TEKA Kom. Mot. Energ. Roln. – OL PAN, 2010, 10, 256–264

USE OF BUILDING MANAGEMENT ELEMENTS OF THE EIB SYSTEM IN SAFETY SYSTEMS

Jacek Majcher, Marek Horyński

Katedra Inżynierii Komputerowej i Elektrycznej, Politechnika Lubelska

Summary. The development of building management systems is accompanied by their gradual connection i.e. integration with other previously separate systems. The purpose of the study is to present the problem associated with the assurance of safety in modern buildings on the user level i.e. the protection of his health and property as well as the protection of the devices incorporated therein. As a result of the change of the functioning concept in the scope of building systems, the principles previously occurring in information system protection e.g. electronic mail or eBank accounts have been introduced into the protections of the modern buildings..

Key words: alarm, EIB bus, safety, integration, dispersed systems

INTRODUCTION

Since the beginnings of mankind people attempted to ensure safety for themselves and their loved ones. The first simple methods have gradually become more and more advanced technologies. However, the introduction of intelligent systems simulating human behaviours and automatically responding to varying ambient conditions depending on the occurring situation in order to ensure the protection for humans and their property was possible not earlier than in the 20th century as a result of violent development of electronic technology.

In the course of safety problem analysis, we have to consider the non – uniformity of this issue. According to the popular and generally functioning definition, the safety system is understood as the elements of the buildings alarm system used to ensure the property protection. However it should be emphasized that the protection of the components of the building systems as well as the protection of health and life of the occupants must not be forgotten in this case. The purpose of an intelligent building system is to protect the safety of its inhabitants and their property but also to fulfil the self – protection functions. Therefore any potential attempts of sabotage and of reprogramming of system components will be prevented. These tasks are performed by the so called building management systems (BMS), performing the task in this scope more or less successfully. In the scope of the systems responsible for human safety the following circuits can be indicated:

– Burglary and attack alarm system - SSWiN
– Access control system – SKD
– Fire alarm system – SSP

– Closed Circuit TV system – STVD
– Public address system – PAS
– Smoke extract system
– Fire fighting system [Mikulik 2005]

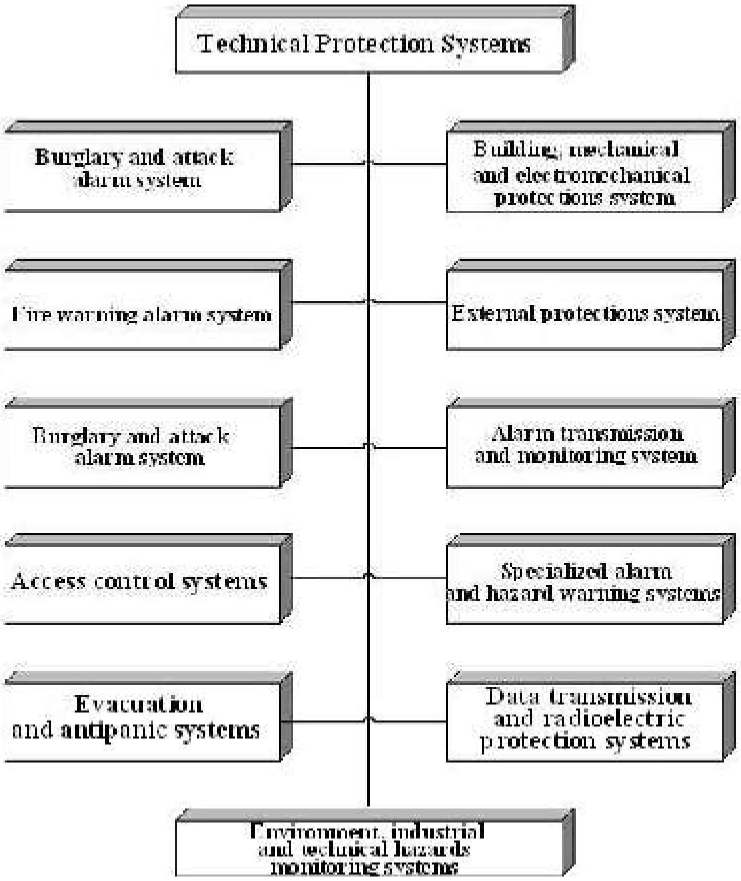

Technical Protection Systems
Burglary and attack alarm system
Building, mechanical and electromechanical protections system
Fire warning alarm system
External protections system
Burglary and attack alarm system
Alarm transmission and monitoring system
Access control systems
Specialized alarm and hazard warning systems
Evacuation and antipanic systems
Data transmission and radioelectric protection systems
Environment, industrial and technical hazards monitoring systems

Fig. 1. Structure of the technical protection of the building [Mikulik 2005]

The purpose of an alarm system is to detect any unfavourable conditions indicating the potential danger and to generate relevant alarm to inform the inhabitants about this fact. Pursuant to Polish Standard PN - 93/E-08390 the protection of objects can be subdivided into the following classes:

- **perimeter protection** – the protection of an object from outside along its fencing (first zone of protected area);
- **external protection** – the protection of direct vicinity of the object, physical object protections from outside, grids, brick walls, other buildings adhering to the protected area (second zone of protected area);
- **internal protection** – the protection of the inner space of the object, all door and window openings in the building (third zone of protected area);
- **local protection** – technical protection of the specified items e.g. safes, documents, etc.

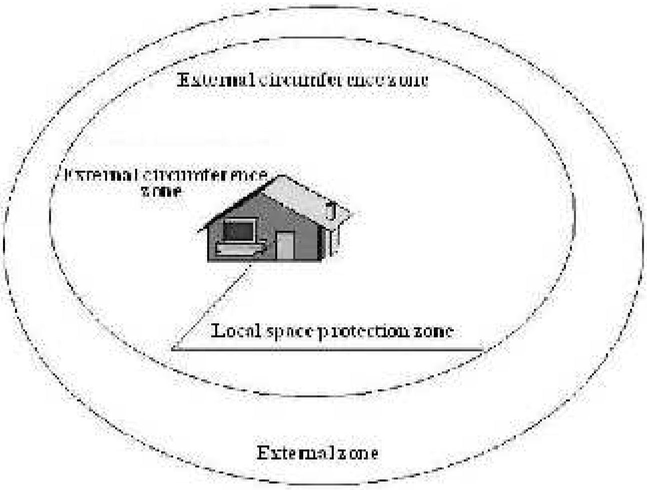

External circumference zone
External circumference zone
Local space protection zone
External zone

Fig. 2. Example of subdivision of the object protection zones

KNX/EIB SYSTEM

KNX has been established as the standard in the scope of intelligent buildings management and combines all subsystems occurring in all types of objects. [knx.org 2010] KNS originates from the European Installation Bus (EIB) designed in the form of open management and control standard for the devices and buildings. After their merger, the organizations developing EIB, Batibus and EHS are actually acting under the name Konnex (KNX). KNX is the only system meeting the requirements included in European Standard EN 50090 which has been designed in order to enable the automatic control for various equipment in the form of an open system – data transmission protocol is generally accessible. The structure of the system is decentralized i.e. each device is provided with microcomputer having its own application and communicating with the bus via bus port. Thanks to such solution, system reliability is maintained, because in case of the defect of single device, the operation of other devices is not affected. The bus port has been designed as a microcomputer consisting of the following elements: processing unit (CPU), memory ROM, RAM, EEPROM, interfaces i.e. user interface and network communication interface. The data transmission along the bus is carried out in an asynchronous manner with CSMA/CA access to the bus (*Carrier Sense Multiple Access with Collision Avoidance)* with the mechanism enabling the avoidance of collisions between telegrams received form various devices installed in the system. Its operation principle consists in the completion of the following procedure: in case of transmission attempted by two or more devices simultaneously, the transmission is commenced by the device with higher priority, when the priority of both the devices is equal, transmission is commenced by the device with higher physical address.

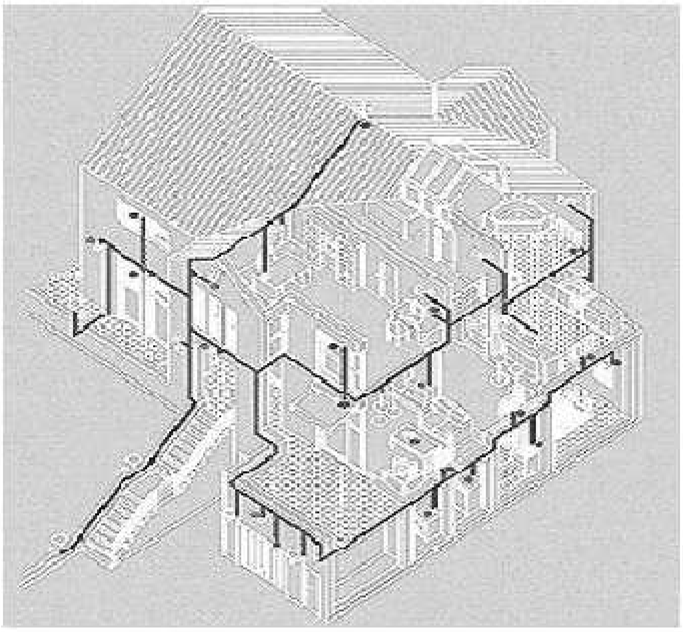


Fig. 3. Structure of KNX/EIB bus tree [Company materials of ABB, Mikulik 2008]

Apart from the sending of telegrams, another task of the bus is to provide the power supply with safe voltage 24V DC i.e. SELV voltage (*Safety Extra Low Voltage*). In the framework of EIB, the measuring, testing and control circuits have been separated from the power supply equipment; therefore the contact of user with the voltage is possible only in the case of SELV voltage [Drop and Jastrzębski 2002, Horyński 2004, 2005, 2006, 2007, KNX 2009, Mikulik 2008]

Such a system encompasses two types of devices: controlling devices – sensors and devices transmitting the signal to the bus. The telegram can also be sent by the device automatically (e.g. if the lighting level setting has been exceeded) or manually (e. g. depressing TRITON pushbutton) and by the actuators – actors receiving the telegrams from the bus and performing the required activities in binary mode (e. g. binary outputs) or generating analogue signals to control other devices [Horyński 2004, 2005, Mikulik 2008, KNX 2009]. Any change of function and changes of characteristics of individual devices are possible by means of ETS software.

BUILDING CONTROL BY MEANS OF KNX/EIB SYSTEM

Contrary to conventional electric system, in order to start KNX/EIB system, apart from the electric integration of bus elements the control system design shall be additionally prepared and the system startup process shall be carried out i.e. adequate applications, previously programmed in the design phase shall be saved in memory of individual devices. An ETS tooling program i.e. European Installation Bus Tool Software is used for this purpose as a standard tool for designing, startup and servicing of KNX/EIB installations. It is distributed by KNX organization with head office in Brussels, ensuring logical compliance of the software on the user interface level.

Operating system	Hardware	KNX network interfaces
Windows 2000 Professional Windows XP, 32 Bit Windows Vista, 32 Bit Windows 7, 32 Bit	1 GHz 512 MB RAM 3 GB HD 1024 x 768	RS232 USB or IP

Fig. 4. ETS3.0f software requirements in the scope of hardware [KNX.org]

Owing to the fact that it is possible to perform control functions in the majority of electric circuits and to take the readings of the actors status, it is also possible to define the work of individual modules in a manner enabling their operation as the safety systems (Fig. 5).

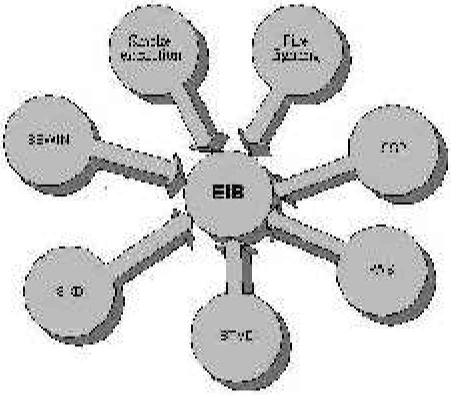


Fig. 5. Integration of components of safety system in KNX/EIB system

For example the following settings can be programmed:

- Automatic lights turning on during night in case of movement detection in a room. Moreover it is possible to send SMS informing abouta the relevant event.
- The simulation of occupants presence is also possible. The programming of individual functions at determined hours is possible by means of ETS program. Therefore it is possible e.g. to turn on the lights or TV or to drop the shutters.
- By means of the module ensuring EIB system integration with the Internet, it is possible to transfer the images of indoor or outdoor cameras and to enforce the corresponding functions of the devices.
- By means of the standard access system it is possible to program corresponding sequences of events in the system e.g. lights turning on, lifting the shutters or turning on the heating.
- In case of hazard detected by smoke sensor, it is possible to activate acoustic alarm or turn on all lights in order to enable quick evacuation.
- In case of building flooding, this event can be detected by relevant sensor and the losses can be limited as a result of the closure of the main valve by the system.
- The system can be programmed in a manner enabling the visualization of the shutters and doors opening status on the display.
- Automatic shutters closure will be possible when the strong wind or rain is detected by weather sensor.
- All statuses qualified by the systems as alarms can be sent to building users in the form of SMS.

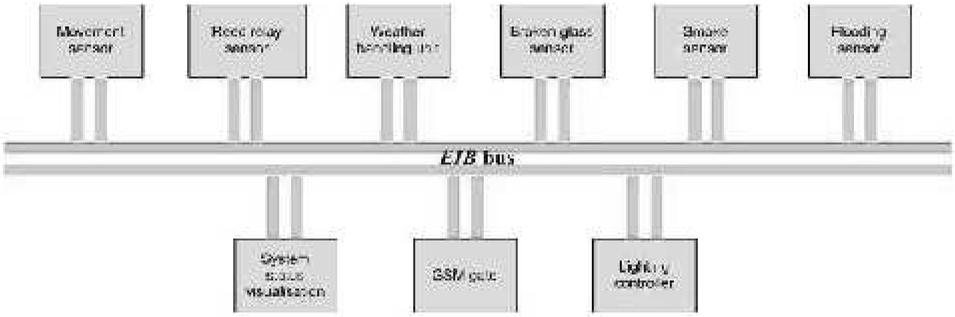
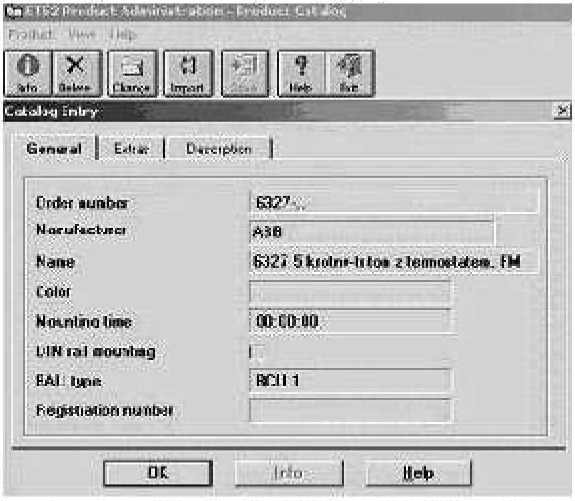


Fig. 6. Examples of modules of KNX/EIB system constituting the building safety system

PROTECTION OF KNX/EIB SYSTEM AGAINST SABOTAGE

The protection of KNX/EIB system against sabotage is as important as the safety systems installed in the building. The intelligence of the system is rather a theoretical feature. The building with such feature may resemble an intelligent being in some respects, but it is unable to learn and to think in abstract manner. Also the anticipation of potential hazard in the form of system sabotage is possible only in accordance with the potential sabotage scenario programmed by the system designer. The protection will be inefficient in case of any deviations from this scenario.

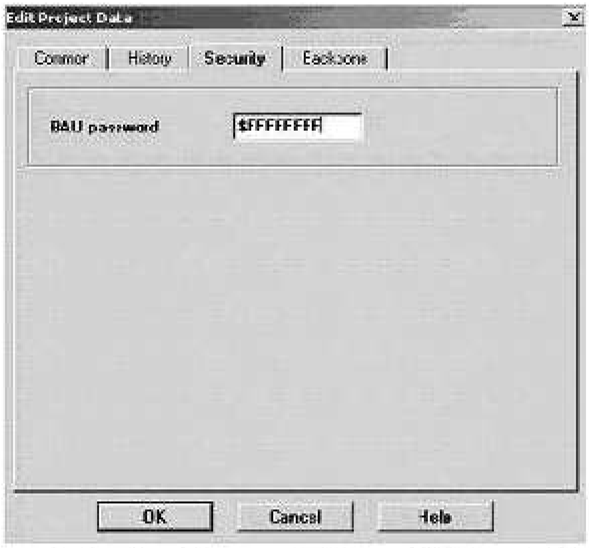
KNX/EIB intelligent system has been provided in certain protective mechanisms, not associated with intelligence feature but preventing potential attack. The bus devices equipped with bus port built in BIM 112 or BCU2 technology are provided with security function enabling the entry of the access password for the configuration setups and application of the devices which have been installed there. The bus port technology is accessible in its documentations and in ETS program used for designing and startup of KNX/EIB system (Fig. 7).



Order number: 6327-...
Manufacturer: ABB
Name: 6327 5 krotny-triton z termostatem. FM
Color:
Mounting time: 00:00:00
DIN rail mounting: □
BAU type: BCU 1
Registration number:

Fig. 7. Catalogue data screen for bus device [ETS manual, KNX.org, Petykiewicz P. 2001]

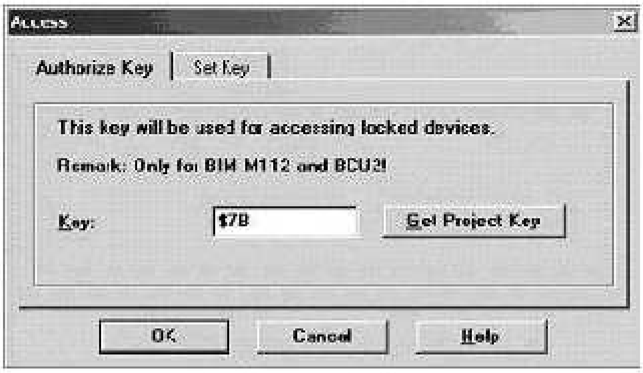
The selection of protections page represents the bus port password (BAU) (Fig. 8).



BAU password $FFFFFFFF

Fig. 8. Bus port safety functions edition screen [ETS manual, KNX.org., Petykiewicz P. 2001]

In order to protect the screen against an unauthorized access, enter an eight character hexadecimal key from the scope 00000000-FFFFFFFF or decimal key from the scope 0-4294967294 into the select field properly prepared in the bus port software for this purpose. It will be protected against the access in the course of entry of physical address and application into the port. In order to unlock the access, the previously entered digital password should be specified. This password is common for all bus ports in the design of an intelligent system (Fig.9).



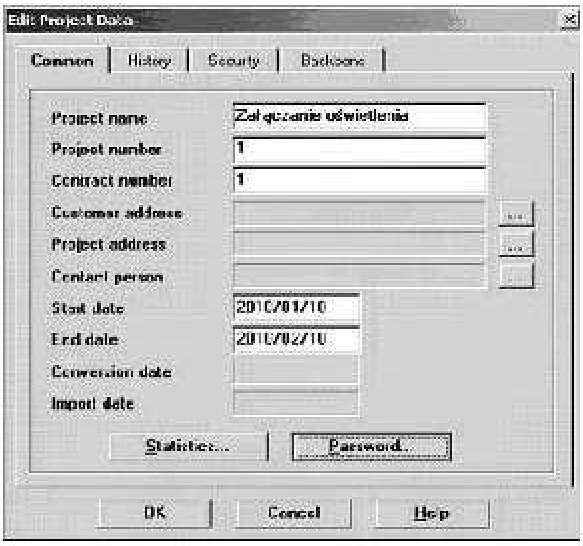
This key will be used for accessing locked devices.

Remark: Only for BIM M112 and BCU2!

Key: $7B

Fig. 9. Access authorization screen to the bus port in BIM M112 and BCU2 technology [KNX.org]

Besides the protections associated with the devices included in the bus system in KNX/EIB installation, the design is also subject to protection (Fig. 10).



Project name	Załączanie oświetlenia
Project number	1
Contract number	1
Customer address	
Project address	
Contact person	
Start date	2010/01/10
End date	2010/02/10
Conversion date	
Import date	

Fig. 10. Deign data edition screen with safety function [ETS manual, Petykiewicz P. 2001]

CONCLUSIONS

Owing to the possibility of the changing of configuration of individual devices, KNX/EIB system functions can be adapted to individual needs of the user. The application of the bus in the tree structure makes further extension or reconfiguration of the system unproblematic. On the basis of KNX/EIB system analysis it has been found out that the system was provided with several functions demonstrating its high fault tolerance and protection against unauthorized access. These functions are particularly important in case of remote access to the system, for instance by means of specially prepared Internet services e.g. domoport.de or private servers equipped with the access and visualization software.

REFERENCES

Drop D., Jastrzębski D., 2002.: Współczesne instalacje elektryczne w budownictwie jednorodzinnym z wykorzystaniem osprzętu firmy Moeller. COSiW, Warszawa.

Horyński M, 2004.: Komputerowo wspomagane projektowanie inteligentnych instalacji elektrycznych, W: Zastosowania komputerów w elektrotechnice ZKwE`2004 : IX konferencja naukowo-techniczna, Poznań/Kiekrz, 19-21 kwietnia 2004, materiały. T.1, Poznań, Wydawnictwo Instytutu Elektrotechniki Przemysłowej Politechniki Poznańskiej, 271-274.

Horyński M., 2005.: Integracja instalacji elektrycznych w inteligentnym budynku, W: Zastosowania komputerów w elektrotechnice : X Konferencja, Poznań, 18-20 kwietnia 2005 : materiały / red. Ryszard Nawrowski, Poznań, Politechnika Poznańska. Instytut Elektrotechniki Przemysłowej, 235-236.

Horyński M, 2005.: Management of the intelligent electric EIB system, W: NEET'2005: New electrical and electronic technologies and their industrial implementation : IV International Conference : Zakopane, Poland, june, 21-24, 2005, Lublin, PWZN ,PRINT-6' Sp. z . oo., 45-47.

Horyński M., 2005.: Programowanie komponentów inteligentnej instalacji elektrycznej w systemie EIB, W: Varia informatica : obliczenia i technologie, Stanisław Grzegórski, Marek Miłosz, Muryjas Piotr [Red.], Lublin, Polskie Towarzystwo Informatyczne, 223-228.

Horyński M. 2006.: Zdalne zarządzanie inteligentną instalacją elektryczną, Motrol: Motoryzacja i Energetyka Rolnictwa, vol. 8A, 142-147.

Horyński M, 2007.: EIB Electrical Installation in Intelligent House - Remote Access, W: New electrical and electronic technologies and their industrial implementation : NEET 2007 : 5th international conference, Zakopane, Poland, June 12-15, 2007 Lublin, Department of Electrical Devices and HV Technology Lublin University of Technology, 77.

2009.: KNX Advanced Course Documentation.

2009.: KNX Handbook for Home and Building Control.

2009.: Materiały firmowe ABB.

Mikulik J. 2007.: EIB - rozproszony system zarządzania budynkiem (cz. 1). Zabezpieczenia.

Mikulik J. 2007.: EIB - rozproszony system zarządzania budynkiem (cz. 2). Zabezpieczenia.

Mikulik J. 2008.: Europejska magistrala instalacyjna, COSiW SEP, Warszawa.

Mikulik J. 2005.: Budynek inteligentny – podstawowe systemy bezpieczeństwa w budynkach inteligentnych. Tom II, Wydawnictwo Politechniki Śląskiej, Gliwice.

Petykiewicz P. 2001.: Nowoczesna instalacja elektryczna w inteligentnym budynku. COSiW SEP, Warszawa.

Plaksina O., Rausch T., 2005.: Fieldbus Systems and their Applications, Vol. 6, Part 1. A Proceedings volume from the 6th IFAC International Conference, Puebla, Mexico 14-25 November.

Polska Norma PN - 93/E-08390.

UŻYCIE INSTALACJI EIB W SYSTEMACH OCHRONY BUDYNKÓW

Streszczenie. Wraz z rozwojem systemów automatyki domowej postępuje stopniowy proces włączenia, czyli zintegrowania z nimi dotychczas odrębnych instalacji. W artykule przedstawiono zagadnienie zapewnienia bezpieczeństwa w nowoczesnych budynkach, zarówno na poziomie użytkownika, czyli ochronę jego zdrowia i mienia jak i urządzeń w nich występujących. Zmiana idei funkcjonowania instalacji budynkowych wprowadziła do zabezpieczeń tych systemów mechanizmy i zasady dotychczas obecne w ochronie systemów informatycznych, np. poczty elektronicznej lub bankowych kont internetowych.

Słowa kluczowe: alarm, magistrala EIB, bezpieczeństwo, integracja, systemy rozproszone