor Sikorsky Kyiv Polytechnic Institute” Kyiv, Ukraine

Review Article

***Corresponding author**
Olena Starkova

Article History
Received: 28.04.2018
Accepted: 13.05.2018
Published: 30.05.2018

DOI:
10.36347/sjet.2018.v06i05.003

Abstract: The article is devoted to the description of the IOT (internet of thing) physical access control system, the main types of identifier, integration of PACS with systems of video surveillance and alarm systems.

Keywords: Internet of Things, Smart Home, Physical Access Control System, user ID, security.

INTRODUCTION

Physical Access Control System (PACS) is one of the most advanced systems that can be integrated into the Smart Home [1]. It is one of the most effective and civilized approaches to solve complex security problems of objects with various forms of ownership. By its very nature, PACS is the intellectual castle. To date, these systems provide their owners with broad opportunities to manage the security for the house, apartment and office.

Actually, any PACS is an electronic system that allows identification of employees and visitors that are entering or/and leaving protected area and provides access to the protected area only to those who have the right to do so. PACS allows at any time to provide control over the situation, safety of personnel and visitors, the preservation of material values and information. Access control system is a round-the-clock supervision and protection of all critical zones, territories and premises.

PACS allows you to set different levels of access to the premises, delineate access rights, keep track of visitors and the length of their stay at the facility. All the differences between existing systems consist in how reliable, high-quality, and user-friendly functions of the access control system are implemented.

THE MAIN TASKS THAT SOLVES BY PACS

The PACS is a complex of technical means that solves 3 main tasks:

- The PACS regulates the movement of people in the house or apartment, in the office, at the enterprise;
- PACS allocates access rights to various zones of the facility (office);
- PACS allows you to create a worktime recording system at the enterprise.

Absolutely simple, logical and necessary things that concern first of all owners of private houses, large apartments with separate rooms, owners of storage facilities or enterprises are implied. For example, if you have an attendant at the home and you do not want to give him/her any access to private rooms - workroom, server, boiler room etc., you can program the access control system, so you will be able to allocate access for attendant only on the certain premises.

CAPABILITIES OF THE PACS

The PACS provides such opportunities:

- allow authorized passage through doors equipped with PACS elements;
- automatic or manual unlocking of doors when the signal "Fire" comes from the fire alarm system;
- the access control system can grant employees access to zones and premises according to the distinction of access rights;
- the ability to issue reports on the time of passage of employees, working personnel for the recording of working hours;
- PACS can be integrated with security and fire alarm systems, video surveillance, Smart House at the hardware and / or software levels;
- archiving of all events occurring in the system - requests for input and output, alarm messages, malfunctions, switching equipment to backup power supply, time correction;

- blocking access points in case of emergency situations and unlocking if necessary;
- PACS can transmit alarms in case of unauthorized access to access areas and allocated premises (for example, door opening);
- Automatic backup of the database in accordance with the set schedule on the servers.

The basis for admission to the premises is the chosen identifier of the identity of the employee, the tenant of the house, the working personnel. Access rights (authorized access zones and time intervals) can be set by the owner of the house, the production manager, as well as the PACS administrator. Entry and exit of employees to the building, as well as passage through the zones should be carried out according to the chosen method of identification according to the authorization system of access in automated mode.

The access control system can consist of centralized and decentralized access controllers connected to the PACS server via Wi-Fi. Peripherals are connected to the controllers. For centralized control of the system and integration of its components with security systems, it is possible to connect the PACS to a single system for collecting and processing information through specially tuned software.

INTERNET OF THINGS CONCEPT

The Internet of Things (IoT) is a general concept of the ability of network devices to sense and collect data from the outside world and then distribute the data over the Internet, partially or completely without human intervention, where they can be processed and used for various interesting purposes.

In the description of the concept of IoT uses several basic concepts:

- Device (thing)-a separate device or a set of equipment equipped with sensors for gathering information, access to the network and having the ability to transmit data and remote control;
- IoT ecosystem is a local or global network of devices, as well as components that allow new ones to be added, providing remote management, storage, transmission and data security.

In the organization there are several levels:

- Physical - refers to hardware solutions used by instrumentation sensors and actuators, ADCs and DACs, microcontrollers for processing information and issuing control signals, memory storage devices, network ports;
- A network, which is understood by the data transmission medium (eg, cable lines or radio), gateways, routers, etc. - all the infrastructure responsible for joining devices on the network;
- Applications level used to transfer data and control signals, identify and interoperate protocols and interfaces.

Integration the IoT concept into the PACS allows creating more efficient and reliable system.

USER ID

This is a device or attribute that defines a user. Identifiers can be magnetic cards, contactless proximity cards, Touch Memory keyboards, various radio keychain, image of the iris of the eye, fingerprints, palm prints and many other physical features [2]. Each identifier is characterized by an unique binary code. In the access control system, the information about the rights and privileges of the owner of the identifier for each code is brought into compliance with data in the system database.

THE TYPES OF CARDS THAT ARE CURRENTLY USED

Contactless radio frequency (PROXIMITY) cards

Contactless radio frequency (PROXIMITY) cards - the most promising and currently used card type. Contactless cards triggered at a distance and do not require a clear positioning, which ensures their steady work, ease of use and high throughput of the system. The reader generates electromagnetic radiation of a certain frequency, and, when a card into the area of the reader, this radiation, through the embedded antenna, feeds the card chip. Having received the necessary energy to work, the card sends identification number to the reader using an electromagnetic pulse of a certain shape and frequency.

Magnetic cards

Magnetic cards a less common option, with several drawbacks - a small service life and the need for a clear positioning. There are cards with a low-coercivity and high-coercivity magnetic stripe with recording on the different paths. Usually used for identifiers with a very limited working duration.

Wigand cards

Wigand cards- named after the scientist who discovered a magnetic alloy having a rectangular hysteresis loop. Inside the card there are sections of the wire made of this alloy, which, when moved by the reading head, allows you to receive information. These cards are more durable than magnetic, but also more expensive. One of the disadvantages is that the code on the card is recorded once and for all.

Barcode cards

Barcode cards - the bar code is applied to the card. There is a more complex option - the bar code is closed with material, transparent only in infrared light, reading occurs in the IR region of the spectrum.

Key "Touch memory"

Key "Touch memory" - a metal tablet, which contains inside the ROM chip. When touching the reader's tablet, a unique identifier code is sent from the memory of the tablet to the controller.

One and the same card can open both one door or a few. Temporary employees and visitors receive temporary or one-time guest passes - cards with a limited term of validity.

THE MAIN COMPONENT OF PACS

Reader

A device designed to read information from an identifier, and transmit this information to PACS controller.

Point of passage

Some obstacle (barrier), equipped with a reader and an executive device. The passageway can be completely controlled or controlled only at the entrance. In the first case, the passage is equipped with two readers - to the input and output. In the second case - only the reader on the input, the output is carried out freely or by the button RTE.

RTE button

The "Request To Exit" button serves as a forced permission to cross the passageway, that is, to open an executable device. In this case, the fact of opening is recorded in the memory of the controller, but who specifically went through remains unknown. Such buttons are put to ensure unobstructed exit from the premises.

PACS Controller

The controller is the PACS heart. A device designed to handle information from ID readers, decision-making and management of executive devices. By way of control, the controllers of the PACS are divided into three classes: autonomous, centralized (networked) and combined.

Autonomous controllers

Fully finished device designed to serve as a rule one point of passage. There are a variety of variations: controllers combined with a reader, controllers, embedded in an electromagnetic lock, and so on. Stand-alone controllers are designed to use different types of readers. As a rule, stand-alone controllers are designed to service a small number of users, usually up to five hundred

Network controllers

A term indicating the possibility of controllers operating in a network under the control of a computer. In this case, the decision-making functions lie on a personal computer with installed specialized software. Network controllers are used to create PACS of any degree of complexity. At the same time, the administration receives a huge number of additional opportunities. Aside from simply allowing or denying passage, you can have the following features:

- Receiving a report on the presence or absence of employees at work;
- You have the opportunity to instantly find out exactly where the employee is;
- You have the opportunity to keep an working time accounting cards;
- You have the opportunity to get a report on who and where to go for almost any period of time;
- You can form a timetable for employees' passage, that is, who, where and at what time can move;
- You are able to maintain a database of employees (e-card files), in which you put all the necessary information about employees, including their photos.

And many other features. That is, there is always the possibility to fulfill the most exotic wishes of the owner of PACS;

Combined controllers

Combination of the functions of network and stand-alone controllers. In the presence of communication with the controlling computer (on line) controllers work as a network device, in the absence of communication - as autonomous. The best solution for today's integrated security systems is to build a fault-tolerant, flexible PACS.

Point of passage

Point of passage, endowed with special functions. A person who has not passed through the point of passage that marked as passable, will not be able to get access into any premises of the object. As a rule, it is precisely from the time the passage through the passage is calculated working time.

Photo identification

Ability to display the owner's photo on a computer (from the database). Photo identification is used for passage as an additional protection against unauthorized access. In this case, the decision on the passage can be taken automatically or with confirmation from the guard at the point of passage.

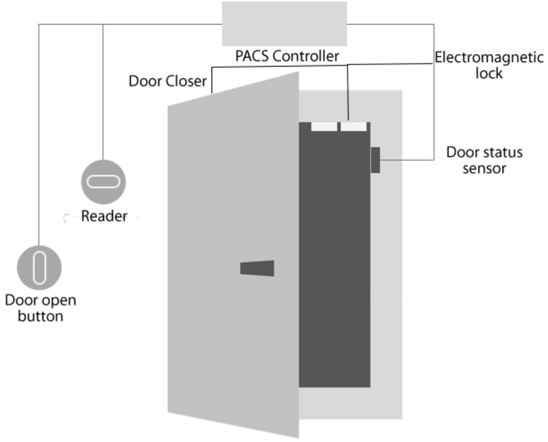

Fig-1: Example of the local PACS

FOR WHOM THE ACCESS CONTROL SYSTEM IS BENEFICIAL?

The system can take into account the time of arrival and departure of not only the guests and employees of the house. The special benefit of PACS is obvious for those who have children in the family. The system can be programmed so that after your child applies his personal key to the reader, you will immediately receive a sms notification on your phone or tablet, and the Smart Home system will launch the necessary script: for example, turn off the alarm, turn on the light in hallway, activates or deactivates the heating, cooling, ventilation systems, and if desired, disables all televisions, so that your child is not distracted from the homework. But the main thing: you will always know that your child returned safely home.

Also, the electronic system of passes is often used in offices, in enterprises, in the banking sector. For medium-sized and large-scale business owners, the use of such systems facilitates at times the process of personnel management, increases the efficiency of working time use, and correspondingly the resources.

The access control system includes reading devices, PACS controllers connected to the server via Wi-Fi, electronic omissions or biometric identifiers. Peripherals are connected to the controllers of the PACS system. All the input / output zones (access points) are equipped with readers.

INTEGRATION OF PACS WITH SYSTEMS OF VIDEO SURVEILLANCE AND ALARM SYSTEMS

The efficiency of the system of access control is increasing when integrating with the systems of video surveillance and alarm systems.

To maintain a large object, it is desirable to install a complex of automated security system consisting of:

- Fire alarm systems.
- Alarm systems.
- Surveillance systems.
- Access control systems.

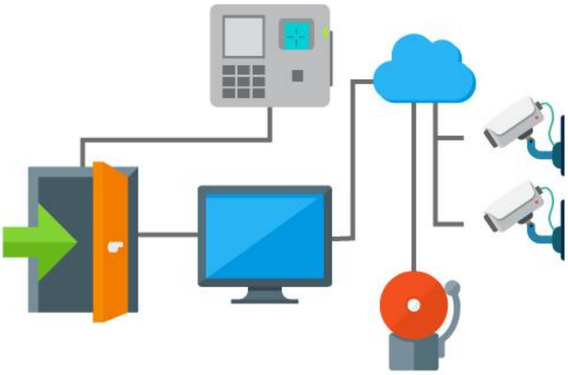

Fig-2: Integration of PACS with systems of video surveillance and alarm systems

THE PRINCIPLE OF FUNCTIONING OF PACS

The principle of functioning of the PACS is as follows:

Every employee, client, visitor receives an identifier (electronic key) - a plastic card or keychain from the content contained in it individual code.

"Electronic keys" are issued as a result of registration of the listed persons by means of the system. Passport data, photos (video) and other information about the owner of the "electronic key" are recorded in the personal "electronic card". The owner's personal "electronic card" and his "electronic key" code are linked to each other and entered into specially organized computer databases.

At the entrance to the building or in the hall of the room, readers reading from the cards their code and information about the rights of access of the card holder and transmit this information to the system controller.

In the system, for each code, information is provided on the rights of the cardholder. Based on the comparison of this information and the situation in which the card was presented, the system makes a decision: the controller opens or blocks the door (locks, turnstiles), transfers the room into a security mode, turn on an alarm, etc.

All facts of presentation of cards and related actions (passages, anxieties, etc.) are fixed in the controller and stored in the computer. Information about events caused by presentation of cards can be used in the future for receiving reports on the registration of working time, violations of labor discipline, etc.

At the enterprises it is possible to allocate four characteristic access points of access control: points of passage, office premises, premises of special importance, and entrance / departure of vehicles. Depending on the task facing you, you can choose the appropriate PACS.

A small PACS will prevent the access of unwanted persons and accurately indicate to employees the premises in which they have the right of access.

A more complex system will, in addition to limiting access, assign each employee an individual hourly schedule, save and then view information about events per day and so on. Systems can work offline and under the control of a computer.

CONCLUSIONS

Complex PACS allow you to solve the issues of security and discipline, automate accounting of working time, and create an automated workplace of the guard. Integrating PACS with the video surveillance systems and alarm systems allows creating more efficiency guarding and security systems. Integration the IoT concept into the PACS allows creating more efficient and reliable system. A set of functions performed by complex systems allows you to use a control system to perform specific tasks precisely at your enterprise or facility.

REFERENCES

1. "Sistemy kontrolya i upravleniya dostupom v dom, ofis, kvartiru, proizvodstvo." [Electronic resource] – Access mode: http://smarton.com.ua/kontrol-bezopasnost-doma/kontrol-dostupa/ (in Russian)
2. "Sistema kontrolyu dostupu" [Electronic resource] – Access mode: http://www.elvis.com.ua/ua/access-ua.html (in Ukrainian)
3. Dariia Ivanova, Olena Starkova, Kostiantyn Herasymenko Realization of the remote power management system based on the concept of Internet of Things / Problems of Infocommunications Science and Technology (PIC S&T), 2016 Third International Scientific-Practical Conference, p. 96-98.
4. Roman Kaporin, Alla Kogan, Olena Starkova, Kostiantyn Herasymenko Organization of secure multipath routing / Problems of Infocommunications Science and Technology (PIC S&T), 2016 Third International Scientific-Practical Conference, p. 103-104
5. Kovalchuk, K., Starkova, O., Herasymenko, K. IoT device for object's power remote control / Third International Scientific-Practical Conference «Problems of Infocommunications. Science and Technology» (PICS&T-2016), p. 112-113.
6. Andrii Polianytsia, Olena Starkova, Kostiantyn Herasymenko Survey of Hardware IoT platforms / Third International Scientific-Practical Conference «Problems of Infocommunications. Science and Technology» (PICS&T-2016), p. 152-153.
7. Ganna Vlasyuk, Kostiantyn Herasymenko, Yurii Kravchenko, Andrii Polianytsia Implementation of the Internet of things concept for remote power management / 2nd International Conference on Advanced Information and Communication Technologies-2017 (AICT-2017), p. 26-30.
8. Kravchenko Yu.V., Starkova O.V., Herasymenko K.V., Kharchenko A.M. Peculiarities of the IPv6 implementation in Ukraine / Forth International Scientific-Practical Conference «Problems of Infocommunications. Science and Technology» (PICS&T-2017), p. 363-368.
9. Kravchenko Yu.V., Starkova O.V., Herasymenko K.V., Kharchenko A.M., Technology analysis for smart home implementation / Forth International Scientific-Practical Conference «Problems of Infocommunications. Science and Technology» (PICS&T-2017), p. 579-584.
10. Andrii Polianytsia, Olena Starkova, Kostiantyn Herasymenko Survey of the IoT data transmission protocols / Forth International Scientific-Practical Conference «Problems of Infocommunications. Science and Technology» (PICS&T-2017), p. 369-371.
11. Olena Starkova, Kostiantyn Herasymenko, Yekatierina Babailova Remote control systems of household appliances / Forth International Scientific-Practical Conference «Problems of Infocommunications. Science and Technology» (PICS&T-2017), p. 585-588.