Paper

Evaluation of the Cyber Security Provision System for Critical Infrastructure

Jacek Jarmakiewicz, Krzysztof Maślanka, and Krzysztof Parobczak

Faculty of Electronics, Military University of Technology, Warsaw, Poland

Abstract—The paper presents an assessment of the functional mechanisms that are part of the security system for the power grid control. The security system, its components, and the real time processes for the control of electricity supply were defined. In particular, SCADA protocols used in the control system and mechanisms for transferring them between the control center and actuators were identified. The paper also includes presentation of a test environment that is used for developed security mechanisms evaluation. In the last fragment of the paper, the test scenarios were formulated and the results obtained in the cyber security system were shown, which cover security probes reaction delay, forged malicious IEC 60870-5-104 traffic detection, DarkNet and HoneyPot interception of adversary actions, and dynamic firewall rules creation.

Keywords—critical infrastructure, cyber security system, power system security, SCADA system.

1. Introduction

The Critical Infrastructure (CI) includes supply of energy, raw materials and energy consumption, communication, computer networks, financial services, food and water supply, healthcare system, transport, emergency medical services. A CI ensures the continuity of public administration, production, storage, handling and use of chemicals and radioactive substances, including pipelines of hazardous substances. CI also comprises real and cyber systems (and devices or facilities included in these systems) necessary for minimal operation of the economy and the state.

In many countries energy supply is controlled in real-time from the Load Frequency Control (LFC) system [1]. The electricity is generated on the basis of electrical devices requests and is adjusted to their load. The power supply realization is centralized in the so called "secondary control process", which means that the produced power is controlled via the Central Control System (CCS). Any disturbance in this system can have significant impact on all industries and citizens.

Recently, the Supervisory Control And Data Acquisition (SCADA) systems have been used to control power supply processes. In the past, such systems run over dedicated analog lines and networks with vendor specific protocols, hardware and software. The network for power generation control was, and still should be, isolated from the public networks. Control systems such as SCADA, power transmission management system, centralized LFC system and intelligent field devices, e.g. Remote Terminal Unit located in the Control and Supervisory Substation (CSS) and Intelligent Electronic Devices (IED) create new concerns for the cyber security.

Today open transmission protocols are broadly used and computers with commercial operating systems work as IED. It significantly improves automation efficiency and decreases costs, but certainly it also increases system vulnerabilities and decreases the security level. Nowadays SCADA control commands and responses flow across IP networks and over IP protocol stack. Control processes run in real-time and are managed by power station generators.

Cyber security in information technology is used to protect computers and networks from intentional and unintentional events and malicious attacks. Many research and development programs in SCADA security assessment and analysis have been conducted, including risks analysis, vulnerability and security assessment, penetrating testing and evaluation, system simulation and emulation. Many works and articles [2]–[7] related to this subject have been written, but it seems that they don't investigate the essence of the problem. Certainly the importance of this issue and security restrictions don't allow publications related to it. Due to the differences in equipment and technologies used in the industrial control networks, the security solutions are unique and must be adapted to the specific CI, because of the limitations relate to the system generation environment, tools and software libraries used for its development, as well as predispositions of design and generation teams documented with security certificates.

The paper presents a developing process of security system for the critical infrastructure. As a result of the design works, solutions were developed and implemented that are aimed at detection and reaction to cyber incidents such as attacks from outside the system and authenticated, but unauthorized actions from inside the power system. The elaborated solutions and mechanisms were combined into a cyber security and incident response system. At present, the security system mechanisms developed by authors are being assessed in the test environment [8]. A number of tests and tools are prepared that are used for evaluation of the efficiency of presented solutions. The research is carried out in quasi-real conditions, whereby the threats

and attacks are detected in the ICT traffic that comes from the real control system of the national energy sector. The power control network environment was very accurately mapped. The research is conducted with the use of tools elaborated for performance of attacks on SCADA control systems that authors use in order to adjust the sensitivity of probes and solutions. The developed system can operate in both a multi-domain, dispersed environment and in a multi-domain, centralized environment, depending of the stakeholders' requirements. Soon after mechanisms adjustment, the system will be used in a real control and supervision station. The authors believe that the developed cyber security system will be successfully implemented in the national power system.

2. Related Works

Many research centers develop and adapt the security systems for the critical infrastructure in an environment mapping the real control mechanisms. At least several approaches to develop a SCADA system testbed were identified, varying from high-level modeling and simulation frameworks interconnecting simulation environments, to specialized tools recreating client-server interactions on protocol level. These environments are prepared to test the solutions for attacks detection and IT protection of the critical infrastructure systems.
The need of European SCADA Security Testbed creation is subject of [9]. SCADA LAB project [10] was an example of such an initiative, which lasted for 2 years, and constituted coordinated efforts of many European partners. The benefits of the project include:

- definition of security requirements for industrial control systems and a methodology for security testing,
- development of a security laboratory reflecting real environment,
- creation of tools to facilitate efficient testing channels and remote testbed as a service, and for effective sharing of results and experiences,
- smart online and offline dissemination of results for beneficiaries in public and private sectors in the EU.

Research work described in [11] presents a high abstraction level method of modeling CI, as transformation from a detailed "potential" system model to a "specific" model reflecting a particular instance of the system.
Authors of [12] describe the Critical Infrastructure Protection and Resilience simulation (CIPRsim) modeling and simulation framework, which has the capability for simulation and visualization of effects and interdependencies associated with a hazard or threat event. The elements of a simulation model communicate through High Level Architecture (HLA) bus [13], which provides a common architecture for distributed modeling, component-based simulation and linking to real systems. Thousands of modeled objects took part in the simulation process, while threats were modeled analytically in order to stress HLA bus performance capabilities, rather than to assess security features of the evaluated CI system.
Only part of the existing solutions was created with security characteristics assessment in mind, the rest being focused on studying the interdependencies in critical infrastructures, information management performance and/or reliability, etc.

3. Analysis of the Domestic Power Distribution Control System

Efficient and proper work of complex power generation, transmission and distribution system is required for common access to the benefits of electricity. The system is characterized by simultaneous generation and consumption of energy, where practically there is no energy storage. The main task of the energy services is to constantly maintain appropriate settings in the system in order to generate the right amount of power to fulfill the ever-changing consumers needs, with appropriate quality parameters and in the agreed quantities. The process of energy supply is realized by power plants within less than 30 s since the moment the demand occurs. This process is controlled in real-time from the CCS. Generators are activated in the power plants by the LFC mechanism in the process of frequency and power control [1]. In CCS, the controller operates in real-time in a loopback. Currently, the power grid consists of 114 centrally controlled energy sources [14].
In LFC, the command and response process time equals less than 10 s (Table 1) The control is implemented using SCADA protocols IEC 60870-5-104, IEC 61850, which are encapsulated in TCP/IPv4 packets. In the case of failure, the control is taken over by redundant systems and manual control is possible as well.

Table 1
Processing and transmission estimated time of control systems by LFC

Name	Estimated time [s]
Downloading data from RTU CSS on the control area exchange lines	5
Front-end to LFC transmission	0.8
LFC processing	2
Transmission of control LFC to ICCP generator	2
Total	10

Generator turbines are controlled from the CCS by sending data through an independent wide area network based on the SDH technology (Fig. 1). Telecommunication cables are suspended on poles along with high voltage cables.

LFC CCS computer network is based on standard IPv4 and Ethernet with VLANs. The exchange of commands and responses with the generators and energy consumption readouts is performed in CSS. Control commands from the CSS are directed through switches and routers to WAN and are transferred to target routers of the power plants generators [15].

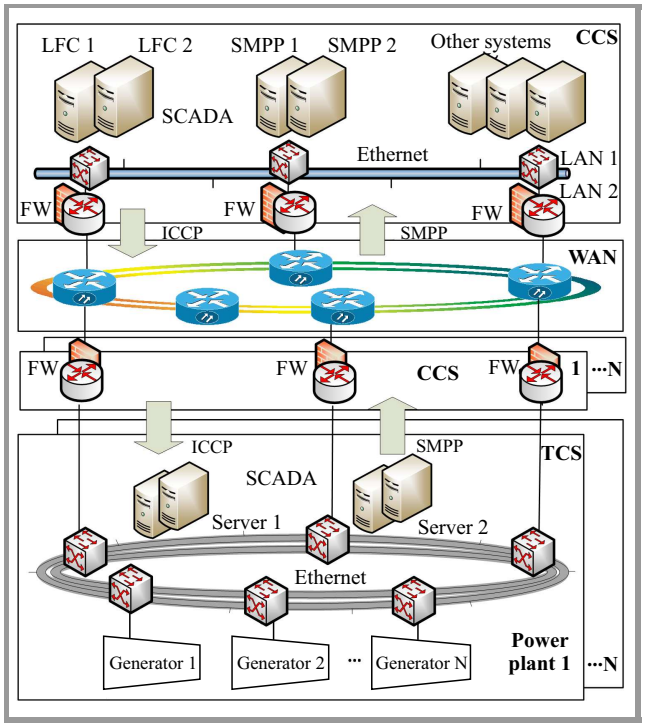


Fig. 1. The power distribution control system architecture.

General example of the station is shown in Fig. 2. Control data are sent to the CSS station, from where they are directed to servers, which send the commands to generators' drivers. The connection equipment and automation systems for the fields are controlled by the CSS as well. The CSS is also used for supervision and monitoring of the stations equipment and systems. At the CSS side of the power plant, the traffic flows by separated VLANs. In the CSS, there are field controllers which are responsible for connection processes of electrical circuits, protection of circuits and cooperation with power plants. Commands from the CCS are delivered to the CSS through routers and modems which are used to perform readouts from IEDs [2]. In addition to remote control from the CCS, it is possible to manually control field automation systems from the CSS, 400 kV protections from Human Machine Interface (HMI) and internal elements of the station from HMI Substation Control. The entire CSS is physically protected using an alarm and supervisory system. Control commands are performed by SCADA systems in the CSS station. SCADA systems are hard real-time systems because the completion of an operation after its deadline is considered useless and potentially can cause cascading effect and severe damage to expensive facilities.

4. Cyber Security System Objectives

The purpose of the developed CI security system is to ensure secure IP communication within the power grid management. The results of the works include a security system prototype providing:

- probing and correlating information with the use of probes and network sensors, aimed at handling,
- automated detection and tracking of threats and appropriate response measures,
- ensuring the security of ICT infrastructure of stations and technological communication through:
  - authentication,
  - advanced access control, e.g. with the use of security policies,
  - monitoring and filtering of management and control IP traffic transferring IEC protocols,
  - encryption of management messages,
  - monitoring of the status of the protected facility and secure storage of information,
  - honeypots and SCADA hardware emulation,
  - secure communication with the central device of Security Information and Event Management (SIEM) and Graphic User Interface (GUI),
  - documentation of management operations and detection of potential unauthorized inside operations.

5. Security System and Testbed Environment Overview

Electricity supply control network is an object of a too high strategic value for direct conducting of tests related to attacks and detection of threats because it could impose a high risk for the power system. Therefore, testing of protective mechanisms of control networks in the power industry requires organization of environment similar to the real one. This is way the environment for testing the cyber security system for the power grid control was developed in the project. Such an environment should reflect power control network elements and imitate processes implemented therein as reliably as possible [3]–[8]. A number of requirements could be formulated in relation to the testbed for cyber security, i.e.:

- similar network resources and protocols should be used that characterize the same vulnerabilities of the real system. The mechanisms should enable reflection of the network structure, elements configuration, routing mechanisms and set of the computer network protocols used;

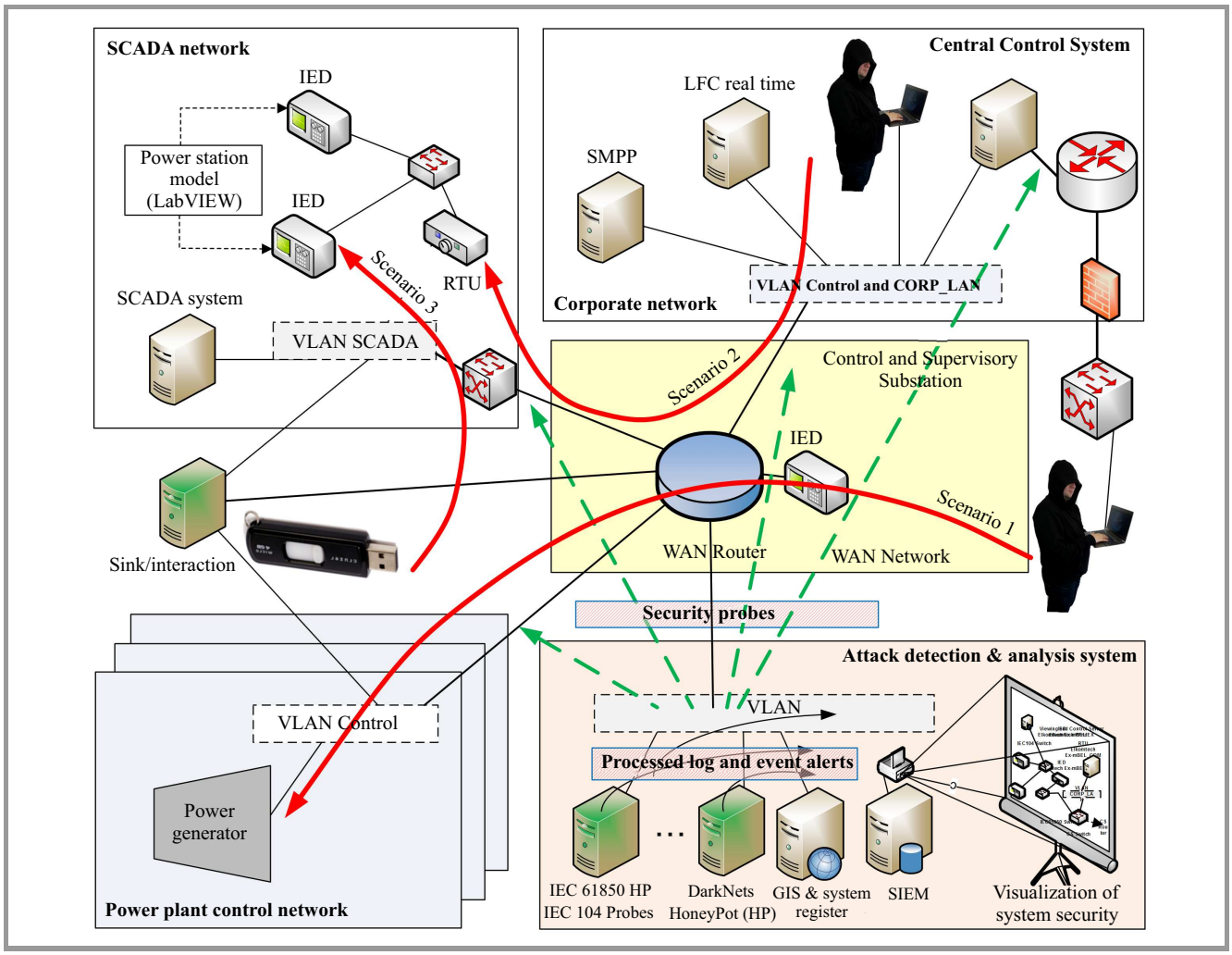


Fig. 2. The CSS station structure and attack scenarios.

- the processes realized in the real system should be reflected as accurately as possible. Controlled SCADA resources should be used as in the real system;
- data traffic exchanged in the testbed should correspond to flows in the real network.

In order to identify, and later reflect the real system properties and solutions for its protection, it is convenient, at the initial stage, to use the ontological model of the critical infrastructure system. It will allow identification of important system resources of the real environment and error prevention consisting in omission of elements influencing the entire system security. Afterwards, the system vulnerability should be determined and, as a result, solutions increasing the system security level should be proposed. Increased security of the control system requires identification of those system properties that will be controlled by the protection system [9].

The authors built a testbed consisting of one control center CCS and several substations CSS, as illustrated in Fig. 2. A communication subsystem is modeled in the form of switch and router is the central node. These elements provide communication within the entire power station, supporting the individual VLANs, and they create virtual network in the entire network using the VRF technology [16]. The individual subsystems of the CCS station operate in the independent VLANs, and they can communicate through a router and CSS firewall. Elements of the CSS system were developed using Cisco devices. The testbed includes real IED subsystem and fields emulators as part of the CSS, communicating using IEC 61850 and 60870-5-104 protocols. The Elkomtech devices were used for its construction: communication hub (RTU) Ex-mBEL_COM [17] and Ex-mBEL field controller [18] (Fig. 3). Extortions for IEDs (single-line-to-ground, symmetrical, short-circuit current) and readouts (measured values) are generated using a custom device and a station model prepared using the LabVIEW environment. Field controllers and the communication hub communicate through an industrial Ethernet switch using IEC-104 protocol. Display and management of the model power system is performed using WindEx software [19] located in the corporate network segment. The control and management processes are performed using IEC 61850 protocol.

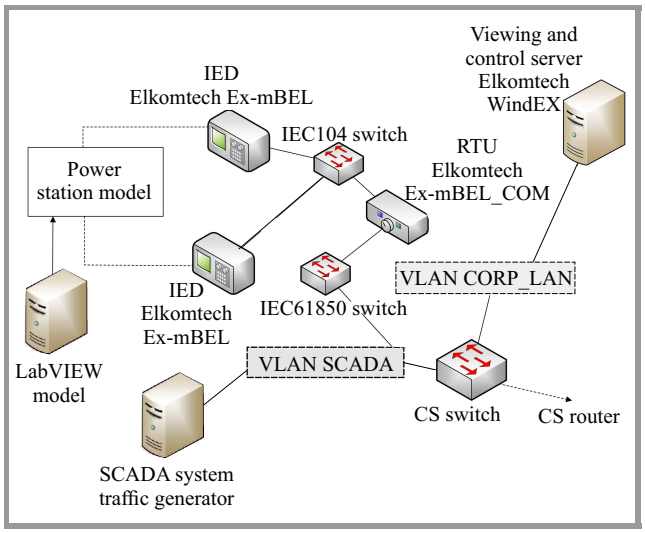


Fig. 3. The power station model and the SCADA system.

SCADA network includes also the SCADA probe (Snort, Bro) which enables monitoring of SCADA traffic. The remaining probes of the security system allow monitoring of i.e.:

- traffic incoming to the power station network, of which copy is fed to one of the probes from CS router,
- both the generation and non-generation traffic from the enterprise network and monitoring and control network – a copy of this traffic is fed on-line from CS switch.

The generated IP network traffic streams are based on traffic samples analysis captured at the boundary of the real industrial power system. The gathered traffic types covered LFC, corporate network, energy trading, measurement and control and network management.
Traffic samples were obtained using FPGA-based hardware probe with nanosecond accuracy and wirespeed record capability. Traffic capture includes corporate network segment traffic and control traffic data (IEC 60870-5-104). Collected samples were regenerated [8] prior to use in testbed generators and targeted to appropriate sinks.
Preliminary analysis of the collected traffic shows the possibility of data packets fields structure and values modification and therefore a chance to slightly overcome protocols inconveniences and limitations (required by industrial equipment manufacturers). These proprietary modifications can be analyzed with customized protocol analyzers, such as Sisco open source Ethernet analyzer based on WireShark for IEC-61850, IEC60870-6 TASE.2 [20].
In such a network (Fig. 2), which reflects the condition of the real power management network (Fig. 1), the functional tests of the developed protection mechanisms were conducted. The researchers intend to verify the efficiency of anomalies and attack detection by tools developed by us, i.e.:

- probes based on Snort and Bro software that are adapted for analysis of SCADA protocols in order to detect anomalies in the power control and management systems,
- commercial IDS/IPS probes that were previously purchased and are currently used in the power control and management network,
- HoneyPots, SCADA HoneyNets and DarkNets for monitoring and logging of all of the threats activities in ICS network,
- mediation device developed to normalize the messages obtained from the other security systems and elements,
- SIEM system gathering, analyzing and aggregating information received from abovementioned elements,
- databases gathering the history of power control and management conditions,
- Cyber security Visualization and Management System processing data developed in SIEM in real-time,
- developed tools and open source tools designed for verification of resilience of the power control and management systems.

6. The Use Cases for Evaluation of the Security System Elements

Functional tests were implemented in a quasi-real environment which is described in Section 5. The experiments were designed to verify the system ability to detect cyber attacks and to protect against them, as well as to adjust the sensitivity of probes and decoys developed in the project.
For the purpose of the experiments, test scenarios were defined, in which the probable directions and sources of attacks were provided. In particular, the scenarios relate to the following directions of attacks were defined:

1. from the Internet and over PSTN with the use of unauthenticated and unauthorized measures by hackers,
2. from the enterprise network, the attacks coming from authorized users of this network who, due to various reasons, attack the power control system,
3. from the control network by persons who know the effects of the attacks and due to personal and/or external reasons conduct attacks on the infrastructure,
4. from the control network by users who are not aware of the threats, authorized to resources, e.g. during a software update, a malware is installed and transferred along with the useful applications.

The attacks may be carried out from outside and inside the control system. They can be performed not only by external attackers, but also by e.g. bribed or intimidated employees, or those unaware of the threat.

(a)

```
[root@pl.bipse.mut.gen1 ~]#nmap -Pn -p 1-100 --min-rate 1000
172.15.102.104
```

Event Time	Phy Element	CSS	Domain	Msg
2015-04-01 13:02:27.797	sonda2-hnp	si2	mut	Many Rejected TCP Packets for IP Addr Pair
2015-04-01 13:02:23.971	ssin1	si2	mut	TCP Packet Rejected

(b)

```
[root@pl.bipse.mut.gen1~]#wget test@172.15.102.100 /  --ask-password
100%[============>] 204         --.-K/s   w  0s
2015-04-01 13:27:42 (10,4 MB/s) - saved `index.html' [204/204]
```

Event Time	Phy Element	CSS	Domain	Msg
2015-04-01 13:27:42.589	sonda2-hnp	si2	mut	TCP Connection Terminated
2015-04-01 13:27:42.589	sonda2-hnp	si2	mut	TCP Connection Terminated
2015-04-01 13:27:42.108	sonda2-hnp	si2	mut	TCP Connection Establish
2015-04-01 13:27:42.108	sonda2-hnp	si2	mut	TCP Connection Establish

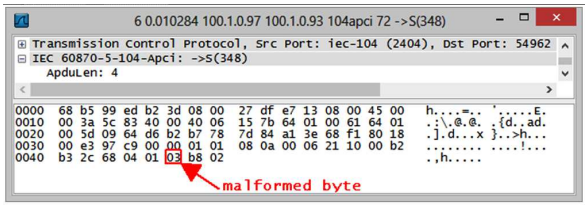
Fig. 4. Functional tests results of DarkNet and HoneyPot.

Let us analyze the scenario of attack from the Internet (no. 1) with the use of PSTN or from the direction of the enterprise network, in which the firewall protecting the control network access was breached (no. 2, Scenario 1 in Fig. 2). In this case, the symptoms of attack are traces left by the control station environment recognition applications. In the scenario with the hacker poorly acquainted with the environment, the attacker has to find out the control station structure, functions performed by the devices, their addresses and protocols used. Two-directional traffic monitoring, from and to the station, will be performed then. Collected features of monitored traffic will be sent toward the attacker. Such actions could be detected on the routers in the form of increased traffic. Scanning of addresses and/or ports may be detected by SCADA decoys – darknets (Fig. 4a) and honeypots (Fig. 4b), emulating operation of station devices.

The authors present the test results that confirm detection of unauthorized operations on the security elements (Fig. 4). The network is scanned directly to the unused DarkNets and HoneyPots addresses, and, as a result of referring to honeypots in GUI of the server with SIEM, the system service is informed on the attempt of unauthorized access to the resources. The next scenario relates to unauthorized operations performed from the control network (no. 3, Scenario 2 in Fig. 2). Unfortunately, this access is possible, e.g. as a result of the CSS personnel carelessness. Suppose that the engineering interface serving for updating the software is not secured and the attacker connected through an external telecom box. It would be also possible to access the CSS control network through a GPRS modem, which, despite prohibitions, was installed by the control devices manufacturer to facilitate the software update process. A dangerous attack would be that performed by an authenticated user authorized to operate within the CSS but, for e.g. religious reasons, wants to cause failure of the unfaithfuls' power supply system. There was once a case of an authorized employee of a large power plant suffering from a heartbreak, who attempted to shutdown the generators. In this scenario an alert information from HoneyPot, HoneyNet or DarkNet systems won't probably be received. The attacker is familiar with the station structure and probably knows that, apart from the regular devices, decoy devices operate there as well. Disconnection of the station devices would immediately result in generation of alerts in the supervision center. Therefore, the attacker wishing to be successful, will seek to incorrectly control the station devices of the power plant generator and possibly forge responses from the controlled device. In this class of attacks in the security system, SCADA probes adjusted to the device and analyzing the status history of the protected systems will be helpful. The SCADA probe is connected in parallel with the protected facility, but it exchanges alerts over a path isolated from the control network to the station security system, so its operation cannot be noticed even by an authorized employee.

Figure 5 presents functional test of SCADA device security. The traffic probe is connected to the IED and it analyzes the traffic and its responses – this is the Probe learning stage. It collects the behavior patterns of the server issuing commands to the IED and feedback sent to the server. After some time, the Probe enters the detection mode. The Probe constantly reports its activity in the facility security system. If it is switched off, the security system will generate an alert. If the Probe detects incorrect data in the control commands, an alert will be generated as well. The second case is presented in Fig. 5. The incorrect control signals are sent to the IED (c), due to which an alert occurs in the security system (d).

(c)



(d)

Event Time	Phy Element	CSS	Domain	Msg
2015-04-01 12:35:16	SCADA Probe	si1	mut	IP_VIOLATION
2015-04-01 12:35:15	SCADA Probe	si1	mut	WRONG_BYTE_2_OF_ACPI_S. Value: 3.

Fig. 5. Functional tests results of SCADA traffic probe.

The use of malware is the last presented scenario (case no. 4, Scenario 3 from Fig. 2), which is in fact not the last possible scenario of attacks. Such software may enter the control station along with the installed hardware or

updated software, or as a result of infection from USB drive or the station personnel laptop containing a virus. The older devices and those used in the station may already contain malware, which is waiting for the right moment to activate. Such cases already happened in the past, an example of which is the Stuxnet worm and its more advanced forms from Flame or Gauss platforms.

(e)
```
[root@pl.bipse.mut.si1.trgen test_mms]# ./kf-mrn-test-mms -s
172.15.102.150
MMS connected.
```

(f)

Event Time	Phy Element	CSS	Domain	Msg
2015-04-01 13:47:52	sonda2-hnp	si1	mut	TCP Connection Terminated
2015-04-01 13:47:51	sonda2-hnp	si1	mut	MMS Association Setup
2015-04-01 13:47:51	sonda2-hnp	si1	mut	TCP Connection Establish

Fig. 6. Functional tests results of DarkNet and HoneyPot.

In this scenario, detection of malware will be possible for each of the developed cyber security measures. If the device recognizes the network environment, it will be noticed on HoneyPot or DarkNet during scanning of addresses or ports in the control network. The alerts will be delivered by channels isolated from the control network to the network protection center. In the case of control sequences sent to SCADA (Fig. 6e) devices by malware, SCADA probe will report anomalies, which will force appropriate action by the station personnel. The result of malware impact will be similar to that obtained in scenario (Fig. 6f). If the malware starts to cooperate with SCADA decoy, an alert will be reported in SCADA DarkNet, similar to that presented in Fig. 6. The changes in the control process will be detected by SCADA probes present in the security system, and the effect will be identical to that provided in the scenario.

7. Summary

The achieved readiness state of the security system allows for its installation in the real power station environment. The paper presents developed the supervision system of the CSS set through the use of domain cooperation mechanisms within one entity and inter-domain cooperation mechanisms of different entities with the use of security policies. Due to the limitations in the volume of the article, they could not be included in the presented content. In addition to the issues covered in this paper, authors have been working on automation of security mechanisms implementation, and they plan to not only passively, but also actively influence certain, selected processes carried out in the control system. In the near future, authors intend to develop the system toward adaption to other critical infrastructure environments, such as the gas industry or smart-grid.
It may be anticipated that the challenges in the smart-grid environment associated with the security level will be even greater.

Acknowledgements

This work is sponsored by the National Centre for Research and Development as a part of a research project for national security and defense of Poland – "System of secure IP communication assurance in power control network", no. ROB 0074 03 001. Project is realized by Military University of Technology, Research and Academic Computer Network, Asseco Poland and Military Communications Institute.

References

[1] "Wymogi wobec JWCD na potrzeby wdrażania systemu LFC (Requirements toward power sources for implementation of the LFC system)", PSE Operator S.A., 2011 (in Polish).

[2] "Vulnerability Analysis of Energy Delivery Control Systems", Idaho National Laboratory, Idaho Falls, Idaho, USA, Sept. 2011.

[3] G. Giannopoulos, R. Filippini, and M. Schimmer, "Risk assessment methodologies for Critical Infrastructure Protection", JRC Technical Notes, European Commission, Joint Research Centre Institute for the Protection and Security of the Citizen, 2012.

[4] "National SCADA test bed", U.S. Department of Energy [Online]. Available: http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed

[5] "About the Cybersecurity for Energy Delivery Systems Program", Office of Electricity Delivery & Energy Reliability [Online]. Available: http://energy.gov/oe/services/technology-development/energy-delivery-systems-cybersecurity

[6] D. Kuipers, "Idaho National Laboratory National SCADA Test Bed", Idaho Falls, IO, USA, Oct. 2010 [Online]. Available: http://www.inl.gov

[7] "Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program", U.S. Department of Energy Office of Electricity Delivery and Energy Reliability, Idaho National Laboratory, Nov. 2008.

[8] J. Jarmakiewicz, K. Maślanka, K. Parobczak, "Development of cyber security testbed for critical infrastructure", in *Int. Conf. Milit. Commun. and Inform. Syst. ICMCIS 2015*, Cracow, Poland, 2015.

[9] *Critical Infrastructure Protection*, E. Goetz and S. Shenoi, Eds., IFIP Advances in Information and Communication Technology, vol. 253. Springer, 2008.

[10] SCADA LAB Project Homepage, https://www.scadalab.eu, Sept. 2012–2014 by INTECO, The Innovative Business Association for Network Security and Information Systems (AEI), Everis Consultancy Ltd, The National Centre for Critical Infrastructure Protection (CNPIC), EFB, Telvent Energía S.A., C Global Services (CGS), Zanasi and Partners (Z&P) and Nisz.

[11] M. Rybnicek, R. Poisel, M. Ruzicka, and S. Tjoa, "A generic approach to critical infrastructures modeling and simulation", in *Proc. Int. Conf. Cyber Secur. CYBERSECURITY 2012*, Washington, DC, USA, 2012, pp. 144–151.

[12] S. Walsh, S. Cherry, and L. Roybal, "Critical Infrastructure Modeling An Approach to Characterizing Interdependencies of Complex Networks", in *Proc. 2nd Int. Conf. Human Syst. Interact. HSI'09*, Catania, Italy, 2009.

[13] 1516-2010 – IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) – Framework and Rules, IEEE Standard Association, Aug. 2010.

[14] "Informacje o pracy KSE (Information on KSE production resources)" (as of 01.12.2014), PSE Operator S.A. (in Polish).

[15] "Standard architektury sieci IP na stacjach elektroenergetycznych PSE S.A (IP Network Standard Architecture for Energetic Station in PSE)", standard tech. specif. PSE PSE-SF.LAN_IP_SE/2014v1, Konstancin-Jeziorna, Poland, 2014 (in Polish).

[16] Configuring Virtual Routing and Forwarding [Online]. Available: http://www.cisco.com

[17] Communication controller Ex-mBEL_COM [Online]. Available: http://www.elkomtech.com.pl/produkty/p/ex-mbel-com-koncentrator-danych/ko/1/3.html (retrieved 12.01.2014).

[18] Communication controller Ex-mBEL [Online]. Available: http://www.elkomtech.com.pl/produkty/g/ex-mbel-1/ko/1/2.html

[19] LabVIEW System Design Software [Online]. Available: http://www.ni.com/labview/ (retrieved 12.01.2014).

[20] Wireshark tool for IEC61850 (8-1, 9-2, 90-5, GOOSE), IEC60870-6 TASE.2(ICCP), UEEE C37.118 and MMS [Online]. Available: http://www.sisconet.com/downloads/Wireshark-win32-1.11.3-SkunkWorksIEC61850.exe

Jacek Jarmakiewicz received his M.Sc. and Ph.D. degrees in Telecommunications and Computer Networks from Military University of Technology (MUT), Warsaw, Poland in 1994 and 2004, respectively. He finished post graduated studies in Telecommunication Management Networks in 2000. He works on MUT as an assistant professor since 2004. At the same time he worked in Military Communication Institute (2009–2014), where he was a member of technical team in Cryptology Dept., and afterwards in C4I Systems Dept. He has held position as a senior researcher, project manager, and head of research groups in national and international, especially NATO RTO IST Panel Support. He was involved in projects in the field of IPv6 tactical networks, resources management in military mobile networks, cryptography, multilevel security, security of power control systems, and Internet of Nano-Things in telemedicine applications. He is author and co-author of 4 books, several chapters in monographs, more than 30 technical papers. He was recipient of Best Paper Award at International Academy, Research, and Industry Association.
E-mail: jjarmakiewicz@wat.edu.pl
Faculty of Electronics
Military University of Technology
Gen. Sylwester Kaliski st 2
00-908 Warsaw, Poland

Krzysztof Maślanka received his M.S. degree in Telecommunication Engineering in 1999 from the Faculty of Electronics, Military University of Technology (MUT), Warsaw, Poland. He is currently working as Assistant Lecturer in Telecommunications Institute, Faculty of Electronics, MUT. He engages in problems of communications and information systems (CIS) modeling and simulation, IP networks problems, telecommunication systems engineering, systems design and implementation for power grid, innovative routing algorithms, and Internet of Nano-Things in telemedicine applications.
E-mail: kmaslanka@wat.edu.pl
Faculty of Electronics
Military University of Technology
Gen. Sylwester Kaliski st 2
00-908 Warsaw, Poland

Krzysztof Parobczak graduated from Military University of Technology in 2009 after achieving M.Sc. degree in area of Electronics Engineering, Teleinformatics speciality. Currently works as Assistant Lecturer at MUT's Institute of Telecommunications, Electronics Faculty. He has participated in ICT security related projects. He is a secretary at AFCEA Polish Chapter, co-author of several publications in field of mobile network security, covert communication channels, power control systems security, and Internet of Nano-Things in telemedicine applications.
E-mail: kparobczak@wat.edu.pl
Faculty of Electronics
Military University of Technology
Gen. Sylwester Kaliski st 2
00-908 Warsaw, Poland