I. J. Computer Network and Information Security, 2013, 9, 1-8
Published Online July 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.09.01

Method and System for Protection of Automated Control Systems for "Smart Buildings"

Dmitry Mikhaylov, Igor Zhukov, Andrey Starikovskiy, Alexander Zuykov, Anastasia Tolstaya, Maxim Fomin

National Research Nuclear University "MEPhI", Moscow, Russia
mdmitry@mephi.ru, i.zhukov@inbox.ru, userandrew@rambler.ru, avzuykov@gmail.com, polynna@yandex.ru, fominmi@gmail.com

Abstract **–** The paper is related to system and method for protection of an automated control system (ACS) against un-authorized devices connected to the ACS via wired or wireless channels that substantially obviates the disadvantages of the related art. The protection system monitors the signals spreading in the network analyzing the performance of the network for malicious code or hidden connections of attacker. The system is developed specifically for this purpose and it can protect the industrial control systems more effectively than standard anti-virus programs. Specific anti-virus software installed on a central server of the automated control system protects it from software-based attacks both from internal and external offenders. The system comprises a plurality of bus protection devices of different types, including any of a twisted-pair protection device, a power lines protection device, On-Board Diagnostics signal protocol protection device, and a wireless protection device.

Index Terms **–** automated control systems (ACS), protection system, anti-virus, twisted-pair, power lines, radio channels.

I. Introduction

Today different automated control systems (ACS) are getting more and more popular. ACSs are widely used for controlling various technological processes. They include not only systems performing separate functions (video surveillance, fire, access control, etc.) but also integrated solutions that combine a great diversity of sensors and devices.

Automated control systems are multifunctional, and therewith complex.

These systems typically include hardware and software means for automated control of technological processes and equipment at production sites equipped with automated production lines (i.e., a plant or a factory). The automated control systems provide control and monitoring of various modules and subsystems of the automated production system and other automated systems at the production site.

Typically, an automated control system controls power supplies, an alarm system, a lighting system, a video surveillance system, an air conditioning system, a heating system, etc (Fig. 1).

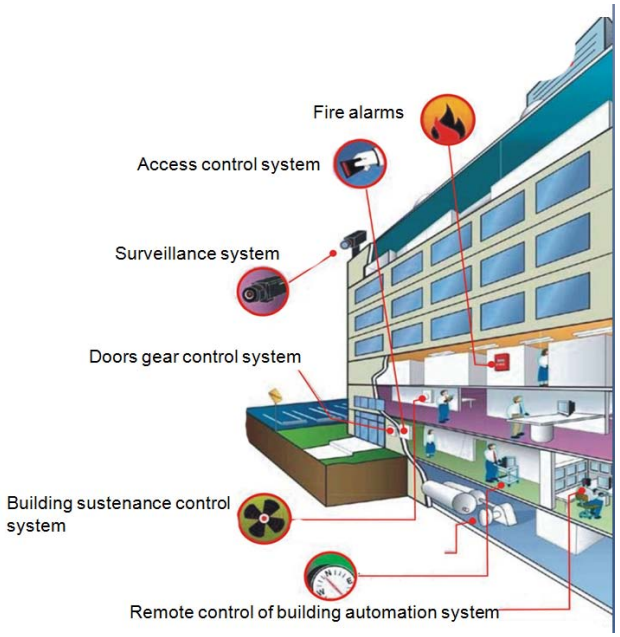

Figure 1. Elements and systems controlled by automated control systems [1].

Additionally, the automated control systems can be responsible for access control to a production site (or a building). Some sophisticated ACSs can be used for complex engineering objects that have a strategic importance for a country. For example, the automated control systems are used at nuclear (or hydroelectric) power plants, military bases, places of mass gathering of people, such as airports, train stations, malls, etc.

The paper is organized in the following way:

- introduction telling about main tendencies in the field of automated control systems;
- description of basic principles of functioning of viruses for automated control systems including the main channels of virus propagation;
- description of the proposed protection system from un-authorized devices connected to the ACS via wired or wireless channels;
- conclusion.

II. Basic Principles Of functioning of Viruses For Automated Control Systems

The combination of different technologies in the construction and the growing complexity of an automated system increase the number of possible grave shortcomings in terms of security. At the same time, such vulnerabilities attract attention of intruders and cyber criminals because of the possibility to obtain valuable, often confidential, information and control over vital systems.

The problem lies within the fact that the server software is usually installed on a dedicated computing machine. This machine is connected with many assistive devices for data transmission, for example, GSM modems, Bluetooth transmitters and Wi-Fi access points. [2]

In addition, the software for work with a local computer network of the building is often installed on the server of automated control system. In fact, it turns out that this computing machine has a large piece of software responsible for all incoming data processing.

The main channels of the virus propagation are:

- Bluetooth channel
  Bluetooth networks are extremely fragile and can easily receive the file with a virus from the attacker without authorization request;
- Wi-Fi channel
  Wi-Fi network can be easily compromised by an attacker and he or she can bypass authentication system by transmission of the virus to the server of ACS;
- HTTP channel for remote access
  HTTP exchange with the Internet can be one of the channels of infection of automated control system of the building. Vulnerabilities of software built on the HTTP protocol are well known [3];
- GSM channel
  Unauthorized system control can be also performed via GSM channel. It can be done, for example, by sending the SMS-message with a fake sender's number that contains malware or hazardous commands;
- Paired channels
  If the server of the automated control system is also connected to the local network the malicious program can easily get to the machine from the network;
- Pre-install the software and logic bombs
  This channel of infection of the server software of automated control system means that during the installation of the control system for intelligent building, an intruder, for example, entering into the confidence of the client, installs the malicious software on the server of ACS. Prove that the virus is installed with an evil intent is impossible. It is also hard to detect such a virus because comprehensive anti-virus software for automated control systems does not exist. [2], [4], [5]

As it is mentioned above, full anti-virus systems providing comprehensive protection against malicious software designed specifically for automated control systems does not exist. Moreover, the program code for typical viruses for ACSs cannot be recognized by most scanners signatures. [2]

The basic vulnerabilities in software systems of ACSs used by attackers to introduce malicious software are:

- lack of possibility of blocking the connection of un-authorized devices;
- lack of control over the broadcast of datagrams in an automated control system`s network;
- lack of authentication of program that transmits packets in an automated control system`s network.

There are several types of virus programs, which can be classified on the basis of the purposes they used for.

1. Viruses, performing control.

In most cases the viruses for "Smart Buildings" can be used to manage the building. These viruses are used by hackers to perform acts of terrorism, to put on and off different equipment, to disable detection system of un-authorized access to the building, and other actions of this kind.

2. Viruses, intercepting information.

These viruses are aimed at intercepting and transmitting information from the ACS to an intruder. These viruses can collect data from different devices, about people in the building as well as access codes. In addition, they can, for example, capture files sent to the printing device.

Transfer of information outside these viruses is carried out in most of the same channels by which they came to the victim's server building.

An intruder may perform an attack on the "Smart Building" systems using a covert channel of data transmission. The attacker could get data, using information about the relative timing of events. There is also a possibility to make an attack based on the resource lock [6].

Moreover, open wiring used to control automated control system makes it possible to connect the system by means of "insert" in communication line.

However, the current automated control systems are not protected from rising malware and computer virus threats. The conventional systems do not have any means for detecting that any un-authorized devices or systems (i.e., the devices not declared in the original documentation) are connected to a given automated control system. Furthermore, there is no anti-virus product adapted for use in the ACSs. The conventional anti-virus applications are not reliable within ACSs, since they are mainly designed for different types of threats.

Accordingly, there is a need in the art for an efficient and effective system and method for protection of the automated control systems.

III. The Proposed Protection System For Automated Control Systems

The system for protection of an automated control system comprises:

- at least one data bus having at least one bus node of a certain type;
- a bus protection device connected to the data bus or node;
- an interface converter integrated into the protection device for converting a signal received from the data bus into internal device interface;
- a module within the bus protection device for checking electric parameters of the received signal;
- a processor of the bus protection device having a module for protection against malicious packets;
- a workstation connected to the bus protection device, wherein the workstation analyses data received from the bus protection device.

The proposed protection system of an automated control system consists of:

- a processor;
- a memory coupled to the processor;
- a computer program logic stored in the memory and executed on the processor, the computer program logic for implementing the below-specified steps (method).

The method for protection of an automated control system of a building comprises:

- analyzing the ACS for presence of un-authorized devices and un-authorized connections;
- detecting undocumented devices connected to the ACS;
- identifying suspicious commands from connected devices;
- detection of ACS activities;
- analyzing different network frequencies for un-authorized data transmissions;
- maintaining device activity logs.

The protection system includes protection from un-authorized devices or un-authorized connections. The system also controls network resources and transmitted data.

The automated control system is protected in the following areas:

1. protection of the ACSs that use power lines (i.e., for example, X10) for data transmission (Fig. 2);

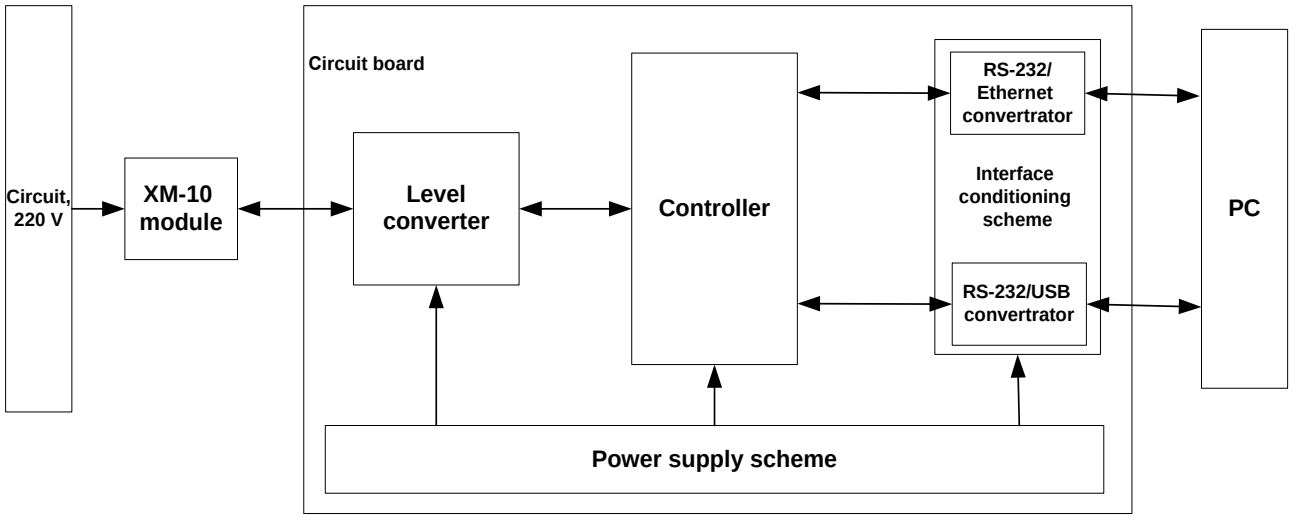

Figure 2. Scheme of X10 control and protection module.

2. protection of the ACSs that use data transmission over a twisted-pair KNX (i.e., for example, protocols INSTEON, BACnet, LonWorks, C-Bus, AMX, Beckhoff I/O, SmartUnity, LON, Crestron, EnOcean, ZigBee, Z-Wave, DALI) or using industrial Ethernet (Fig. 3);

3. protection of the ACSs that use radio channels (e.g., Wi-Fi, Wi-Max, ZigBee, Bluetooth, GSM, Tetra) for data transmission (Fig. 4).

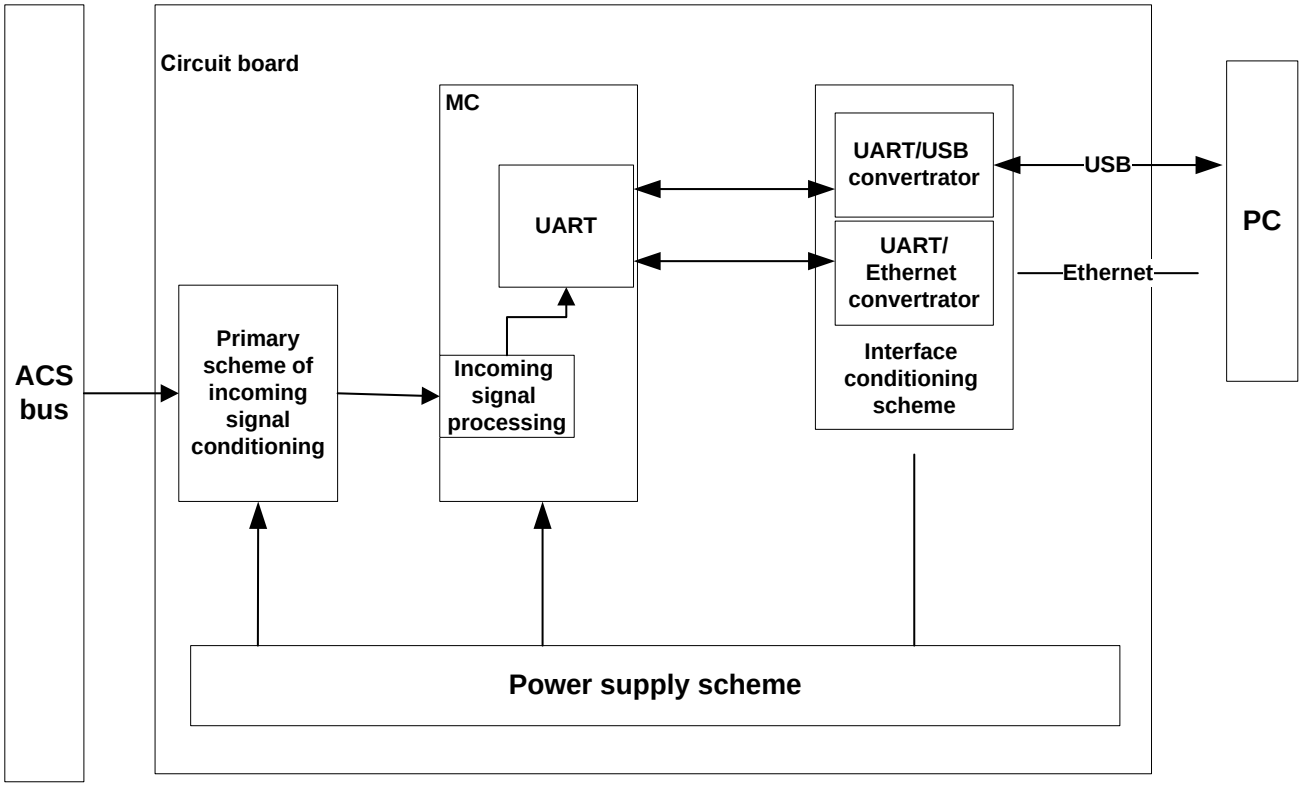

Figure 3. Scheme of KNX control and protection module.

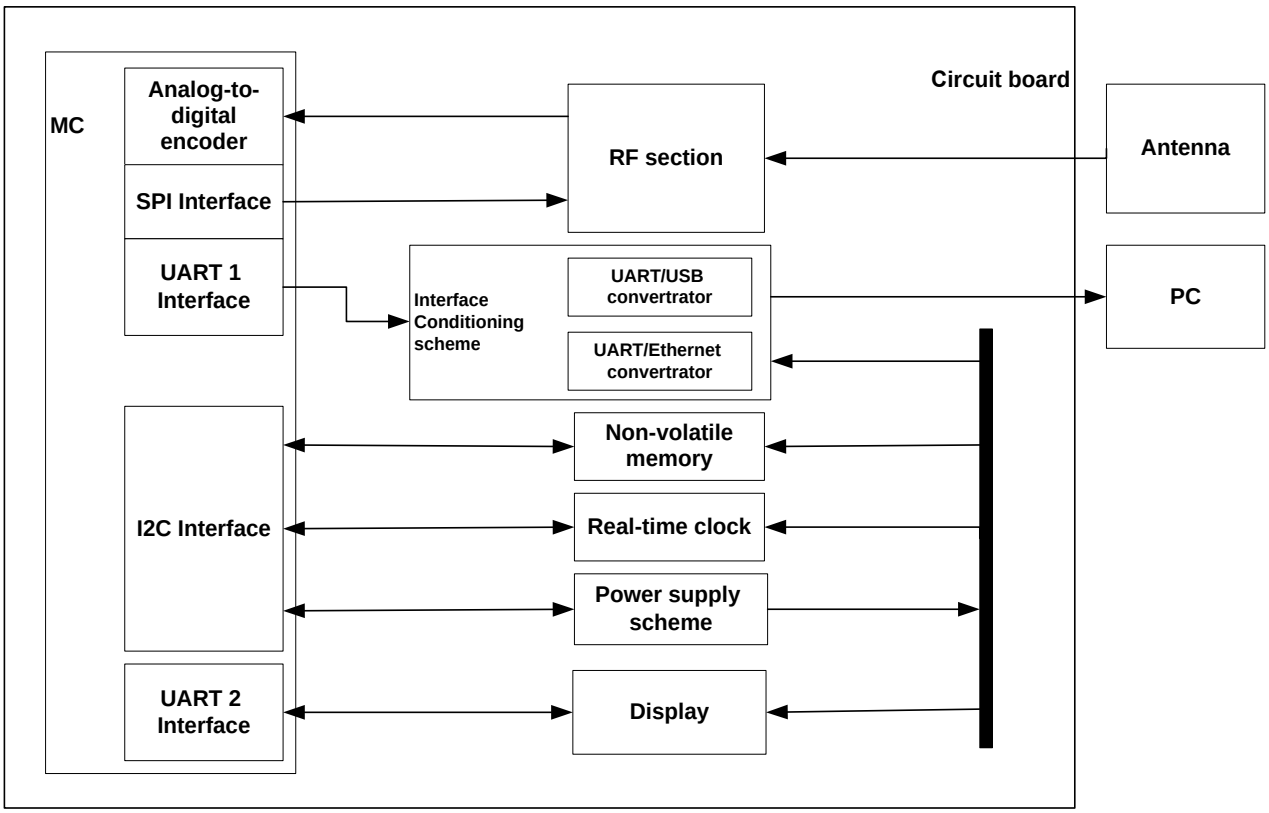

Figure 4. Scheme of wireless protocols` control and protection module.

The automated control systems are protected from connection of new (un-authorized) devices by constant monitoring of commands transmitted over system network. At any given moment a user can obtain data about the commands transmitted over the data channel. If an un-authorized device connects to the line, the protection system notifies the user about un-authorized data transmission and saves all the relevant data (i.e., time, data, executed command, addresses of sender-devices and addresses of receiver-devices).

In order to monitor and detect un-authorized devices, the protection module is placed onto the network (Fig. 5).

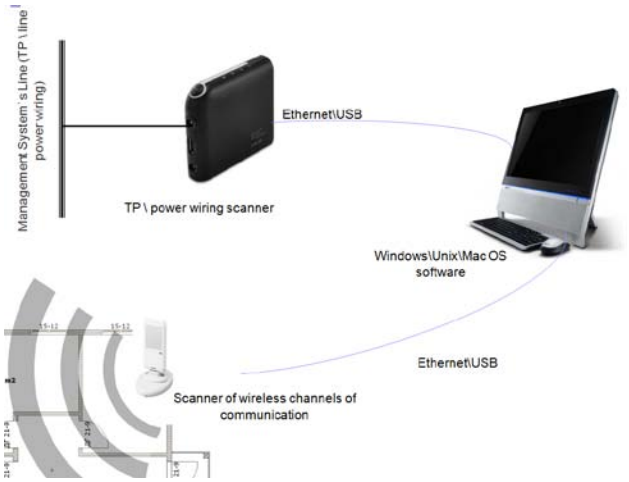

Figure 5. The scheme of provision of ACS`s information security by proposed protection system.

The protection system allows collection of statistics of the events occurring over the data transmission channels. Then, the statistics are analyzed using graphical representations and data filters. The statistical data can be filtered by time (i.e., for example, show all transmissions over last three days) and by content (i.e., for example, show all commands for switching off). The filtering parameters can be combined arbitrarily.

Additionally, if the commands are modified and differ from the ones described in the system protocol, all data transmission attempts are detected and prevented. The user is notified about a potential threat.

Then, the data can be analyzed using graphs and tables. For example, if a packet length differs from the length allowed for a given type of ACS or, if a portion of the packet containing odd/even flag does not match the correct value for this packet, the user is notified about a potential threat.

The protection system can survey all device addresses within the system for their activity. As a result, the user can have a complete picture of all of the devices that are currently present in the system. Even if the un-authorized device is inactive, it will be detected by the user.

The above mentioned features of the protection system are effective for automated control systems having a twisted-pair data bus, as well as for the systems that use power lines (for example, X10). The protection system controls the network resources and the transmitted data as follows. The protection system employs a filtering module for filtering network traffic. The network packets are filtered using special filtering rules (set of parameters). The system is protected from un-authorized access to subsystem data and the protection system notifies the user of all suspicious traffic, attempts to infiltrate into the sub-network or system attacks.

The protection system also protects against overloads (and attacks) of telecommunication devices that result in errors. The outgoing traffic from a sender-device incoming into a protected device is limited by the protection system. Additionally, dynamic allocation of network identifiers of devices (ports, MAC addresses, IP addresses) is used. Furthermore, the system uses device duplication for higher reliability. The backup (duplicate) devices are implemented in exactly the same way in order to defend the system against a denial of service attack targeted at one device.

The data transmitted between system components of the automated control system are protected from being falsified. In order to protect data, a special set of symbols is added to check for data integrity and to authenticate the data source.

Alternatively, the data can be encrypted by an encryption module that encrypts only part of the network traffic. Thus, a remote user of the automated control system can exchange data with other network resources without additional encryption. The protection system also protects ACS from un-authorized access by allocating only certain time periods for reading and writing data in which the user can access the automated control system`s network to get and to send data.

The protection system prevents unauthorized use of a data channel. It analyses the data channel and detects un-authorized data transmissions that use a protocol different from a protocol of a given system. For example, if the structure of transmitted packets differs from the structure used in a given ACS, the packets are intercepted.

The protection system continuously monitors the data channel and as soon as a command appear on line, the system checks if a device with a declared address has actually sent this command through the network. If the device with the declared address has not sent anything at the moment, the protection system notifies the operator and the received message is saved.

The wired data channels are analyzed in a wide range of voltage and frequency. For example, in case of KNX data channel using twisted-pair (having parameters 30 Volts constant between the lines, signal amplitude 5 Volts, and data transmission frequency 9600 Hz), a signal with an amplitude or frequency that is different from the KNX parameters is detected by the protection system and the user is notified of an un-authorized transmission.

The proposed system can be used with all existing protocols: INSTEON, BACnet, LonWorks, C-Bus, AMX, Beckhoff I/O, SmartUnity, LON, Crestron, EnOcean, ZigBee, Z-Wave, DALI, Lan Drive and LCN.

The information related to the transmitted data (time, data of transmission, frequency, signal amplitude, transmission length etc.) is saved.

Thus, the protection system collects the statistics of the data channel events. The collected statistics can be analyzed using graphs or by applying time and/or content filters. The protection system also works with the "Smart Building" ACSs that use power lines data channels. For example, X10 data channels use power lines 220/110 Volts (50/100 Hz).

In order to limit access to the transmitted data, the communication channel is divided into:

- a data channel that serves for transmitting data between the system devices, controllers and computers, and
- a control channel that serves only for sending the commands to control and measuring devices.

The system for protection of radio channels is implemented. Most of the modern buildings have Wi-Fi, Bluetooth and GSM devices [2]. Their radio channels can be used by intruders for eavesdropping. The system monitors activities of all radio devices in a wide frequency range from 400 MHz to 3000 MHz.

If an un-authorized transmission is detected on a radio channel, the protection system informs a user and records the transmission frequency and power. This data is used in further analysis. The collected statistics are shown by charts (i.e., spectral characteristics) reflecting power and frequency of all of the transmissions over a period of time selected by the time filters.

A separate frequency range can be monitored, for example GSM range (850 MHz, 900 MHz, 1800 MHz and 1900 MHz). Thus, the protection system can guarantee security of confidential conversations.

If an active transmitter is detected or somebody has a cell phone on, the protection system notifies the user. Additionally, it can find persons who break the rules in offices having Wi-Fi, where this type of data transmissions is not allowed.

The protection system controls the integrity of the automated control system. It blocks possible substitutes of connected dynamic libraries and limits read and write of system critical data operations by external processes. Thus, the data reflecting system operations, reports, strategic data, etc. is protected. Alternatively, these data are encrypted.

The protection system employs a blacklist of digital certificates that are used for subject identification and determination of operations allowed for this subject. Any actions by the subjects, with digital certificates that belong to the blacklist, are blocked.

The developed system checks the file system and the processes executed in the memory during the protection system functioning. It compares state of the processes and parameters of the files against their previous or expected values.

The protection system of ACS maintains a list of signatures for accurate identification of files and processes that are most commonly used and notifies the user once a file or a process with a wrong signature is detected.

Additionally, the protection system duplicates software processes. The parameters of duplicated processes and executed actions are compared to each other in order to detect the differences that are reported to the user or an administrator. If the main process fails, the duplicate process is executed.

The proposed protection system of "Smart Building" blocks any un-authorized attempts to use the system functionality and protects it from unknown possible threats. Any un-authorized attempts to access a file system, system configurations or data channels are detected. It also automatically scans external application for malware components, suspicious executable instructions and for calls for system functions.

Additionally, the protection system checks device operations using behavior patterns (the pre-defined or predicted pattern of device's functioning sequence). The behavior pattern can be created before hand or during the execution of the process. The behavior pattern is periodically updated.

The communication network is divided into independent segments, in order to limit the access to some devices in case of malicious activity occurring in one part of the ACS network.

The protection system detects interruptions of data transmission, unexpected changes in traffic speed, deviations in electric and electro-magnetic parameters, as well as noise in the data channel. All of the detected anomalies are reported to the system administrator of the automated control system.

The protection system controls and limits interactions with the external data media. The external media employed by the system use a proprietary file system that allows read/write operations to be performed only by a limited set of trusted devices.

Alternatively, the external data media has a unique digital signature. When the external media is connected to a device, the signature is checked first. If the signature is verified, the device is allowed to exchange the data with the media. Otherwise, the data exchange is blocked.

As yet another alternative, the external media has a list of trusted devices and a module for acquiring device identifiers. The device identifiers are read first and, if the device is trusted, the data exchange is allowed. If the media is connected to an untrusted device, the data can be automatically erased from the media.

The device actions with connected external media are logged. The device that connects to the external media stores a full history of modification of each object located on the external media (i.e., files, catalogs and links). All object versions are also stored on the device.

One key is stored on the external data media and another key is stored on the device. The data on the external data media is encrypted with both keys. The keys can be dynamically changed as long as the correlation of the keys remains the same. Each device that connects to the external data media can have a unique pair of keys. Thus, the data on the external media can be decrypted only by the device the data are intended for.

As yet another option, the communication channels within the automated control system can use encryption, implemented in hardware, software, firmware, or any

combination thereof. Each device connected to the ACS may be front-ended by an encryption module This has the effect of replacing an unsecure bus of the automated control system with a secure one, which significantly reduces the probability of an unsanctioned connection to the ACS for the purposes of sending false commands or data.

The encryption module converts any outgoing data of a device that it front-ends to a secure bus format, for example, using AES [7], DES [8], RSA [9] or other algorithms. Also, each can include a digital signature of the sender, which permits the receiving device to authenticate the sender and then decrypt the packet. The decryption key can be hardwired into the device or can be generated using Diffie-Hellman technique [10], for example.

VI. Conclusions

This paper is devoted to description of a new method and system for protection of an automated control system against un-authorized devices and connections. The protection system includes protection from un-authorized devices or un-authorized connections. The system also controls network resources and transmitted data.

The developed protection system of automated control system solves the following problems:

- protection of automated management systems, built on data transmission over power lines, for example, X10;
- protection of automated management systems, built on data transmission over twisted-pair, for example, KNX, C-Bus, use of Industrial Ethernet;
- protection of automated management systems, built on data transmission over the air, for example, Wi-Fi, Bluetooth.

The protection of the automated control systems includes the following features:

- analyzing a system for presence of un-authorized devices or un-authorized connections;
- detection of undocumented (i.e., not declared) devices and suspicious commands from connected devices;
- detection of various types of activities (i.e., wrong packets, unidentified activities, certain types of commands, etc.);
- analyzing different network frequencies for data transmissions;
- maintaining device activity logs;
- performing automated database searches for any parameter or set of parameters;
- implementing graphic analysis of ACS device activities.

Work is underway to increase the number of supported protocols and to study new methods of ACS protection.

References

[1] Dmitry Mikhaylov, Igor Zhukov, Andrey Starikovskiy, Alexander Zuykov, Anastasia Tolstaya, Stanislav Fesenko and Stepan Sivkov. Hardware-software complex ensuing information security of automated building management systems. International Journal of Application or Innovation in Engineering & Management, Volume 2, Issue 3, March 2013. P 408-412. URL: http://www.ijaiem.org/Volume2Issue3/IJAIEM-2013-03-27-092.pdf.

[2] Starikovskiy A.V., Zhukov I.Yu., Mikhaylov D.M., Tolstaya A.M., Zhorin F.V., Makarov V.V., Vavrenyuk A.B. Research on vulnerabilities of digital home. Scientific-technical Journal "Special Equipment and Communication" №2, Moscow 2012. Pages 55-57.

[3] Kasperski K. Notes of researcher of computer viruses. St.-Petersburg.: "Piter", 2006. 216 p.

[4] Babalova I.F., Shustova L.I., Pronichkin A.S., Aristov M.I., Evseev V.L., Fesenko S.D. Attacks on automated management systems based on vulnerabilities of wireless data transmission channel Wi-Fi. Scientific-technical Journal "Special Equipment and Communication" №4, Moscow 2012. Pages 20-22.

[5] Beltov A.G., Novitskiy A.V., Pronichkin A.S., Krimov A.S. Attacks on automated management systems based on vulnerabilities of digital data transmission devices. Scientific-technical Journal "Special Equipment and Communication" №4, Moscow 2012. Pages 26-28.

[6] Zhukov I.Yu., Mikhaylov D.M., Starikovskiy A.V., Smirnov A.S. Covert channel of data stovepiping in automated building control systems. Scientific-technical Journal "Special Equipment and Communication" №4, Moscow 2012. Pages 9-11.

[7] "Specification for the ADVANCED ENCRYPTION STANDARD (AES)". Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001. URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[8] Gilmore, John, "Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design", 1998, O'Reilly.

[9] Bakhtiari M., Maarof M. A. Serious Security Weakness in RSA Cryptosystem // IJCSI International Journal of Computer Science. — January 2012. — В. 1, № 3. — Т. 9. URL: http://www.ijcsi.org/papers/IJCSI-9-1-3-175-178.pdf.

[10] Diffie-Hellman - technical definition. Computer Desktop Encyclopedia. URL: http://computer.yourdictionary.com/diffie-hellman.

Dmitry Mikhaylov, PhD, associate professor of National Research Nuclear University "MEPhI", Moscow, Russia. Computer Systems and Technologies Department.

Igor Zhukov, Doctor of Engineering Science, Professor. National Research Nuclear University "MEPhI", Moscow, Russia. Computer Systems and Technologies Department.

Andrey Starikovskiy, teaching assistant of National Research Nuclear University "MEPhI", Moscow, Russia. Computer Systems and Technologies Department.

Alexander Zuykov, Ph.D. candidate of National Research Nuclear University "MEPhI", Moscow, Russia. Computer Systems and Technologies Department.

Anastasia Tolstaya, graduate of National Research Nuclear University "MEPhI", Moscow, Russia. Department of Management and Economics of High Technologies.

Maxim Fomin, graduate of National Research Nuclear University "MEPhI", Moscow, Russia. Department of Automation and Electronics.

