Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FIRE ALARM SYSTEM COMMUNICATION PROTOCOL RESEARCH BASED ON THE COMPONENTS OF THE "BOLID C2000M" SYSTEM

S.D. FESENKO, Y.Y SHUMILOV, A.D. EGOROV, A.S. FILIMONTSEV, A.A. SHINKARENKO, D.T. RUBIN, V.L. EVSEEV

National Research Nuclear University "MEPhI" (Moscow Engineering Physics Institute), Kashirskoe highway 31, 115409, Moscow, Russian Federation

E-mail: stas_fesenko@mail.ru, shumilovyy@gmail.com, egorovalexeyd@gmail.com, asfeliks@mail.ru, antonshink@yandex.ru, mr.dmitry.rubin@gmail.com, vlevseev@mephi.ru

ABSTRACT

This article considers the issues of engineering systems as a particular case of automated control systems information security from unauthorized access to the automation equipment. That includes intruders and threats classification. Next, on the basis of the obtained data, algorithms for the analysis of closed protocols in such systems are developed. Practical research of a typical engineering system protection was also described, for this purpose the data transfer protocol used by the system "Bolid C2000M" was studied. This work is a preliminary step for further development of the device protecting the system from an unauthorized access.

Keywords: *Cybersecurity, Engineering Systems, Fire Alarm System, Automated Control System, Communications Links, Data Transfer Protocol.*

1. INTRODUCTION

Currently, information systems (IS) are the basis of most life processes. Information system is a combination of technical equipment, software, hardware and resources for classification, storing and processing information [1].

An automated control system (ACS) is a particular case of IS [2]. ACS are used everywhere in one form or another. There are many ACS classifications [3] by the scope, the architecture, the set of tasks.

Today the information tools allow intruders to perform a breach of an ACS aiming at causing malfunction, information theft or substitution without significant financial and time expenses [4-6]. The possible attacks aimed at APCS are especially critical. Harmful impacts aimed at a large-scale manufacturing enterprise can first breach the synchronicity of APCS commands, then affect the field level equipment, disrupt the technological process. The consequences of such actions can have irreversible nature and cause both material and moral damage.

For example, in 2010 the experts found virus "Stuxnet" at the uranium enrichment plant in Natanz. It was the first virus infecting programmable controllers. It is assumed that the infection took place in June 2009. The virus has infected the computers of employees, then through USB drives got to the control equipment. Seizing control of the automation object, the virus put IR-1 centrifuges out of operation. [7]

This attack is significant because it is the first incident of harmful impacts on the object of critical infrastructure using APCS vulnerabilities. Further, parts of the original Stuxnet virus worm formed the basis of new viruses for APCS: Duqu, Flame, Gauss [8].

In addition, APCS are notable for large extension and low degree of access control on the object, which gives the attacker a chance to connect to the system, cutting into any signal line on the site. Engineering systems is a special case of APCS.

Modern automation engineering systems is widespread [9]. These include ventilation, heating, air conditioning and air recirculation, power distribution, intelligent video surveillance system, monitoring, access control and many others. In some cases, it is the engineering systems that determine the functional safety of automation systems.

A very common use case for an automated approach in everyday life is the fire alarm system. Such systems are required to be installed into all

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

industrial, office, trading buildings and any crowded areas such as train stations, airports, museums, etc. [10]. Fire alarm systems were selected as the object of study because of being widespread.

A characteristic feature of the fire alarm systems is that, despite a wide range of manufacturers, a large number of models and architectures, all such systems are based on similar principles [11]. Thus, the protection algorithms created for a specific fire alarm system can be used to ensure the security of any fire alarm system.

Research for the development of safety devices for fire alarm system has become urgent because of the growing attention to the issues of cyber-security of automated systems in general, and of engineering systems of buildings in particular, and also because of the active development of regulatory and legislative base of the Russian Federation in the field of automate d systems [12].

This problem has been selected for the study as the reviewed by the authors literature has no information about the studies of the problem.

2. THE DATA TRANSFER PROTOCOL STUDY

Within the framework of studying the data transfer protocol used in the fire alarm system "Bolid C2000M", an experimental stand comprising the basic components of the studied system was made. To determine the most likely channels of harmful impacts a classification of possible intruders and possible threats was created. Next, the problem was the formally set to analyze package for communication channels of engineering systems based on the 2-wire communication lines, and package analysis algorithms were developed. The efficiency of the developed algorithms for analyzing the "Bolid C200M" data transfer lines packages was experimentally verified.

2.1 Description of the System Studied

Sections and subsections should be numbered and titled as 1.0, 2.0, etc. and 1.1, 1.2, 2.1, 2.2, 2.2.1, etc. Capital letters should be used for the section titles. For subsections, the first letter of each word should be in capital letter and followed by small letters. One line space should be given above the sub section while no space should be given below the heading and text.

As an object of the practical study a fire alarm system "Bolid C2000M" was selected. This technical equipment has a number of functional capabilities (high number of sensors, simplicity of installation, adjustment and use, the integration with fire distinguishing tools and so on), which ensured the high demand in the market of fire alarm systems [13].

"Bolid C2000M" (see Figure 1) fire alarm system is one of the most advanced systems of this class and it is widespread in Russia. For instance, new stations of SUE "Moscow metro" are equipped with it. "C2000M" is intended for gathering informational from fire alarm devices to organize a single management center and collect system messages, to merge alarm circuits in sections, create cross-links between sections and outputs of different devices, and enrich information display capabilities [14].

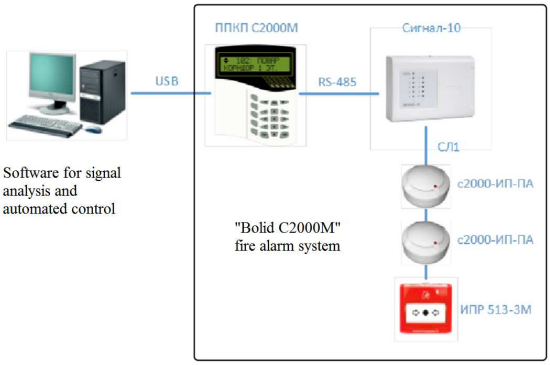


Figure 1: Diagram of the "Bolid C2000M" Fire Alarm System.

The "Bolid C2000M" system comprises:

- FCIE "C2000M" (ППКП «С2000М») is intended for use as control and indicating equipment, management and access control equipment in the complex of technical means of security and fire alarm systems, management and access control systems and automated fire equipment. Programmable from a PC via the USB interface;
- The signal-10 (Сигнал-10) is the fire and security alarm control and indicating equipment intended for use in standalone mode or as part of integrated automated fire alarm systems, at industrial, commercial and residential objects (enterprises, banks, offices, hospitals, shops, warehouses, residential buildings etc). It is the signal lines switch.
- C2000-SF-SA (С2000-ИП-ПА) are specific fire smoke alarms;
- MFA 513-3M - manual fire alarm.

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

This is the minimum required configuration for a fully functioning "Bolid C2000M" fire alarm system. Thus, this configuration will reduce the complexity of the analysis, allowing the testing to be performed in full.

2.2 Intruders and Threats Classification

Due to the urgency of the problem of information security of automation engineering systems [15], [16] the problem of fire alarm system protection from unauthorized access was solved first. Different ways of obtaining unauthorized access can be divided into two fundamentally different classes by type of access (Figure 2):

- Inside access, i.e. when the intruder attempts to gain access from inside the system. This intruder may be, for example, the security officer of the enterprise on which the system is installed, staff or someone who illegally resides on the site.
- Outside access, i.e. when the intruder attempts to gain access to the system from the outside world by means of cutting into external communication channels.

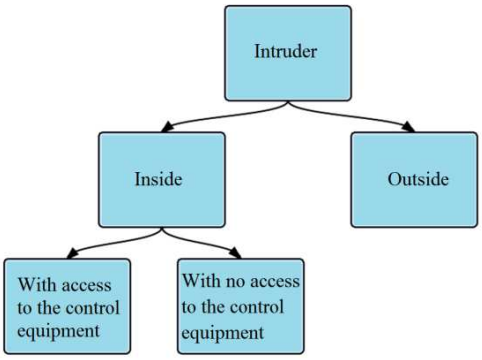


Figure 2: Intruders Classification Scheme.

Usually fire alarm systems, including "Bolid C2000M", are isolated to the automation object, i.e. have no external communication links. It eliminates the possibility of the access from outside the system. Thus, fire alarm systems can be accessed only from within. Insiders can also be divided into several types according to the access level [17]:

- Insider has access to the control equipment. Typically, the control panel of such systems are located in isolated areas. Therefore, personnel and site security have access to it.
- Insider does not have access to the control equipment. In this case, the harmful effects may be directed to the communication links of the system located in the building. This type of insiders is the most likely one. In addition, in this case, the attacker can act secretly, which increases the risk associated with his activities.

The most interesting case from the security point of view is the case of the insider that does not have access to the control equipment, as such insider is much more difficult to detect [18]. The most dangerous threats [19] originating from this type of insiders are presented below (see Figure 3):

- Bringing communication channels of the fire alarm system out of operation, which violates fire security of the protected object.
- Substitution of data transmitted in the data transfer system, with the purpose of obtaining unauthorized access to the control equipment. The result of it may be:
  - Full control over the system.
  - Substitution of sensor signals to cause false alarms or incorrect system response in case of alarm.

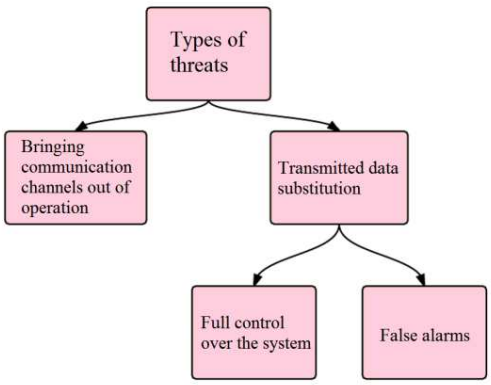


Figure 3: Types of Threats.

Considering the threats listed, it may be noted that intelligent security tools of automation systems based on hardware-software electronic means may not be applied to protect against threats of physical disruption of communication links, as well as from threats of gaining full unauthorized control over the system. These threats should be eliminated by organizational measures and functional safety. However, it is possible to detect the substitution of signals from sensors and smart devices in the network using a hardware-software complex for automation systems protection. In addition, such harmful impacts on the automation system can be hidden and hard to detect using standard automation tools. Therefore, next we will focus on the detection of such malicious actions.

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2.3 Formal Packages Analysis Problem Specification

Due to the use of closed communication protocol in data transmission line ("Signal line" according to manufacturer specifications) of any complex fire alarm systems, it is necessary to analyze the signals of the sensors of this system as per normal and in case of a fire alarm. Signal analysis is performed by identifying consistent patterns in the waveform of the signal from the sensors.

The waveform represents a set of m time series $X_j,\ j = \overline{1,m}$, m is the number of sensors in the fire alarm system. In practice, these time series contain a finite set of values. For each sensor $X_j = \{x_{j1}, x_{j2}, \dots, x_{jn}\}$ with discrete intervals T, dependent on the configuration of the oscilloscope. Where n is the number of captured signal values. $x_{jl} = \{0,1\},\ i = \overline{1,n}$.

As two-wire communication line are exclusively used in bus bars in fire alarm systems (this reduces the cost of installation and maintenance of system) [11], the sensors' scanning in the system is repeated after a certain interval of time ΔT, and the sequence is strictly defined – from the first to the last sensor m. Based on the physical features of the two-wire line, it can be concluded that between scanning every next sensor there will be a time delay Δt, that is different from ΔT, associated with the need to charge sensors (during the delay time the capacitors of the sensor is charged).

It is important to note that the pause Δt is definitely longer than the informative signal [20]. The informative signal of each sensor is a time series $S_t = \{sb_t, sig_t, stb_t\}$, which begins with a start bit sb_t, and ends with a stop-bit stb_t sig_t is a data package, where sb_t, sig_t, stb_t are some time series. Moreover, the duration of the informative signal of each sensor is denoted by ΔS_t. In addition, because any system must uniquely differentiate each iteration of the sensors' scanning cycle from one another, we can draw the following conclusion, which will form the basis for further analysis:

$$\Delta T > \Delta t > \Delta S_i$$

Thus, for the analysis of packages it is necessary to determine ΔT, Δt, ΔS_i, as well as to receive the signal $S_t,\ i = \overline{1,m}$, extract the start and stop bits sb_i, stb_i and the informative signal sig_i itself.

2.4 Algorithm Description

In order to analyze directly the informative signal, it is first necessary to set the time pauses between packages Δt and between scannings ΔT. The Algorithm consists of the following steps:

- In accordance with the specification of each protocol (any system must notify the fire in no longer than the critical time τ), it is necessary to scan no less than two full scanning cycles of the sensors S with sufficiently small discrete intervals T, i.e. the time of data scanning should be no less than 2τ. In addition, the length of the signal scanned must be 3τ to ensure that at least one set of signals was surrounded by pauses between sets.
- After this time interval, it is necessary to identify all intervals consisting of zeros, and save their duration $\Delta Z = \{\Delta z_1, \Delta z_2, \dots, \Delta z_k\}$.Then all lengths sequences should be sorted in descending order, removing repetitive.
- The Δz_1 obtained after sorting will be the desired pause length ΔT
- Selecting a time interval ΔT, we can identify period S_T between two sequences of zeros of ΔT duration in the source signal S.
- Inter-signal intervals Δt are denoted in the calculated signal S_T in the way similar to the steps 2 and 3.
- After getting Δt value, it is necessary to denote all possible S_i similar to the step 4.

The block diagram of the algorithm can be seen in figure 4A.

Having received all informative signals from each sensor S_i, it is necessary to analyze a set of signals and to identify the start and stop bits $sb_i, stb_i,\ i = \overline{1,m}$. In addition, in accordance with the wire line specification length of each data package sig_i is fixed, as the time for charging each sensor is fixed.

1. It is important to note that in such systems it is possible to implement additional start or stop bits for the entire scanning cycle. To search for the start

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and stop bits of informative signals, informative signals S_1 and S_m should be excluded from consideration.

2. Having received a set of signals $S_i, i = \overline{2, m-1}$ of equal length ΔS, we combine a different set of signals from them $S' = \{|S_2 - S_3|, |S_3 - S_4|, \dots, |S_{m-2} - S_{m-1}|, |S_{m-1} - S_2|\}$
Meanwhile, the duration of each signal is fixed. Operation "-" means bitwise diminution of the signal S_j from the signal S_i.

3. Checking every signal $S_i', i = \overline{1, m-2}$ in the set S', it is necessary to identify the first non-zero bit from the beginning and the signal end. The structure S' in the form of a bit sequence of S' components can be seen in table 1. Thus, the first bits are start bits, and the last n-u-e bit is the stop bit. The S package structure can be seen in table 2.

Table 1: S' Set Structure

Bit No	1	2	…	u	u+1	u+2	u+3	…	u+e-1	u+e	u+e+1	u+e+2	…	n
The first element	0	0	...	0	0	sig'_{11}	sig'_{13}	...	sig'_{1e-1}	0	0	0	...	0
The second element	0	0	...	0	0	sig'_{21}	sig'_{23}	...	sig'_{2e-1}	0	0	0	...	0
	...													
The q-th element	0	0	...	0	1	sig'_{q1}	sig'_{q3}	...	sig'_{qe-1}	0	0	0	...	0
	...													
The g-th element	0	0	...	0	0	sig'_{g1}	sig'_{g3}	...	sig'_{ge-1}	1	0	0	...	0
	...													

4. By calculating the values of u and n-u+e, we can find start bits, stop bits, and the signal S, the structure of which can be seen in table 2.

5. Considering the fact that in step 1 signals S_1 and S_m were excluded, it is necessary before analyzing the signals to conduct a check of these signals in order to reveal difference between start and stop bits.

Table 2: Structure of the Informative Signal S

Bit No	1	2	…	u	u+1	u+2	u+3	…	u+e-1	u+e	u+e+1	u+e+2	…	n
Sensor No 2 signal	sb_1	sb_2	...	sb_u	sig_{11}	sig_{12}	sig_{13}	...	sig_{1e-}	sig_1	stb_1	stb_2	...	stb_l
Sensor No 3 signal	sb_1	sb_2	...	sb_u	sig_{21}	sig_{22}	sig_{23}	...	sig_{2e-}	sig_2	stb_1	stb_2	...	stb_l
	...													
Sensor No q signal	sb_1	sb_2	...	sb_u	sig_{q1}	sig_{q2}	sig_{q3}	...	sig_{qe-}	sig_q	stb_1	stb_2	...	stb_l
	...													
Sensor No g signal	sb_1	sb_2	...	sb_u	sig_{g1}	sig_{g2}	sig_{g3}	...	sig_{ge-}	sig_g	stb_1	stb_2	...	stb_l
	...													

Block-diagram of revealing the start and stop bits is shown in the picture 4b.

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

After getting the very data package sig_i of the informative signal S_i, $i = \overline{1,m}$, it is necessary to reveal within the signal a part responsible for the fire of normal mode. For this purpose the following should be done:

- the set of informative signals S from the sensors in normal mode and the set of informative signals $\bar{S}$ from the sensors in "fire" mode should be obtained;
- data packages $sig_i, \overline{sig_i}$, $i = \overline{1,m}$ are received from each of the informative signals;
- after receiving data package, a set of signals $Z = \{Z_i\} = \{|S_i - \overline{S_i}|\}, i = \overline{1,m}$ is built;
- each element Z_i of the set Z is searched for the elements other then zero. The bit found are the bits responsible for indicating every particular fire sensor mode;
- all the other bit consequences are left unchanged as only the input mode fire-norm changed.

Block-diagram of the algorithm is shown in the picture 4c.

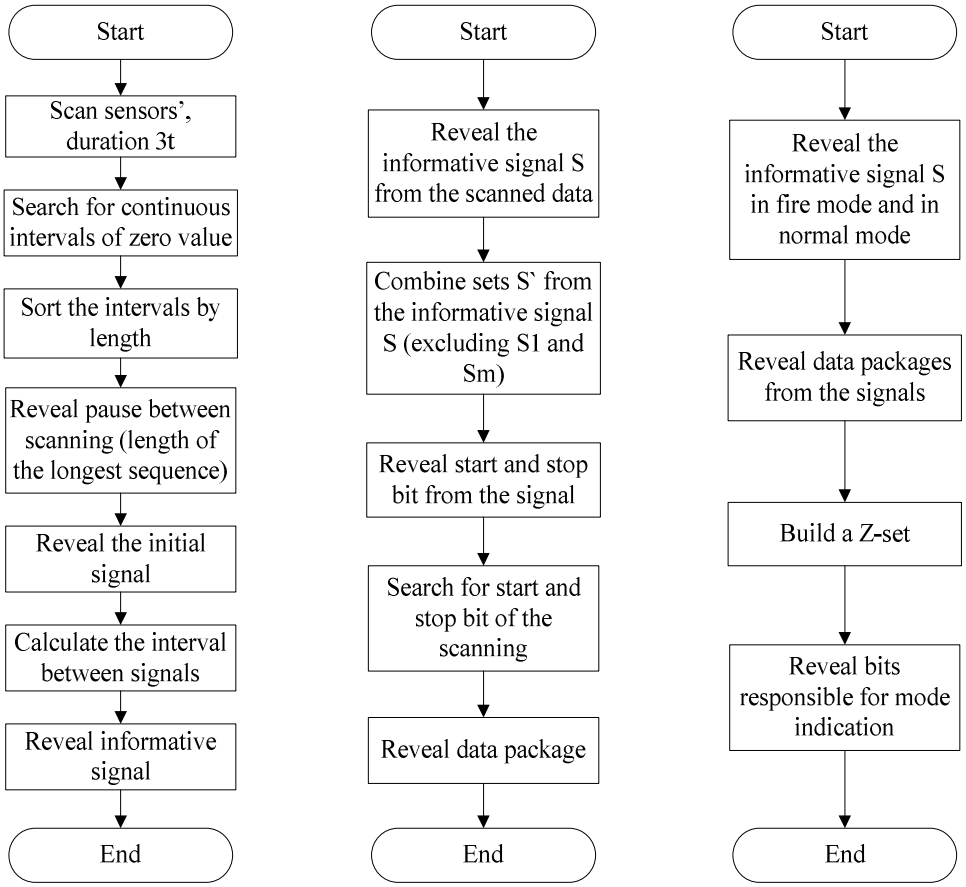


Figure 4a. Block diagram for revealing informative signal

Figure 4b. Block diagram for revealing data package

Figure 4c. Block diagram for revealing mode indicator bits

Figure 4: Package Analysis Algorithms.

Thus, all the data necessary for system protection was obtained.

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. "BOLID C2000M" FIRE ALARM SYSTEM PROTOCOL ANALYSIS

The testing steps are the following:

- system assembly;
- sensors` addresses are programmed in a given range. For example, for 3 sensors we give addresses from 1 to 3;
- the algorithm is tested ensuring the coincidence of obtained address and the specified range;
- the sensors are reprogrammed to a new range;
- the actions are repeated 50 times from the step №3;
- the conclusions about the correct performance of package parsing algorithm are made.

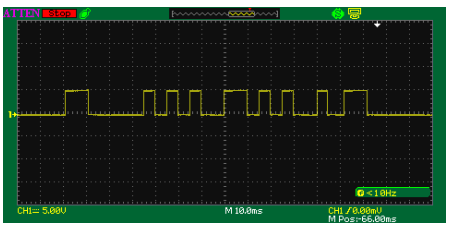
To test the algorithm we used the stand, based on the fire alarm system "Bolid C2000M". The discrete intervals of data scanning by oscilloscope are T=10 μs.

First, the pause between scanning circuits was calculated, then the pause between signals was, and then the length of the informative signal was calculated. The results of the calculations are presented in table 3.

Table 3: Lengths Values of the Signal Key Parts.

ΔT	400 ms
Δt	200 ms
ΔS	160 ms

Based on the lengths, the input signal was divided into informative signals, examples of which can be seen in figure 5. After receiving input signals, on the basis of the previously described algorithm, the start and stop bits and then part of the signal responsible for "fire" - "norm" mode are identified.



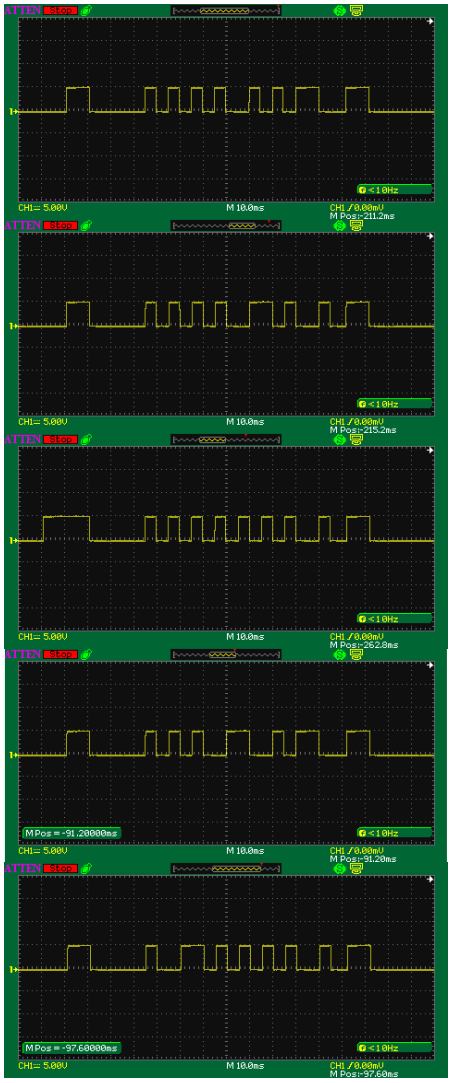


Figure 5: Waveforms of the Signal Line.

The following sequences of start and stop bits, presented in Table 4, were revealed in the "Bolid C2000M" system.

Table 4: Sequences of Start and Stop Bits.

Scanning start bit	11100010
Informative signal start bit	1100010
Stop bit	011

After identifying the start and stop bits the search for sequence responsible for "fire"-"norm" mode indication was conducted (Figure 6).

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

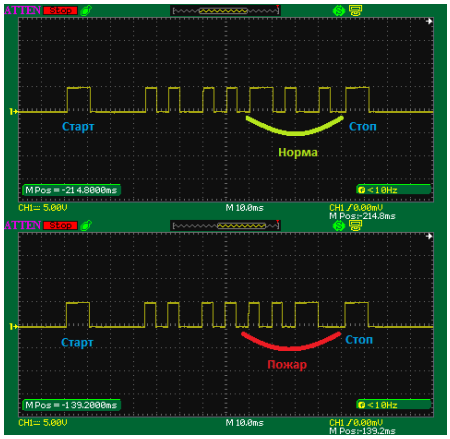


Figure 6: Informative Signal Analysis.

Based on the results of the analysis, commands for each of the sensors can be seen in Table 5.

Table 5: Commands for Sensors.

Package	Mode
1010101010101001	1 norm
1010101010010110	1 fire
1010101001101001	2 norm
1010101001010110	2 fire
1010100110101001	3 norm
1010100110010110	3 fire
1010100101101001	4 norm
1010100101010110	4 fire
1010011010101001	5 norm
1010011010010110	5 fire
1010011001101001	6 norm
1010011001010110	6 fire
1010010110101001	7 norm
1010010110010110	7 fire
1010010101101001	8 norm
1010010101010110	8 fire
1001101010101001	9 norm
1001101010010110	9 fire
1001101001101001	10 norm
1001101001010110	10 fire

The following can be concluded from the experiment:

- The signals in the system "Bolid C2000M" are easy to identify and dismantle;
- On the basis of the received signals, any intruder can simulate any sensor signal, both in "norm" and "fire" modes, modern technical tools allow to control the signal remotely.

4. CONCLUSION

In the modern world many vital and production processes are implemented using information systems and automation systems in particular. The architecture of these systems often does not provide mechanisms to protect against harmful impacts from outside. This is particularly dangerous for APCS and engineering automation systems in particular.

Currently implementation of the data line in popular fire alarm system does not provide protection mechanisms against unauthorized intrusion and signals substitution.

Based on the system "Bolid C2000M" data transfer protocol analysis we can conclude that modern technical means allow development and implementation of protection means for communication links of fire alarm systems from unauthorized intrusions. In addition, the necessity of such means becomes obvious. For this reason, as the next step of work, development of devices to protect data links of the system from unauthorized access and signals substitution by intelligent devices is planned. Such a device must be connected to the data lines of the fire alarm system and analyze traffic for the connection to new sensors with previously unregistered addresses, producing commands from illegitimate addresses. The full functionality of the protection devices will be approved during the development of this means of protection for fire alarm system "Bolid C2000M" in accordance with the selected architecture.

As the paper highlights the vulnerabilities of the "Bolid C2000M" data channel it is planned to develop the protection means for the Bolid communication channel.

REFRENCES:

[1] Marat Telemtaiev. The information system. MCT; Moscow, 2010.
[2] What is an information system. IT CONCORD, 2012. URL: http://itconcord.ru/articles/information-system.
[3] Peroumalnaik M., Énée G. Prediction using pittsburgh learning classifier systems: APCS use case. Proceedings of the 12th Annual Genetic and Evolutionary Computation Conference, GECCO '10 - Companion Publication. 2010, Pages 1901-1907.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[4] Bellettini, C.; Rrushi, J.L. Vulnerability Analysis of SCADA Protocol Binaries through Detection of Memory Access Taintedness. IEEE SMC Information Assurance and Security Workshop, 2007. IAW '07. Pages: 341 – 348.

[5] Morris, T.; Vaughn, R.; Dandass, Y. A Retrofit Network Intrusion Detection System for MODBUS RTU and ASCII Industrial Control Systems. 45th Hawaii International Conference on System Science (HICSS), 2012. Pages: 2338 – 2345.

[6] Stoian, I.; Ignat, S.; Capatina, D.; Ghiran, O. Security and intrusion detection on critical SCADA systems for water management. IEEE International Conference on Automation, Quality and Testing, Robotics, 2014. Pages: 1 – 6.

[7] Stuxnet и Иран: загадка модуля A26. ATOMINFO.RU, ОПУБЛИКОВАНО 28.12.2010. URL: http://www.atominfo.ru/news4/d0249.htm.

[8] Boldizsár Bencsáth. Duqu, Flame, Gauss: Followers of Stuxnet. BME CrySyS Lab. 2012. URL: http://www.rsaconference.com/writable/presentations/file_upload/br-208_bencsath.pdf.

[9] Gleb Gritsai, Alexander Timorin, Yuri Goltsev, Roman Ilyin, Sergey Gordeychik, Anton Carpin. Safety of industrial systems in figures v2.1. Moscow, 2012. Pages: 25 - 28.

[10] Federal law dated 22.07.2008 N 123-FZ (as amended on 23.06.2014) "Technical regulations on fire safety requirements" (changed and added, comes in effect 13.07.2014).

[11] Sergey Levin. Innovative communication protocols used in analogue addressable fire alarm systems. The journal "Technology protection" No 5, 2010.

[12] The order of the FSTEC of Russia "On approval of requirements to ensure the protection of information in automated control systems of production and technological processes on the critical objects, potentially dangerous objects, and objects of high danger for life and health of people and the environment" dated 14 March 2014 N 31.

[13] FIRE AND ALARM CONSOLE S2000M Maintenance guide. URL: http://bolid.ru/files/373/566/s2000m_ver_2.04_eng.pdf (дата обращения: 13.08.2014)

[14] Bolid. Системы безопасности. Пульт контроля и управления охранно-пожарный С2000М. URL: http://bolid.ru/production/orion/network-controllers/s2000m.html (дата обращения: 04.08.2014)

[15] Alex Chernobrovtsev. Information security of industrial enterprises. Protection of APCS is among the problems, which now receive close attention in the world and in Russia. "Computerworld Russia", No 30, 2013.

[16] APC: Vulnerability Statistics. CVE Details. URL: http://www.cvedetails.com/vendor/625/APC.html (date of access: 13.08.14)

[17] Classification of insiders. PC Magazine/Russian Edition. URL: http://www.pcmag.ru/elearning/course/lesson.php?COURSE_ID=7&ID=40 (date of access: 13.08.14)

[18] The model threats and security intruder of personal data processed in a typical personal data information systems industry. The Ministry of communications and mass communications of the Russian Federation. Moscow, 2010. URL: minsvyaz.ru/common/upload/publication/1410065MC.pdf.

[19] Veronica Coshina. The danger of insider. The NATIONAL BANKING JOURNAL, December 2011. Page 2-4. URL: http://www.infowatch.ru/sites/default/files/publications/os_vtb.pdf.

[20] Kupriyanov, MS, Matyushkin D. Digital signal processing. Processors, algorithms, design tools, 1999.