Solution for the integration of the security systems in the global building automation system

DANIEL POPESCU[1], CALIN CIUFUDEAN[2]

[1]Electrical Department
Technical University of Civil Engineering Bucharest
Bd. Pache Protopopescu nr.66, 021414 Bucuresti Sector 2
ROMANIA
dpopescu@instal.utcb.ro

[2]Computers and Control Systems Department
"Stefan cel Mare" University of Suceava
Str. Universitatii nr.9, 720225 Suceava
ROMANIA
calin@eed.usv.ro

Abstract: This article present an overview of the standards usually used in Building Automation System (BAS), adopted to implement the concept of intelligent building. The building is fitted with a global automation system that allows the intelligent building to react positively to the occupants needs and increase their productivity, through the use of the monitoring and control functions. An analysis is made for the feasibility of the integration of the security systems in the building automation system, at its data acquisition and control level, while preserving the essential legal technical requirements of the security technique. The integration solution proposed in this article, allows the interaction between different security systems and the traditional building services, when these detect events and trigger alarms, allowing them to be solved in an efficient way. The special requirements for the building security systems that can not be integrated in the proposed solution can be made maintaining the communication through the independent standardized connection, between the security systems and the centre for monitoring and alarm receive. This centre integrates the solutions for electronic security with security agents.

Key-words: Building Automation System, Building Management System, Intelligent Buildings, Security systems, Monitoring and alarm receiving centre, HVAC automation systems, Fire security system, Intrusion detection system, Access control system, CCTV system.

1 Overview of the standards used in Building Automation System

With the continuous progress and development of society, more attention is paid to improve the safety of the living conditions as well as the reliability of life quality. A Building Automation System (BAS) or a Building Management System (BMS) assures the good working of the buildings by monitoring and controlling of the heating, ventilating and air conditioning (HVAC) systems, lighting, energy monitoring, lifts, indoor air quality. The equipments that compose the BMS or the BAS are a network and communicate in between them by using a communication protocol based around an open communication standard. Frequently used standards are BACnet, LON, C-Bus and ModBus.

Network communication has a series of advantages in comparison with the transmission through other types of dedicated connections: lower cabling costs, data errors detection and correction by specific procedures, data transmission can be made at longer distances and with larger volumes. The disadvantage is that the equipments need to have a minimum „intelligence" in order to be able to communicate by a communication protocol.

BACnet is a standard data communication protocol for Building Automation and Control Networks which defines the way the communication takes places between the building automation equipments, using a specific number of wires [1]. The physical level can be made according with the RS-485 standard [2]. The open architecture of BACnet allows the control and monitoring of any

process that takes place inside a building. The first and obvious benefit is the savings in physical resources. BACnet standard is the choice for big companies in the field of building automation.
LON is a leading networking solution for Building Automation and it is a standard technology for many of the global standards organizations including ASHRAE, IEEE, ANSI. Technically, the LON standard covers all seven layers of the OSI (Open Systems Interconnect) reference model from the physical interfaces such as wired, power line, RF, and IP, to the application layer and all layers in between. The main difference between the LON protocol and other languages of equal recognition like BACNet and ModBus, is that LON was designed from the bottom up as a controls communication platform.
C-Bus is a communication protocol based on a seven layer OSI model for building automation. C-Bus is very powerful and highly scalable; the smallest installation can comprise only two nodes, but many large commercial installations comprise a number of interconnected networks and can include tens of thousands of nodes. C-bus is a two-wire bus that carries both power and data and uses a dedicated low-voltage cable. A single bus segment can address 255 individual devices and bus segments can be extended by the use of bridges. The wired C-Bus system uses a standard category 5 UTP (Unshielded Twisted Pair) cable as its network communications cable and does not require end of line termination. The maximum length of cable used on a C-Bus network is 1000 meters.
ModBus is a protocol based on the message exchange between equipments connected to the network. The protocol specifies the format for the interrogation and response messages, and from this point of view it is a level 2 -data link- protocol in the OSI Model. At level 1-physical level- it can be used as a physical support, a serial communication channel, for example, made according to the RS-485 standard which allows asynchronous data transmission on a twisted pair of wires with a differential type transmission interface.
In a ModBus network there is a master unit that initiates the communication and many other slave units that receive the data and answer to the interrogation. The master unit decides the order for network communication and the frequency for data transmission.

2 Essential technical characteristics for the building security systems

The comfort inside the buildings made by the traditional building services can be complemented nowadays by the safety offered to the occupants by the fire security system, intrusion detection system, access control system and the closed-circuit television (CCTV). All these security and traditional building services can be integrated in a global automation system that assures the comfort and well-being state for the occupants living and working inside the buildings.
The level of security reached in each building will depend on the budget available. Effective security comes at a price. Decisions must be made regarding the level of risk versus the cost of securing the building and people from harm or loss. The building which was designed to fulfil a whole series of criteria and it is equipped with integrated building automation in a global building control, can be considered as an intelligent building [3]. An intelligent building reacts in a favourable manner to the occupants needs, due to its functionality and supports the increase in occupant's labour productivity [4]. As shown in [5], the intelligent building contains, among others, the three basic elements: communication network system, building automation system (BAS), office automation systems. The combination of these elements provides a comfortable, efficient, safe, living and a good working environment.
The detectors that form the building security systems are usually addressable and are connected in loops made by wire conductors, fibre optic or wireless, customised for each type of security system. The detectors can not be connected directly to the BMS or BAS bus, because in this way the requirements imposed by the regulations for the security technique would not be fulfilled. The standards and the communication protocols are different for the BAS and for the security systems. A clear separation is needed between the security systems and the other types of traditional building services, in order to comply with the current regulations regarding the security technique: the systems have to be fitted with back-up power sources [6] that should assure a certain working autonomy if the main power source fails, images captured from the surveillance cameras need to be stored, a list has to be stored with all the events that took place over a period of time in the protected objective, etc. Another reason is the fact that the design and installation of the building security systems, as well as the activities for their

ISBN: 978-1-61804-189-0

maintenance, are subject to authorisation (licensing) from the competent authorities, because these systems are of great importance for life security and for material goods safety inside the buildings. Due to this reason, the security systems from the buildings have to be made out of certified devices, to be produced by distinct entities and to be able to work independently from any other technical systems that exist inside the buildings.
The technical expertises conducted after a fire took place, or after a burglary start from the way the security systems were designed, installed and used.
Security systems are based on an addressable loop. The main characteristic of addressable systems is that it allows the identification of the detector (or the detectors) that has triggered the alarm. In the example from figure 1, the intrusion detection system contains one detection loop, characterised by the fact the intrusion alarm panel controls the both ends of the loop circuitry on which the addressable intrusion detectors are. The main advantage of such a connexion is that if the loop cable is cut in one point, the automated intrusion detection and alarm system remains in working condition; intrusion detectors are being addressed alternatively through the both ends of the loop.

The addressable loop is implemented at its' physical level according to the RS-485 standard, but the communication protocols inside the loop differ from one system to another or from one equipment producer to another. The RS-485 standard defines the electrical characteristics of the balanced multipoint systems for data transmission [2]. Its technical characteristics recommend it for industrial automations as well as building automations. Because the processes inside the buildings are usually distributed across the building, the maximum length of the RS-485 link is 1200m, which makes this standard ideal for connecting devices found at a distance inside the building.
The RS-485 standard allows the implementation of linear topologies using as a physical support for data transmission only two simple, twisted copper conductors. Many other emitters can be added to the circuit, which can be controlled in the on or off state. Each information carrier electrical signal transmitted is characterised by differential voltages, so the receiver is sensible only to the voltage difference between the two signal lines [2].

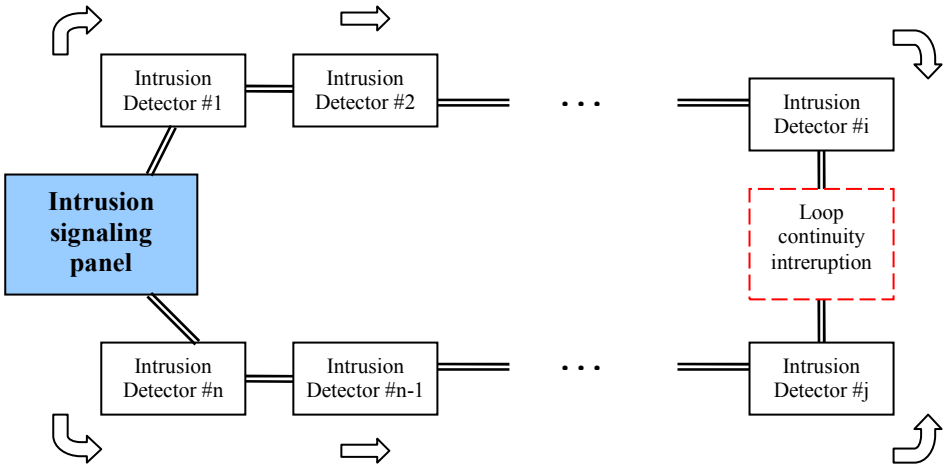

Fig. 1: Intrusion detection system with addressable detection loop.

3 The interaction of the security systems with other building services systems

Each security system should be separated from the other technical systems of the building and should be fitted with the possibility to inform the other security systems or traditional building services systems about the occurrence of an event in the area of building kept under monitoring. The monitoring is currently made by the use of electrical signals that can be the logical 0 or the logical 1, generated by the electrical contacts specially designed for this purpose. For example, the start of a fire can be announced to the other systems by closing an electrical contact and the event can be processed at the own automation level of the informed building services systems, by: triggering the fire extinguishing systems, smoke and hot gasses extraction, unlock the doors for

ISBN: 978-1-61804-189-0

emergency evacuation, elevators sent to the ground floor and stop them with the doors opened, switch off the ventilation in order to reduce the fire development, the activation of the video surveillance cameras from the area where the alarm was triggered, to allow the possibility to assess the fire, etc.

4 BMS monitoring and control functions

The automation systems installed in an intelligent building evolve towards the design of some complex and unique BAS for a building [7], which should realise the monitoring and control of all the building services systems, traditional ones as well as security ones (fig.2).

The exchange of information between levels 1, 2 and 3 suits the needs for a BAS, and the commands sent from level 2 to level 1 account the interaction between the security systems and the other building services systems.

All the equipments and building services from level 1 needs maintenance which is managed centralised at level 2. The structure in the figure does not allow the direct information exchange between the equipments that make up the level 2.

5 The integration of the security systems in the BAS

On the BAS and BMS bus can be connected equipments found at the acquisition and control level of the security systems, like the fire alarm and signalling panel, intrusion signalling and alarm panel, the units for access control inside the protected objective, the equipment for video images recording. The inclusion of the security systems in the BAS is possible only through the equipments at the acquisition and control level, if they are fitted with the necessary interfaces to be connected to the BAS network.

The field devices of the security systems found on the lower level of a BAS, remain connected to the

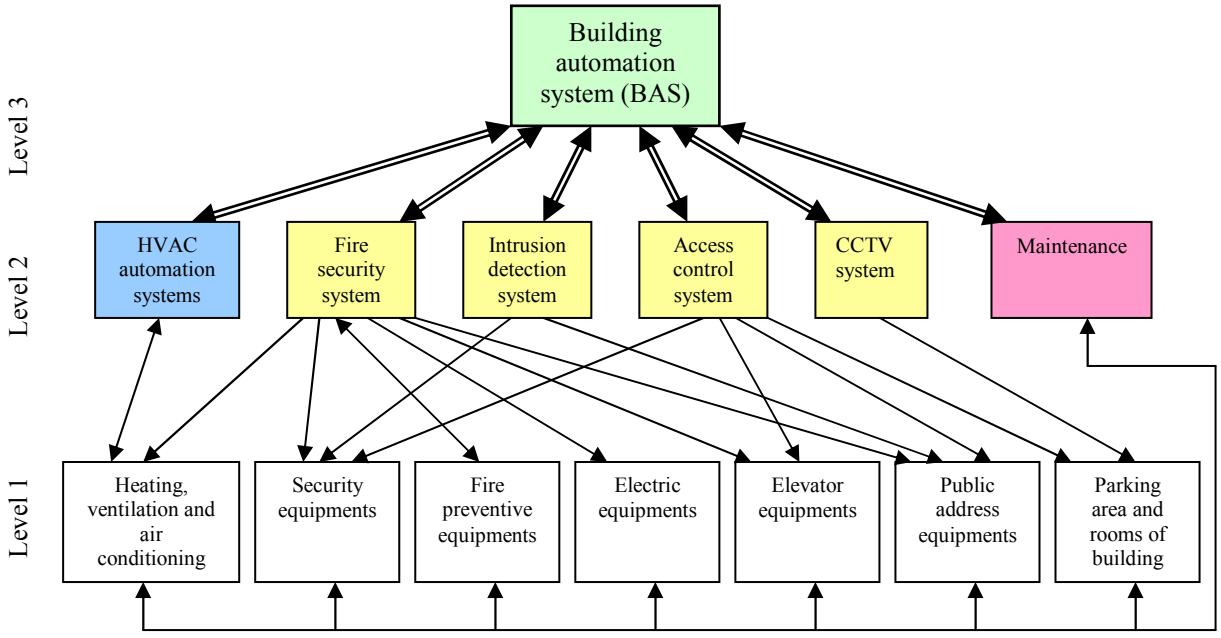

Fig. 2: The structure of the BAS for building monitoring and control.

signalling and alarm panel, to the units for access control or at the video images recording and storing equipments, according to the legal requirements for security systems (see figure 3 for an example of an access control system). The installation inside the protected objective, the equipments from the two hierarchical levels of the security systems, is not going to be affected by the integration in the BAS, and can be according with the current regulations and standards [8, 9, 10, 11, 12, 13, 14].

The integration of the security systems into a BAS requires the assurance of the compatibility of all the local equipments for control, found on level 2 in figure 2, so their electrical connection on a unique bus is possible (the BAS bus from figure 4),

ISBN: 978-1-61804-189-0

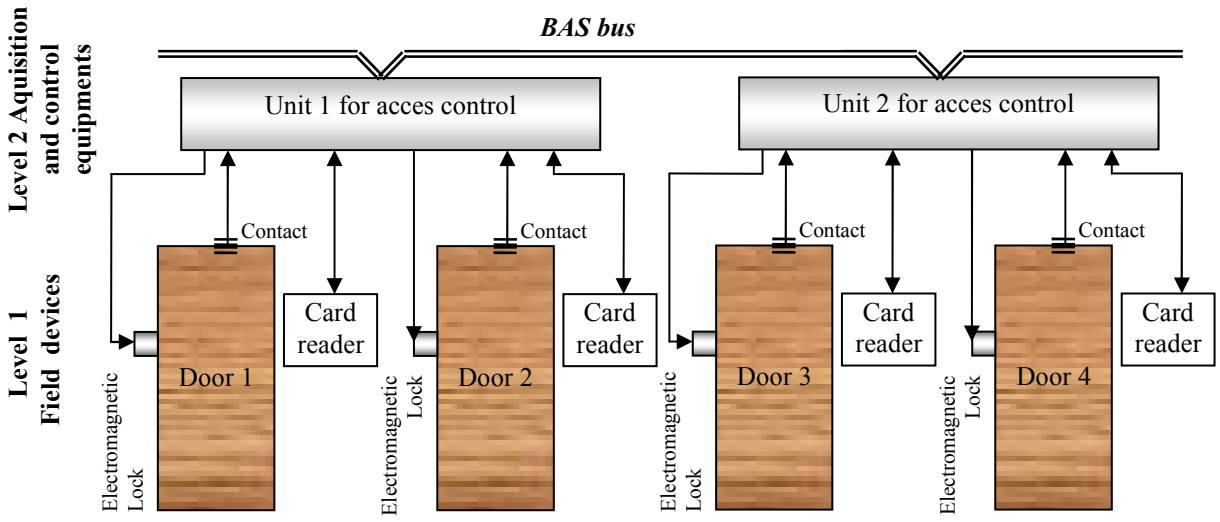

Fig. 3: The integration of access control system into the BAS or BMS.

according with a certain communication standard. The dialogue through the bus between the equipments has to be made according with communication protocol accepted by all the equipments and with the compliance of the regulations for security systems; the standard and the protocol have to stay at the base of the interface used in each equipment found at level 2 from figure 4.

This unitary treat of the automation systems from the intelligent buildings is possible because any security system installed in a building can be controlled using the same philosophy as for BAS or BMS. Can be created an open standard protocol to develop BAS client application, capable of displaying, controlling and monitoring all entities, irrespective of the manufacturer and also to develop a gateway to interface fire security systems, access

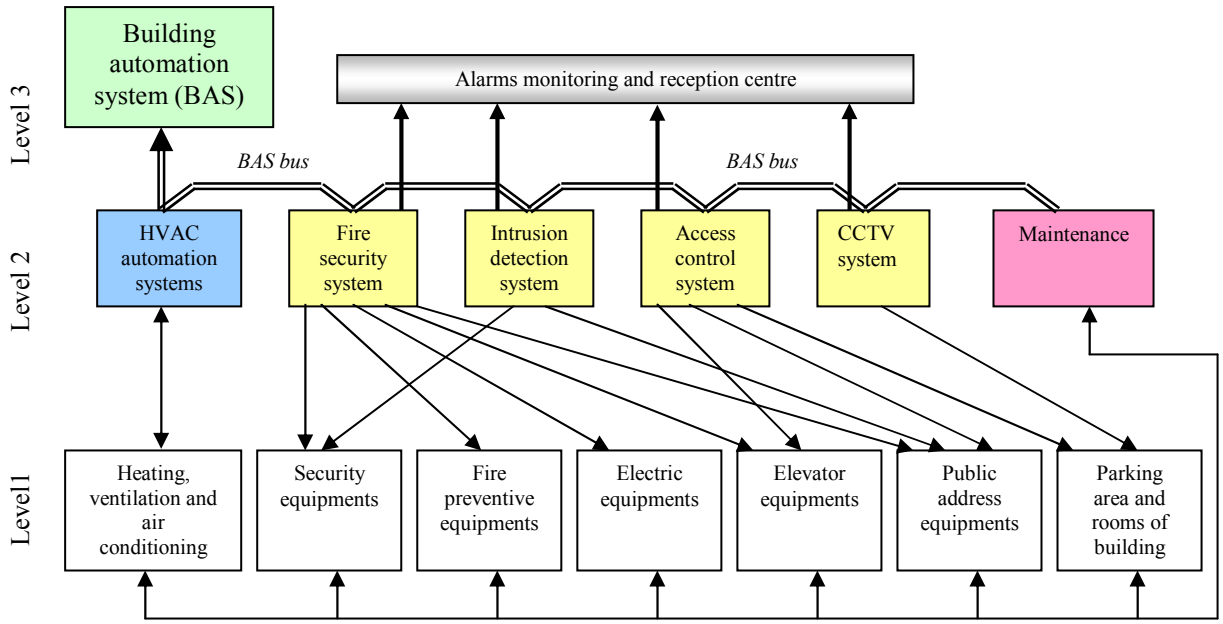

Fig 4: The structure of a BAS which includes the security systems.

control systems, intrusion detection systems, CCTV systems, through which to communicate in network building automation.
Activities in this sense are presented in [15].

The BAS structure depicted in figure 4 allows the systems from the second level to take the proper control decisions to respect the building fire scenario or the intrusion risk analysis, as a result of

ISBN: 978-1-61804-189-0

the dialogue between the equipments on the BAS bus. For example, when a fire is detected by the fire security system, HVAC automation systems stop the ventilation system to retard fire propagation, CCTV system activates the cameras in the area where the alarm was initiated, in order to assess the fire; the public address equipments are activated to announce the building occupants by voice messages about the danger and to evacuate safely the building, to stop the elevators with doors opened at the ground floor, to power off the electrical systems from the building, to unlock the doors for the safely personnel evacuation, etc.

The main purpose of CCTV systems installed in building is to survey the indoor spaces and outdoor spaces of building. But the CCTV systems may be used in modern buildings for different other purposes; using of smart cameras, some safety or security events that may lead to an alarm condition can be detected autonomously (e.g., security events like glass break, safety events like fire). Integrating CCTV systems into BAS provides the opportunity to inform the human operator about the occurrence of critical events. The operator can evaluate a fire alarm, an intrusion in the safety space, forcing of the access control system and so on. A possible way of integrating such CCTV systems into BACnet is presented in [16].

In the paper [17] is presented a solution to integrate into the overall building automation system the water circulating subsystem and air conditioning units, in accordance with ModBus RTU or PROFIBUS protocol. In this paper is solved the network communication problems in the building automation network due to the inconsistency of subsystem equipment by different manufacturers.

6 Requirements for building security systems that can not be assured by a BAS

In figure 4 one can notice that the building security systems are connected to the alarm monitoring and reception centre, situated at a hierarchical level 3; this centre offers services for electronic security solutions integration with the human guard's security.

The purpose of an alarm in a secured building is to initiate a reaction on a local area or from a remote location. The alarm can prevent something from occurring, like for example the intrusion, or to attract the attention to a required action in case something happens.

Assuring an efficient protection for a building is possible if one can find a correlation between the technical protection and the human guards. The optimum solution is a family of measures destined for mechanical, electronic and human guards protection, doubled by procedures applicable to the protected building.

The monitoring of the security systems from the buildings allows the initiation of some response and human intervention actions based on the information provided by the:

- fire detection and alarm systems, made according to [6];
- intrusion alarm systems made according to [18];
- access control systems made according to [19];
- video surveillance systems made according to [20];
- social alarm systems.

All the security systems can transmit remotely the information, including the alarms, in order to be processed, assessed and for taking the human intervention measures.

The monitoring and reception centre is organised and works according to [21, 22].

7 Conclusions

The BAS or BMS systems are made according to some standards that can be learned and applied voluntarily by the users, after which their respecting is compulsory.

The security systems can be designed, implemented and operated only by respecting some specific regulation specific for the security technique domain, by the authorised persons.

The integration of the security systems in the BAS can be made at the acquisition and control level, by the use of a unique BAS bus. The RS-485 standard is used at the physical level in the BAS or in the BMS, as well as in the security systems addressable loops. The advantages of the standard RS-485 are: good noise immunity, great communication range, multipoint connections, possibility broadcast, and simple implementation of drivers. The greatest disadvantage of this standard is large energy consumption.

The traditional building services systems and the security systems from the buildings have to interact in order to assure the comfort and the occupants' well-being. The interaction should not affect adversely the requirements for the security technique imposed by regulations.

ISBN: 978-1-61804-189-0

References:

[1] BACnet – A Data Communication Protocol for Building Automation and Control Networks. ANSI/ASHRAE 135, 2008.

[2] RS-422 and RS-485 Applications eBook, *B&B Electronics,* 2010

[3] Oancea, C., Contributions to the implementation of the artificial intelligence in the determination of the global comfort in intelligent buildings, *PhD Thesis*, Technical University of Civil Engineering of Bucharest, 2012.

[4] Oancea, C., Caluianu, S., Analysis of non-residential buildings in Romania from the labour productivity and intelligent buildings concept point of view, *Intelligent Buildings International,* ISSN 1750-8975 (Print), 1756-6932 (Online), Publisher: Taylor & Francis, Volume 4, Issue 4, October 2012, pp. 216-227.

[5] Jun Hu , Huaiwen Hu, Automation and Control Systems Research of Intelligent Building, *2012 International Conference on Education Technology and Management Engineering,* Hunan mechanical & electrical polytechnic 410151, ChangSha, 2012.

[6] EN 54 - Fire detection and fire alarm systems

[7] Ler, Eng Loo, Intelligent Building Automation System, ENG4111/4112 – *Research Project,* University of Southern Queensland, Faculty of Engineering and Surveying, 2006.

[8] EN 54-3 - Fire detection and fire alarm systems - Part 3: Fire alarm devices – Sounders.

[9] EN 54-5 - Fire detection and fire alarm systems - Part 5: Heat detectors - Point detectors.

[10] EN 54-7 - Fire detection and fire alarm systems - Part 7: Smoke detectors - Point detectors using scattered light, transmitted light or ionization.

[11] EN 54-10 - Fire detection and fire alarm systems – Part 10: Flame detectors - Point detectors.

[12] EN 54-11 - Fire detection and fire alarm systems - Part 11: Manual call points.

[13] EN 54-12 - Fire detection and fire alarm systems – Part 12: Smoke detectors - Line detectors using an optical light beam.

[14] EN 54-20 - Fire detection and fire alarm systems – Part 20: Aspirating smoke detectors.

[15] Bharadwaj, C.V., Velammal, M. , Raju, M., A BMS client and gateway using BACnet protocol, Conference *Communications in Computer and Information Science, 1st International Conference on Advances in Computing and Information Technology, ACITY 2011*, Chennai, 15-17 July 2011, Volume 198, pp. 437-449.

[16] Mauser, C., Granzer, W., Kastner, W., Integrating CCTV systems into BACnet, *IEEE Symposium on Emerging Technologies and Factory Automation, ETFA,* Toulouse, September 2011. ISBN: 978-145770018-7. DOI: 10.1109/ETFA.2011.6059140. 2011.

[17] Zhang, G., Research and design of automatic control system for central air conditioning in building automatic network system, Proceedings - *2012 IEEE Symposium on Electrical and Electronics Engineering, EEESYM 2012*. ISBN: 978-146732365-9.
DOI:10.1109/EEESym.2012.6258687.

[18] EN 50131 - Alarm systems - Intrusion and hold-up systems.

[19] EN 50133 - Alarm systems - Access control systems for use in security applications.

[20] EN 50132 - Alarm systems. CCTV surveillance systems for use in security applications.

[21] EN 50518 - Monitoring and alarm receiving centre.

[22] EN 50316 - Alarm systems. Alarm transmission systems and equipment.