System of Localisation of the Network Activity Source in APCS Data Lines

D. M. Mikhaylov, S. D. Fesenko, Y. Y. Shumilov, A. V. Zuykov,
A. S. Filimontsev and A. M. Tolstaya
National Research Nuclear University "MEPhI" (Moscow Engineering Physics Institute),
Kashirskoe shosse 31, Moscow, Russian Federation

Keywords: Communication Technologies, Wired Data Transmission, Management Information Systems, Information Security of Lines.

Abstract: Automated control system (ACS) is a complex engineering system covering virtually all spheres of industrial production support. The rapid advent of ACS leads to a fast growth of threats aimed at obtaining control over such systems. ACS intrusion may lead to privacy violation, equipment malfunction, loss of time in business processes and even endanger people`s life. This paper proposes a hardware-software complex 'Shield' ensuring comprehensive information security of automated control systems, mainly focusing on its hardware part. The system providing localisation of the network activity source in ACS data lines is described as well as its operational principle and main specifications. As the paper deals with the hardware-software complex, efficiency comparison of 'Shield' software part with the nearest analogues is presented. The hardware design of 'Shield' is now on the final stage, so the testing results of its performance effectiveness are not provided in this paper.

1 INTRODUCTION

Today automated control systems (ACS) are widely present in all fields of technology. An automated control system is a complex of hardware and software for controlling various processes within the technological process and manufacturing of enterprises. ACS is used in various branches of industry, energy, transport, etc. Such systems are generally used to control dispersed assets using centralised data acquisition and supervisory control. Modern automation technologies save time and labour costs and reduce risks and costs of production. These control systems are vital for critical infrastructures operation. (Stouffer 2013, Ibrahimkadic 2011)

The increasing relevance of such systems brings along the problem of an increasing number of malicious agents whose main task is to obtain unauthorised access to information or management control of the infrastructure. The result of such exposure to harmful agents is generally the violation of privacy, equipment troubles and malfunction or time loss in business processes. Many scientific papers, for example (Stouffer 2013, Peng Jie 2011, Cotroneo 2013, Mikhaylov 2013a, Zhukov 2014), were devoted to the problems of ACS vulnerabilities.

ACS vulnerabilities are largely because their software part is often installed on standard personal computers based on Windows and UNIX operating systems, which can be attacked by malicious software. Moreover, open cabling that is used to control automation systems allows connection to management systems by 'tapping' into the data transmission line. At the same time the interest of attackers in such systems is growing because of the possibility of obtaining valuable, often sensitive, data and control of vital systems (video surveillance, access control systems, etc.). This condition gives rise to various kinds of cyber-terrorism and information sabotage from DDoS-attacks (Denial of Service) to complex viruses such as Stuxnet, which can incapacitate the entire infrastructure (Zhukov 2014, Mikhaylov 2013a).

By getting an unauthorised access to the ACS, an attacker can easily derail a train, crash a plane explode a nuclear plant, leave a town without

M. Mikhaylov D., D. Fesenko S., Y. Shumilov Y., V. Zuykov A., S. Filimontsev A. and M. Tolstaya A..
System of Localisation of the Network Activity Source in APCS Data Lines.
DOI: 10.5220/0005332202450251
In *Proceedings of the 17th International Conference on Enterprise Information Systems* (ICEIS-2015), pages 245-251
ISBN: 978-989-758-097-0

electricity etc. (Mikhaylov 2014)

Given the attention paid to counter-terrorism issues by leading countries, careful monitoring of critical facilities (plants, nuclear power plants), as well as public places (shopping malls, airports, etc.) should be maintained in view of possible cybercrimes: cessation of vital critical systems, disabling alarm systems, power outages, etc. It is also important to note that we are talking about life-support systems, and about people's lives. Thus, perhaps for the first time in human history, there is a situation when a computer attack could, in fact, pose a direct threat to human life.

Based on the description above, it can be concluded that today automated control systems need special protection from illegal actions by attackers. There is a need for tools to prevent intrusions into the system. In case the intrusion has already happened there is a need for rapid detection tools to identify the 'weak spots' and respond to the threat. Therefore, this paper describes the system 'Shield' which localise the source of network activity data in ACS lines.

2 RELATED RESEARCH

Recently there was a high activity among developers of ACS protection tools (Melin 2013, Mantere 2012). For example, Stoian et al. propose protection techniques that can reduce the number of attacks on critical SCADA systems for water management (Stoian 2014). Spyridopoulos and his team describe the implementation of viable system model principles and game theory for a novel systemic approach towards cyber security management in Industrial Control Systems, taking into account complex inter-dependencies and providing cost-efficient defence solutions (Spyridopoulos 2014). Oates (2013) describes practical extensions of safety critical engineering processes for securing ICS.

One of the leading software companies in the field of ACS protection is Positive Technologies. Their main products are: MaxPatrol and XSpider.

MaxPatrol is a software product for security and compliance control for SCADA-systems. The program allows performing behavioural security analysis and forecast based on the analysis of the system's vulnerabilities. (MAXPATROL 2014)

XSpider is a similar product designed to audit information systems' security. It also works with the upper level of ACS (SCADA). The main difference is the mechanism of automatic generation of recommendations to strengthen control at the facility and, in particular, to optimise the policy of building information systems. (XSpider 2014)

In fact, Positive Technologies products are designed for network security audit of the facility at the top level of ACS.

Another major player in the market of information system security is JSC 'NTC Stankoinformzaschita'. This company has developed a program called Scanner 'SCADA-auditor' (2014). This product is also only suitable for the analysis of the overall structure of SCADA-systems and obtaining interim conclusions about the need for protective measures.

The above solutions are software solutions and they are not always able to provide comprehensive ACS protection from attacks. Software anti-virus systems cannot solve the problem of the full protection of automated building systems due to lack of the hardware component of the complex. Thus, it can be argued that the existing anti-virus software does not completely protect the system and is not intended for ACS. It is confirmed by the results of tests conducted in the course of theoretical work on the project (see 'Testing and applications'). At the same time, the transfer of the functions implemented to hardware significantly improves the reliability of tools for ensuring security of automation systems.

Therefore, a solution that would implement a comprehensive hardware and software protection of ACS is required. In this regard, we will now consider some of the patented device.

There is a device for detecting electromagnetic radiation by means of a resistive bolometer, and further forming an image using a matrix of such devices. This device comprises a resistive imaging bolometer sensitive to electromagnetic radiation, and is designed to be electrically connected to the signal conditioning circuit (Vilain 2008).

The disadvantage of this device is the low accuracy of the radiation source detection and the point of connection, respectively, as well as the low flexibility of systems on their basis. It does not allow the diagnosis of the range of possible electrical faults in data transmission lines.

The Induction-type linear position detector device has the closest technical nature to the proposed useful model. This device contains a set of inductance sensors sensitive to electromagnetic radiation to be detected, and is designed to be electrically connected to the signal conditioning circuit. (Goto 2000)

The disadvantage of this device is the low accuracy of determining the location of the radiation source and, correspondingly, the point of

connection. Another disadvantage is that it is impossible to use for the control of the structure of data transmitted in transmission lines.

Given these shortcomings of existing solutions, this paper presents a system for determining the location of the signal source with a given accuracy without the suspension of activities of investigated sites of the wired communication networks. This solution will take into account the shortcomings of the above-described devices for the protection of ACS and significantly improve the overall security of the system against the intrusion of third parties.

This paper consciously does not consider the software component of the 'Shield' system, as this issue was the subject of many articles, for example, Mikhaylov (2013a), Mikhaylov (2013b), Starikovskiy (2012) and Beltov (2012).

We will consider development of the 'Shield' hardware component for the protection of ACS system from external and internal attacks.

3 SYSTEM TO LOCALISE THE SOURCE OF NETWORK ACTIVITY

The technical result of the developed system aims to provide a device for determining the location where foreign devices are introduced into the protected automatic process control system (APCS) data networks of the controlled facility or building (ACS comprises APCS). The high-precision determination of the place where malicious data is received into the network is achieved without exposing the existing system of data transmission to changes and thereby without stopping the processes in the protected object even at the time of installation and adjustment of the protection system.

A mechanism to monitor and maintain constant temperature, as well as a hardware cryptographic scheme is introduced into the system of localising the source of network activity in APCS data lines. The APCS also contains a signal distortion sensor, which is coupled to the primary unit of information processing, and an electronic computer. Each of the elements is connected to the primary information processing unit, together with the signal distortion sensor from a combined unit for network activity monitoring. The number of units in the system can be from 1 to n, and each of them is connected to an electronic computer.

The new qualitative result is that the effects of the temperature factor in the system for localisation of the network activity source in the ACS data lines are reduced due to the mechanism of control and maintenance of constant temperature. The mechanism is introduced into the unit of primary information processing to ensure the continued accuracy of inductance, since the signal distortion sensors can affect temperature instability. Also the cryptographic scheme, introduced in the hardware, can increase the security of data transmitted through the creation of a secure data transmission channel aimed to prevent access to this data by unauthorised people.

An example of specific implementation of the proposed device in a general form is shown in Figure 1. The system consists of a unit of network activity monitoring (1) consisting of a signal distortion sensor (2), which is connected to the unit for primary data processing (3), which in turn is connected to a mechanism to monitor and maintain constant temperature (4). There is also the hardware cryptographic scheme (5) and an electronic computer (PC) (6). The number of units of network activity monitoring the system to localise the source of network activity in APCS data lines varies from 1 to n.

The proposed device operates as follows. The system to localise the source of network activity in APCS data lines contains a set of blocks for network activity monitoring. These blocks are installed directly on the data lines, which are connected to a central analysing device. That device is an electronic computing machine of general or specialised performance. The central analysing device is connected to the blocks that are monitoring network activity in communication lines, via a wired connection. Controlled data network of the facility is completely covered by a system of blocks, which are installed on the transmission line without disturbing its work.

The signal from the data line is read by the signal distortion sensor and is passed to the block of primary information processing, which is equipped with a mechanism to monitor and maintain constant temperature. The mechanism is introduced in order to reduce the effect of temperature on the results of measurements of noise distortion. Then, passing through the primary information processing unit, the data is converted into analogue form which is encrypted by means of the hardware cryptographic scheme. Next, the data is transmitted to the computer for comparison with data from other blocks of network activity monitoring.

The operational principle of the system is as follows. The contemplated configurations are

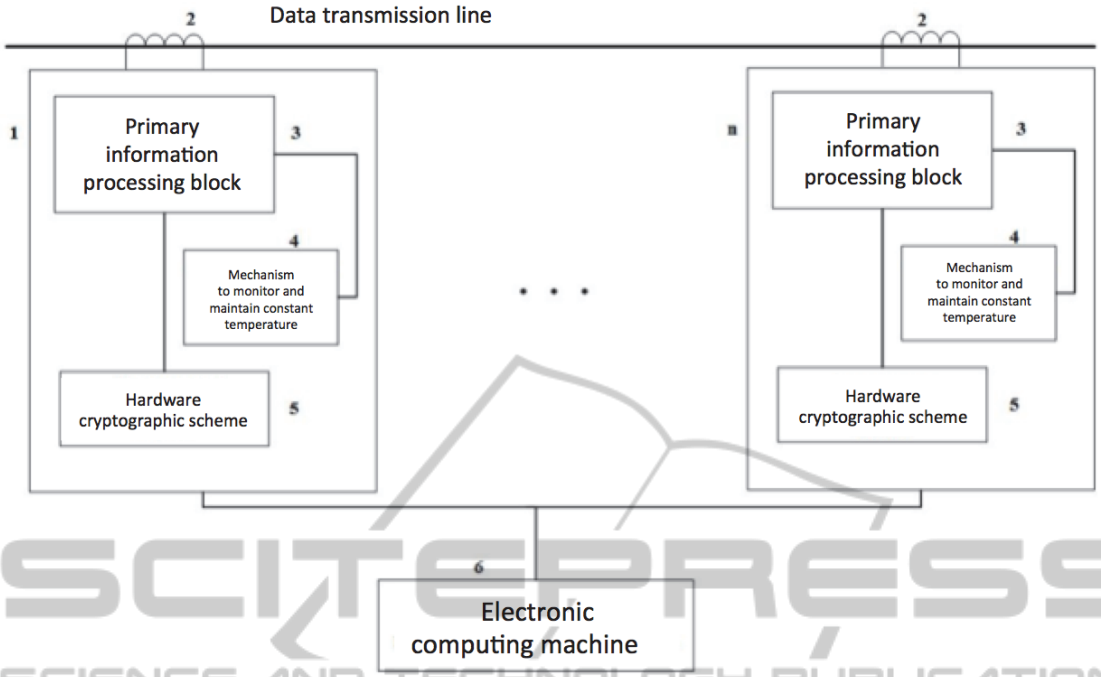

Figure 1: The system to localise the source of network activity 'Shield'.

detectors of electromagnetic radiation, which is spread as a result of change of the electric current flowing along the cable for data transmission. The central analysing device compares data from sensors, located on the respective parts of the protected network in wired channels, and based on that comparison it decides the source of the signals. Thus, the device enables detection of the malicious signal's source.

Specification of the hardware device is shown in Table 1.

The device described in the paper performs the following functions to provide protection against unauthorised access:

- check of the electrical characteristics of the data transmission channel, protection against hidden data leakage;
- protection against destructive packages and malformed data, which can lead to faulty operation of the device;
- overload protection and protection against DDoS-attacks;
- verification of addresses of sending devices and performing devices, protection against undocumented devices, protection against unauthorised commands to devices;
- control of the transmitted data, detection of tampering, unauthorised data addition and blocking data along all its way;

Table 1: Specifications of the system to localise the source of network activity in APCS data lines.

Hardware platform	x86/64
Form factor	19" cross-panel, 3U / 4U, 6 / 8 4HP slots, 6U motherboard
Operating system	OC Linux / Windows
Data exchange with external devices	2 x USB 3.0, VGA / DVI, 2 x 1-Gbit Ethernet
Data exchange with automation systems	Changes due to expansion cards with Ethernet / RS-485 / RS-232 / CAN / analogue inputs
Internal data exchange	CompactPCI
RW memory	4 - 32 Gb DDR3 DRAM
Onboard memory	SATA SSD 2,5" 120 ГБ
Security elements	HSTLM, hardware watchdog timer, tamper switch, hardware peripherals control module, hardware monitoring module Trusted Platform
Power	400 - 750 W, 3.3V, 5V, 12V DC
Operating temperature	-20..+80 C
Cooling system	Built-in air cooling

- protection against prohibited commands, protection against packages that are initially banned (for example, to turn off important

nodes);
- monitoring the integrity of the system, the presence of all the documented system control devices, accuracy of their work and the validity of data sending and receiving.

It is notable that this solution supports rapid adaptation to a variety of industrial protocols and allows the provision of comprehensive protection for the distributed network of automated facilities.

4 TESTING AND APPLICATIONS

The 'Shield' system was tested in a small factory on the territory of the National Research Nuclear University at the Moscow Engineering Physics Institute. The efficiency of the software part of 'Shield' was compared with respective parameters of MaxPatrol and SCADA-auditor. The results of testing the software component are shown in Table 2 (UA stands for unauthorised access; UF stands for undocumented features).

Table 2 shows that the 'Shield' device has a broader scope of program features, as compared with its closest peers. It is notable that the hardware design of 'Shield' is now on the final stage, so the results of its tests are not provided in this paper. However, the authors suggest that the system will show high efficiency and stability in the definition of undue interference in ACS's critical infrastructure.

The localisation system for the network activity source in APCS data lines, described in the paper, can be used in various industries:
- The transport sector: protection of automation and engineering systems of public and freight transport (airports, railway and bus stations, subways, ports, warehouses, storage and sorting facilities, etc.).
- Oil and gas industry: protection of automated transport nodes such as oil and gas pipelines, as well as their associated communication channels, the main gas compressor stations, meter stations of raw materials, etc. Protection of systems accounting final consumption at filling stations.
- Power systems: protection of automation and metering systems for power generation plants – telemetry complexes, automation of technological processes on hydropower, thermal power, nuclear power plants, wind farms, etc., based on the use of industrial data communication protocols.
- Production: protection of automated production systems.

Table 2: Comparison table for ACS software protection.

Parameter	'Shield'	MaxPatrol	SCADA-auditor
Hardware and software implementation	Hardware and software	Software (scaner)	Software (scaner)
Prominent features for protection of industrial controllers and actuators	+	-	-
Prominent features of specialised protocols	+	-	+
UA detection in proprietary protocols	+	-	-
UF detection at the signal level	+	-	-
Integrated safety and security (the ability to integrate with the system of access control; locations monitoring)	+	-	-
Protection against malicious software	+	+	+
Audition of security and integrity of ACS infrastructure	+	+	+
The ability to protect each individual device or group of devices	+	-	-
Detection of underground intrusions	Upon request	-	-
Number of UA/UF detection algorithms	83	N/A	N/A
Backup secure wireless data transmission channel to the server	+	-	-
Security analysis of architecture in accordance with the model of facility threats	+	-	-
Inspection of data exchange protocols	+	-	-
Validation of hardware and software versions in order to detect vulnerabilities in the database	+	+	+

5 CONCLUSIONS

The detection system for signal sources with a given accuracy without the suspension of activities studied areas of wired communication networks, as presented in this paper, will reliably protect the automated control systems from illegal intrusion by third parties. It will improve the reliability of such systems in terms of protection against unauthorised actions by a third party and internal intruder or malicious software and hardware.

The system is in its final stage of development. Soon, the authors are planning to go for testing and further improvement of the existing functionality. All tests of the hardware-software complex 'Shield' are performed in the enterprises of the National Research Nuclear University MEPhI (Moscow Engineering Physics Institute).

In the future the functionality of the system will be expanded: the unit housing the primary information processing of the localisation system is to be covered with a layer of radiation-resistant material as an additional option. This will reduce the influence of the exposure to ionising radiation on the results of monitoring. The layer of radiation-resistant material applied to the surface of the housing unit for primary data processing will ensure that the unit is functional in high background radiation conditions.

Also, the authors plan to develop four solutions from existing design, which will focus on a specific type of facility and protected systems:

- to protect the automation systems of 'smart homes' and some engineering systems (heating, air conditioning, multimedia control, fire alarm);
- to protect major smart facilities with automated control systems and a variety of engineering systems: underground, business centers, stadiums, filling stations, etc.;
- to protect industrial sites with complex automated control systems of technological processes: oil and gas, railways, electric and nuclear facilities, etc. .;
- hardware and software security scanners that can be used to monitor major smart objects and industrial facilities.

The provided in a paper study can be used to improve existing ACS security means, eliminating the vulnerabilities and ensuring more detailed protection from attackers.

Moreover, this study can be taken in account during creation and update of the regulations governing in the field of automated systems` security.

REFERENCES

Stouffer, K., Falco, J., and Scarfone, K., 2013. 'Guide to Industrial Control Systems (ICS) Security'. *NIST Special Publication 800-82*. Revision 1. National Institute of Standards and Technology, May 2013.

Ibrahimkadic, S., Kreso, S., 2011. 'Characteristics of modern industrial control systems'. *Proceedings of the 34th International Convention MIPRO*. Pages: 845-849.

Peng Jie, Liu Li., 2011. 'Industrial Control System Security'. *International Conference on Intelligent Human-Machine Systems and Cybernetics* (IHMSC), Vol. 2, 2011. Pages: 156-158.

Cotroneo, D., Pecchia, A., Russo, S., 2013. 'Towards secure monitoring and control systems: Diversify!' *43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. Pages: 1-2.

Mikhaylov, D., Zhukov, I., Starikovskiy, A., Zuykov, A., Tolstaya, A., Fomin, M., 2013a. 'Method and System for Protection of Automated Control Systems for "Smart Buildings"'. *International Journal of Computer Network and Information Security* Vol. 5, No. 9, July 2013. Pages: 1-8.

Zhukov, I., Mikhailov, D., and Sheremet, I., 2014. *Protection of automated systems against information technology exposure*. Moscow, NRNU MEPhI. 184 pages: illustrated ISBN 978-5-7262-1980-6.

Mikhaylov, D., Zhukov, I., Starikovskiy, A., Zuykov, A., Tolstaya, A., Fesenko, S., Sivkov, S., 2013b. 'Hardware-software complex ensuing information security of automated building management systems'. *International Journal of Application or Innovation in Engineering & Management*, Vol. 2, Issue 3, March 2013. Pages: 408-412.

Mikhaylov, D., Zhukov, I., Sheremet I.Protecting information systems from information and technical influence. Moscow, NRNU MEPhI, 2014. 184 pages.

Melin, A. M., Ferragut, E. M., Laska, J. A., Fugate, D. L., Kisner, R., 2013. 'A mathematical framework for the analysis of cyber-resilient control systems'. *6th International Symposium on Resilient Control Systems (ISRCS)*. Pages: 13-18.

Mantere, M., Sailio, M., Noponen, S., 2012. 'Feature Selection for Machine Learning Based Anomaly Detection in Industrial Control System Networks'. *IEEE International Conference on Green Computing and Communications (GreenCom)*. Pages: 771-774.

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

Spyridopoulos, T., Maraslis, K., Tryfonas, T., Oikonomou, G., Shancang Li., 2014. 'Managing cyber security

risks in industrial control systems with game theory and viable system modelling'. *9th International Conference on System of Systems Engineering (SOSE)*. Pages: 266-271.

Oates, R., Foulkes, D., Herries, G., Banham, D., 2013. 'Practical extensions of safety critical engineering processes for securing industrial control systems'. *8th IET International System Safety Conference incorporating the Cyber Security Conference*. Pages: 1-6.

MAXPATROL, 2014. Compliance and vulnerability management system. Positive Technologies, London. URL: http://www.ptsecurity.com/maxpatrol/kf/ MaxPatrol %20product%20leaflet_eng.pdf.

XSpider, 2014. Positive Technologies, Moscow. URL: http://www.ptsecurity.ru/files/ XSpider_7.8.pdf.

Vulnerability Scanner 'SCADA-auditor' JSC 'NTC Stankoinformzaschita', 2014. Moscow. URL: http://cis-forum.ru/assets/images/Prez/Polyansky_AV_Stankoinformzachita.pdf.

Vilain, M., Dupont, B., 2008. *'Device for detecting electromagnetic radiation, comprising a resistive imaging bolometer, system comprising an array of such devices and a method for reading imaging bolometer of such a system'*. Patent RU No. 2486689, 10 Oct 2008.

Goto, A., Yuasa, Y., Tanaka, S., Akatsu, N., Sakamoto, K., Sakamoto, H., Yamamoto, A., 2000. '*Induction-type linear position detector device'*. Patent US 6034624 A, 7 Mar 2000.

Starikovskiy, A., Zhukov, I., Mikhaylov, D., Sheptunov, A., Savchuk, A., Krimov, A., 2012. 'Improving the security of automation systems for buildings management from cyber attacks'. *Construction equipment and communication,* No. 4, July-August 2012, Moscow. Pages: 2-5.

Beltov, A., Novitsky, A., Konev, V., Fomin, M., Evseev, V., Fesenko, S., 2012. 'Analysis of vulnerabilities of smart home automation technology'. *Construction equipment and communication* No. 4, July-August 2012, Moscow. Pages: 15-19.