ActaEnergetica
POWER ENGINEERING QUARTERLY

Testing Situation Awareness Network for the Electrical Power Infrastructure

Authors
Rafał Leszczyna
Robert Małkowski
Michał R. Wróbel

Keywords
electric grid, cyber security, situational awareness, testing

Abstract
The contemporary electrical power infrastructure is exposed to new types of threats. The cause of such threats is related to the large number of new vulnerabilities and architectural weaknesses introduced by the extensive use of Information and Communication Technologies (ICT) in such complex critical systems. The power grid interconnection with the Internet exposes the grid to new types of attacks, such as Advanced Persistent Threats (APT) or Distributed-Denial-of-Service (DDoS) attacks. When addressing this situation the usual cyber security technologies are prerequisite, but not sufficient. To counter evolved and highly sophisticated threats such as the APT or DDoS, state-of-the-art technologies including Security Incident and Event Management (SIEM) systems, extended Intrusion Detection/Prevention Systems (IDS/IPS) and Trusted Platform Modules (TPM) are required. Developing and deploying extensive ICT infrastructure that supports wide situational awareness and allows precise command and control is also necessary. In this paper the results of testing the Situational Awareness Network (SAN) designed for the energy sector are presented. The purpose of the tests was to validate the selection of SAN components and check their operational capability in a complex test environment. During the tests' execution appropriate interaction between the components was verified.

DOI: 10.12736/issn.2300-3022.2016308

1. Introduction
Today electrical grids take advantage of Information and Communication Technologies (ICT) and they are often interconnected with the Internet. This exposes them to a completely new type of threats, namely cyber-threats, from which Advanced Persistent Threats (APT) or Distributed-Denial-of-Service (DDoS) attacks, pose a specifically serious challenge in protection of the electrical infrastructure. The most exposed components of the Polish Power System are SCADA systems in substations and Distributed Control Systems (DCS) in power plants.

Advanced Persistent Threats (APT) are dedicated attacks able to persistently target a specific entity and to cause a specific effect, such as an interruption to the power supply [1, 2]. DDoS attacks, on the other hand, attempt to delay, block or corrupt the communication in the grid [3]. Stuxnet [4] was the first wide manifestation of malware that was specifically designed to attack networked industrial control systems in facilities such as gas pipelines or power plants. Detected for the first time in 2010, Stuxnet is a cyber worm able to infect process control servers and Programmable Logic Controllers (PLCs) and alter physical processes in order to sabotage the targeted facility. Later studies revealed that Stuxnet was not the first threat of that type. In fact that it had its precursor called Flame that was undetected until 2012 [5].

To counter the evolved, highly sophisticated threats, advanced cyber security technologies are required, such as Security Information and Event Management (SIEM) systems, application whitelisting, and Trusted Platform Modules (TPM) [1, 6]. Developing and deploying Situation Awareness Networks (SANs) with SIEM software will improve situational awareness and will allow for better control and faster response to threats [7].

Such a Situation Awareness Network is being developed in project DEnSeK (Distributed Energy Security Knowledge) [8]. The project aims at improving the security and resilience of the new energy infrastructure against cyber-threats. It will provide a platform for the security knowledge exchange between companies of the European energy sector. It shall result in establishing a European Energy ISAC (Information Sharing and Analysis Centre) which will enable interactive and real-time knowledge and information sharing between all involved parties [8].

In this paper the results of testing the Situational Awareness Network (SAN) designed for the energy sector are presented. The purpose of the tests was to validate the selection of SAN

components and check their operational capability and interoperability in a complex test environment.

2. Cyber security in the electrical power infrastructure

The contemporary electrical grid due to the intensified use of Information and Communication Technologies (ICT) is exposed to new types of cyber-threats. The most vulnerable components of the Polish Power System are Industrial Control Systems (ICS) which include SCADA systems in substations and Distributed Control Systems in power plants.

Cyber security is defined as the ability to protect or defend the use of cyberspace from cyber attacks [9] and is inextricably linked to information security i.e. the state of information when its confidentiality, integrity and availability are preserved [9, 10].

Whereas [10]:

- Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes
- Availability is the property of being accessible and usable upon demand by an authorized entity
- Integrity is the property of safeguarding the accuracy and completeness of assets.

This definition applies to Information and Communication Technologies in general. Industrial Control Systems (ICS), however, have characteristics that make them very different from traditional information processing systems. There are two fundamental factors which drive most of the others: ICS systems have different priorities and imply risks with a much broader scope and impact. ICS were designed to meet tight performance and reliability requirements which are not typical in a conventional ICT environment. At the same time, many of these ICS serve to control and monitor very critical processes, such as nuclear power generation. This means that the risks include impact on the health and safety of human lives, serious damage to the environment, production losses, impact to a nation's economy, etc.

These differences influence the fact how the systems should be protected and what priorities must be assigned in the protection process. In result the risk management objectives for the two types of systems are not the same (see Fig. 1).

The most important differences between ICT systems and ICS are described below.

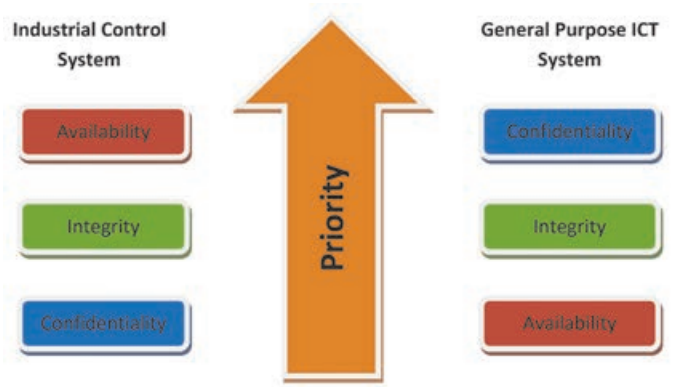


Fig. 1. Comparison of risk management objectives [11]

Performance requirements

ICT systems are normally non-real-time systems, where high data throughput is demanded (and available) and where high delay and jitter may be acceptable in data being communicated as long as data is consistent. On the other hand, ICS may need to operate in real-time and therefore delay/jitter is not acceptable. Throughput is not so important, and as a result the underlying communication infrastructure may be limited in this aspect [11].

Availability requirements

Outages of ICS are not acceptable in most cases and therefore components redundancy is a common practice. Moreover, many control systems are not easily stopped or started without affecting production. This means that common IT system practices such as rebooting are not acceptable [11].

Risk management requirements

In traditional IT systems information confidentiality and integrity are the main concern. For ICS systems human safety, environmental impacts and the process itself (loss of equipment/production) are the main concerns. For this reason, from the three fundamental characteristics of computer security, availability and integrity are the priorities for ICS [11].

Time-Critical machine-human interaction

ICS system response to human interaction is very critical. Requiring password authentication should not hamper or interfere with emergency actions [11].

System operation

Legacy systems are vulnerable to resource unavailability and timing disruptions. Control networks are often more complex and their operation require a different level of expertise (e.g. are typically managed by control engineers). Software and hardware applications are more difficult to upgrade and many systems do not have desirable security features (e.g. encryption, error logging, password protection, etc.) and it may be difficult to include them since they are resource-constrained systems [11].

Change management

Software updates on ICS systems need to be thoroughly tested by the vendor and the end user before being implemented and ICS outages often must be planned and scheduled days/weeks in advance. Moreover, many ICS systems utilise older versions of operating systems that are no longer supported. [11]

There are many challenges related to the protection of Industrial Controls Systems and ICT in the electrical infrastructure. For more details an interested reader may refer to [11–14].

3. Security information and event management systems in situation awareness

Situation awareness

Various definitions of Situation Awareness (SA) [15, 16] exist, from which Tadda and Salerno adapt the one of Endsley [17] to the area of Cyber Situation Awareness:

"Situation awareness is the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future to enable decision superiority" [10].

Endsley provides a reference model for situation awareness, which includes the following levels:

- Level 1: Perception of Elements in Current Situation
- Level 2: Comprehension of Current Situation
- Level 3: Projection of Future Status.

Perception is the lowest level of situational awareness. It provides information about the status and behaviour of relevant elements within the environment and represents it in a conceived form. Without a correct perception of important environmental elements, the probability of forming a distorted view of a situation increases dramatically [16].

Comprehension of a situation is related to combining, interpreting, storing, and retaining information. It extends perception with the integration of multiple pieces of information and the determination of their relevance to established earlier objectives, which can result in inferring or deriving conclusions about the objectives. Comprehension provides a structured outlook of the current situation by determining the significance of objects and events. It links new information to already existing knowledge in order to produce a compound view of the situation as it evolves [16].

Projection is the top level of situation awareness. It is defined as the ability to make predictions based on the outcome of comprehension (and perception) [16].

McGuinness and Foy [18] extended the model by adding a fourth level, called Resolution, which aims at identifying an optimal path to achieve the desired state change to the current situation. Resolution is based on choosing a single course of action from a subset of available actions [18].

Within the DEnSeK [19] project dashboard for the Situational Awareness Network operators was developed. This software visualises the data collected from a distributed set of sensors. At the time of test design dashboard was able to retrieve data from two sources. The first – network analyser Argus – was used to collect data about network traffic activity in protected network. The second is OSSIM – comprehensive and open source security information and event management system. By treating OSSIM as an intermediate layer, the dashboard can be connected with a vast number of sensors, including the most popular IDS systems such as Snort and Suricata.

The Situational Awareness Network proposed in the DEnSeK project may be described as the three-tier architecture, presented in Fig. 2. The lowest tier, data tier consists of sensors such as Network and Host Intrusion Detection Systems, network monitors and analysers. OSSIM software works on the logic tier. It collects and processes data from sensors and transmits them to the top layer. Finally at the presentation tier, the dashboard, after the further processing visualise the data as a user-friendly operator interface.

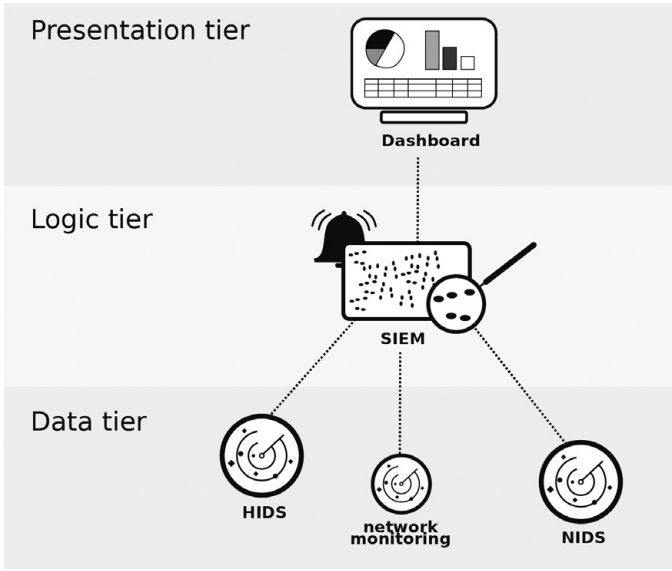


Fig. 2. SAN three-tier architecture

4. Testing environment

The tests were performed in the Cyber security Laboratory located in the ENEL Engineering and Research area of Livorno.

The laboratory aims at replicating the network architecture and the main process control components of a real power generation plant (Combined Cycle Gas Turbine). It was conceived, designed and developed for the testing and development of applications for process automation. From the ICT perspective, the network is layered in the same way as in a production plant, there are all the main components of industrial process control networks, including PLCs and Distributed Control System (DCS) from different vendors. From the industrial process perspective, the controlled process resembles the cold and warm water loops needed by a thermoelectric power plant. This physical process is equipped with field devices (sensors and actuators) such as pressure meters, valves, pumps, inverters, etc. controlled by the PLCs.

A power plant has a quite complex environment, comprising several kinds of systems, subsystems and components namely:

- The Field System, hosting all the PLC, RTU and sensors of the power plant
- The Process Control and Data Acquisition System (Process SCADA), which basically control the field system
- The Control Network, which provide the communication service among the whole Power Plant
- The Data Network, allowing to interconnect different Power Plants
- The Business (Offices) Network with the typical intranet applications
- The Demilitarised Zone where servers for sharing process related data are located.

These systems were reconstructed in the secure isolated (physically disconnected from any other networks) environment of the laboratory based on computer and network equipment, as well as SCADA devices set up over physical hydrologic installation – the Physical Power Plant Emulator (see Fig. 3 and Tab. 1).

The information system of the power plant was reconstructed with very high fidelity. The identical subnetworks were created. All the key workstations of the power plant were copied in one-to-one relation. It means each of the workstations was reflected

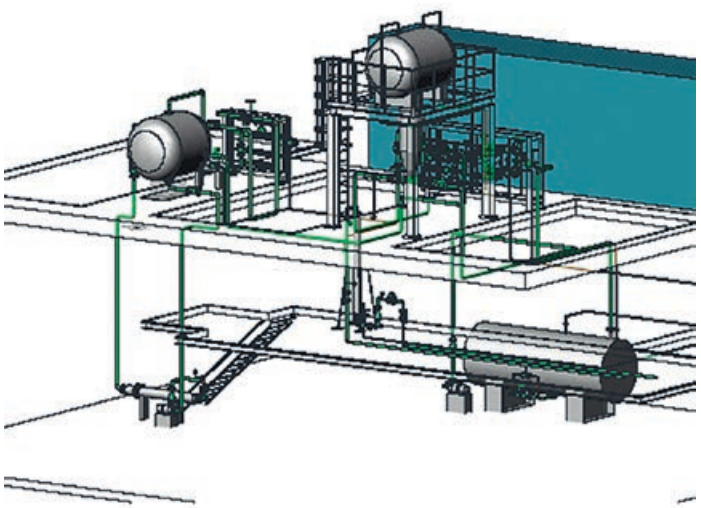


Fig. 3. Physical Power Plant Emulator

into one host of the simulation environment. Only stations of the Intranet were approximated with a lower number of hosts, but this was without loss of generality. In the reconstruction, the same network addresses were used, the same software installed (including the level of patching), the same configurations of firewalls applied etc.

The schema of the network in laboratory is presented in Fig. 4. The laboratory is commonly used to carry out different cyber security tests, especially in the process control network, that help corporate security, ICT security and the different business units of ENEL to make informed decisions or take actions related to cyber security. Security tests include penetration tests, by leveraging the production-like network layers of the laboratory, vulnerability assessments, which can be invasive since the laboratory process does not have any uptime requirement and can afford

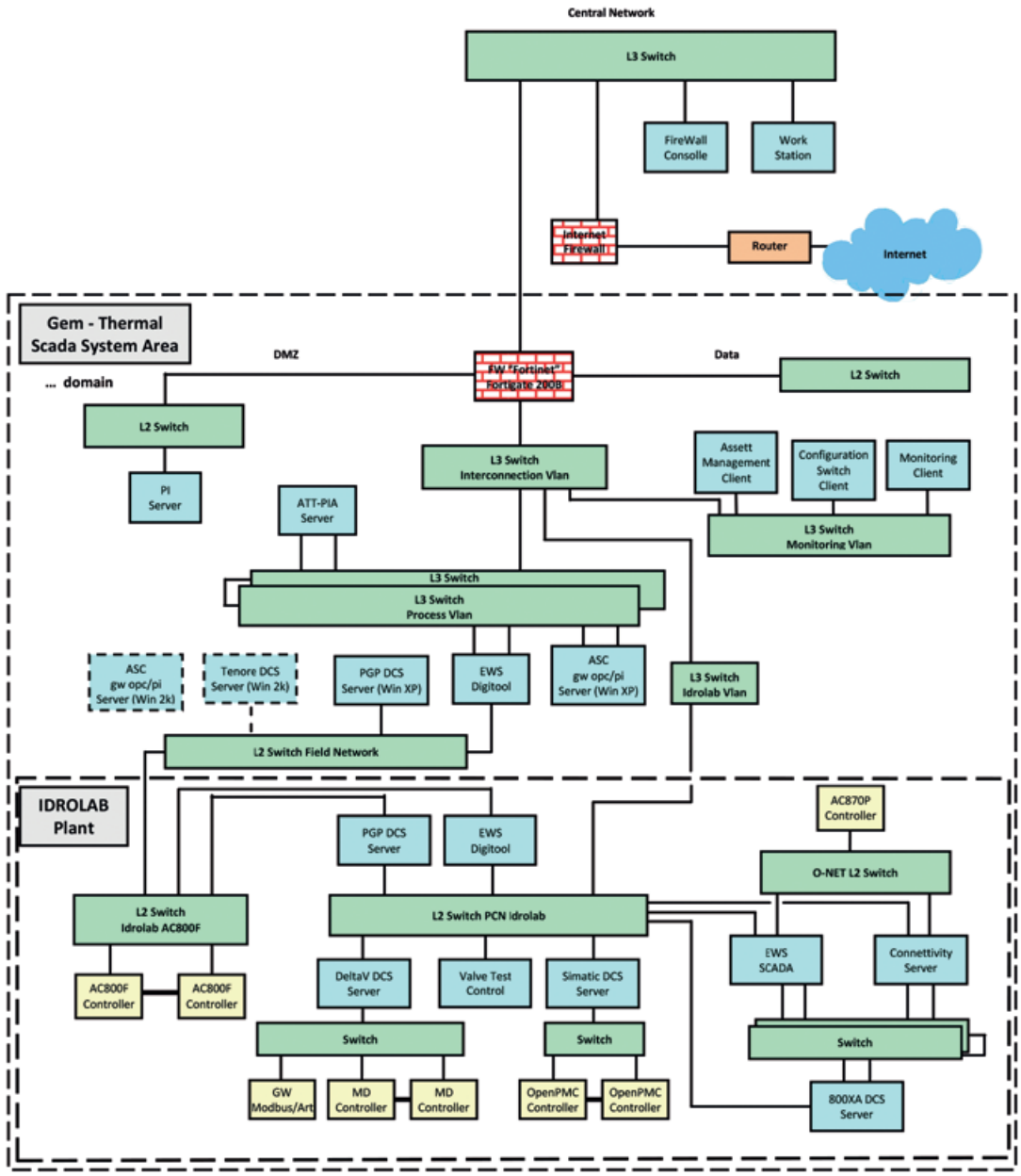


Fig. 4. Cyber Security Laboratory Schema

Siemens	Emerson	ABB	Field Dev.
2 x OpenPMC (PLC) 2 x IM157 (DP Link) 2 x DP/ PA Coupler 2 x ET 200M (active bus) 1 x SM321 (DI) 1 x SM322 (DO) 2 x SM331 (AI) 2 x SM332 (AO)	2 x Ctrl MD (PLC) 1 x KLD-2 (DP/PA) 1 x KLD-2 (DP/PA)	2 x AC 800F (PLC) 3 x RLM 01 (Y Link, repeater) 1 x Converter F.O./ RJ45 Ethernet 1 x Switch Ethernet 2 x CI 840 1 x RLM 01 1 x DP/ PA Power Link 2 x LD 800 HSE 1 x Converter F.O./ RJ45, Ethernet 1 x Switch Ethernet	21 PA, DP, FF, 3 Hart, 12 analog I/O.

Tab. 1. Components of the Physical Power Plant Emulator

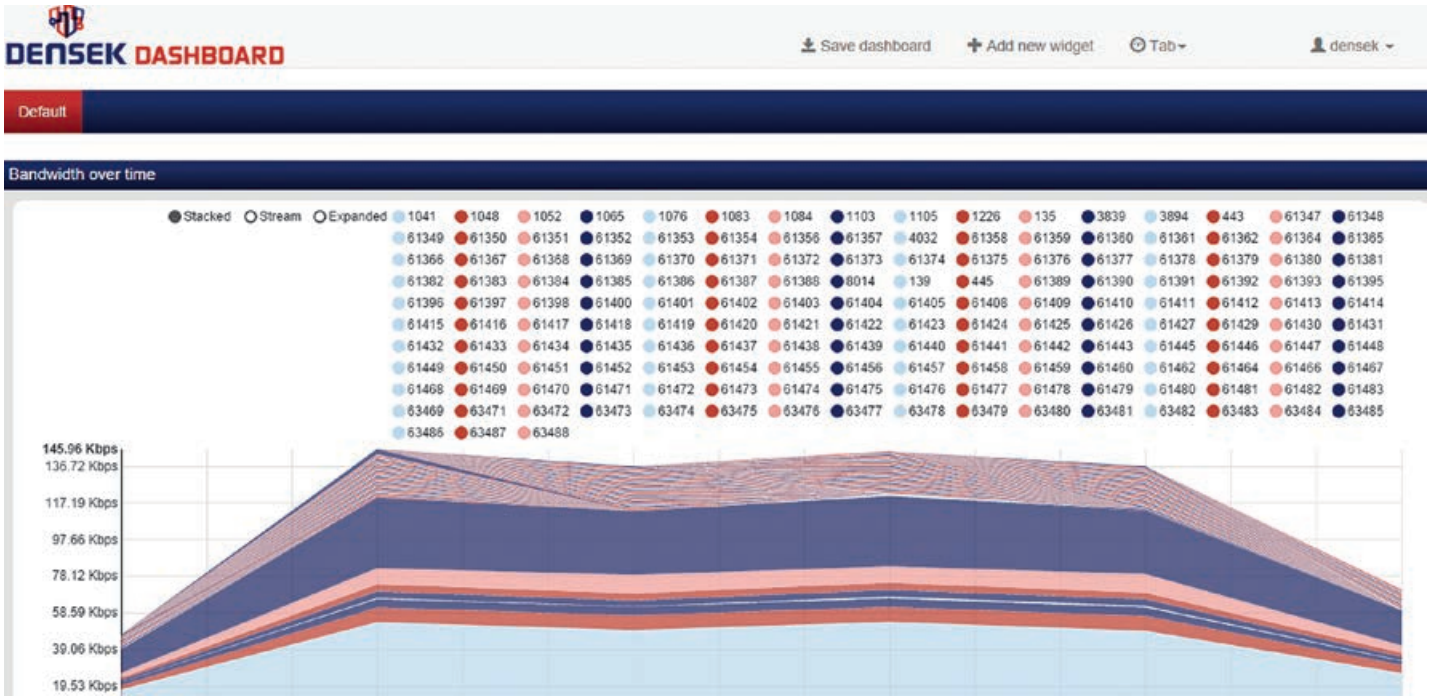


Fig. 5. Illegible presentation of data on the dashboard

to fail, and for the validation of security solutions. The laboratory is also used to test security policies or technical guidelines before they are approved, and for testing security patches before their application into critical production environments, to verify that they do not cause malfunctioning of the SCADA equipment. Finally, also risk assessments benefit from feedback from the laboratory, especially about the impact and effectiveness of security approaches, procedures and technical solutions.
All tests, except Scenario 4 with configuration 2, were performed in the IDROLAB Plant area.

During the test execution 3 computers were used as hosts for the Virtual Machines. Two run under Linux operating system, one under Microsoft Windows.

- Windows 7: Intel Core i7-Q720, 8 cores, 1.6 GHz, 16 GB RAM
- Linux Mint: Intel Core i5-3317U, 4 cores, 1.7 GHz, 8 GB RAM
- Kali Linux: Intel Core i3, 2 cores, 1.2 GHz, 4 GB RAM.

5. Testing process

The aim of the performed tests was to verify whether the architecture and selected components prove their suitability in a complex power plant environment. For this purpose integrity tests were designed. Five test cases were prepared to check the SAN components interoperability. The following components were involved in the tests:

- Argus – network analyser
- Snort – Network Intrusion Detection System (NIDS)
- OSSIM – Security Information and Event Management (SIEM) system
- DEnSek Dashboard – Situational Awareness Network dashboard.

In order to carry out tests additional open source programs were used, including TCPReplay, Oinkmaster and Barnyard2.
In the first part of the testing process appropriate interaction between individual systems components was verified.

Execution of the first two test cases aimed at checking the dashboard operation with the Argus analyser as the data source. During these tests several problems were identified. All of them were related to the processing and visualisation of large amount of data specific to the power plant environment (e.g. Fig. 5). Feedback from testing helped developers to identify and fix bugs.

During the second phase of testing (cases 3 and 4), the integration between Snort IDS and Ossim SIEM was verified. Since both systems are mature Open Source projects their deployment and configuration was smooth. However testing in the large scale environment facilitated identification of problems with communication between subnets. In a production environment sensors will be spread across regions, countries or even continents. It is therefore necessary to develop a method of communication with the central SIEM system.

Finally, the last tests were devoted to the full integration of the SAN. Communication through all the tiers of the SAN (Fig. 2) has been tested. The data collected by the sensors (Snort IDS) were transmitted to the SIEM system (OSSIM). There, based on the analysis and aggregation, alarms were raised and the dashboard was notified. The operator was informed about detected threats through the dashboard widgets. The tests have shown that the SAN architecture was designed correctly. Although there were several problems and bugs system proved its usefulness in the complex test environment.

6. Conlusions

The risk associated with a cyber attack on the Polish energy infrastructure is slowly but steadily growing. This results on the one hand from the increasing dependence of the economy and society from electrical energy, on the other hand, from a gradually implemented ICT in energy sector. Situation Awareness Network supports monitoring of the infrastructure for early detection of threats and reducing their impact. In the DEnSeK project a three-tier SAN platform was designed and implemented. Integration tests conducted in the complex and extensive ENEL Cyber Security Laboratory proved that the architecture and system components were properly selected and the system operates as intended.

REFERENCES

1. Y. Aillerie et al., Smart Grid Cyber Security, 2013.
2. Y. Yan et al., A Survey on Cyber Security for Smart Grid Communications, *IEEE Commun. Surv. Tutorials.* 2012, No. 14, pp. 998–1010.
3. W. Wang, Z Lu., Cyber security in the Smart Grid: Survey and challenges, *Comput. Networks.* 2013, No. 57, pp. 1344–1371.
4. N. Falliere, L.O. Murchu, E. Chien, W32.Stuxnet Dossier, 2011.
5. D. Kushner, The real story of stuxnet, *IEEE Spectrum* 2013, No. 50, pp. 48–53.
6. A. Carcano et al., A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems, *IEEE Trans. Ind. Informatics.* 2011, No. 7, pp. 179–186.
7. H. Khurana et al., Smart-grid security issues, I*EEE Secur. Priv.* 2010, No. 8, pp. 81–85.
8. DEnSeK (Distributed Energy Security Knowledge), project website [on-line], http://www.densek.eu/.
9. R. Kissel, NISTIR 7298 Revision 2 Glossary of Key Information Security Terms, 2013.
10. ISO/IEC: ISO/IEC 27001:2005(E): Information technology – Security techniques – Information security management systems – Requirements, 2005.
11. K. Stouffer, J. Falco, K. Scarfone, NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security, 2011.
12. ENISA: Protecting Industrial Control Systems – Recommendations for Europe and Member States, ENISA, 2011.
13. ENISA: Smart Grid Security: Recommendations for Europe and Member States, 2012.
14. G. Ericsson, Managing Information Security in an Electric Utility.
15. M. Vidulich et al., Situation Awareness: Papers and Annotated Bibliography, 1994.
16. G.P. Tadda, J.S. Salerno, Overview of Cyber Situational Awareness, in: S. Jajodia et al. (eds.), Cyber Situational Awareness, Springer US, Boston, MA 2010, pp. 15–35.
17. M.R. Endsley, Toward a theory of situation awarenss in dynamic systems, *Human Factors* 1995, No. 37, pp. 32–64.
18. B. McGuinness, L. Foy, A Subjective Measure of SA The Crew Awareness Rating Scale – GetInfo. Proceedings of the first human performance, situation awareness, and automation conference., Savannah, Georgia, USA 2000.
19. R. Leszczyna, M.R. Wrobel, Security information sharing for smart grids: Developing the right data model, Proceedings of the 9th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 163–169. IEEE 2014.

Rafał Leszczyna
Gdańsk University of Technology
e-mail: rafal.leszczyna@zie.pg.gda.pl
Dr. Rafal Leszczyna is an assistant professor at Gdańsk University of Technology, Faculty of Management and Economics. He holds the M.Sc. degrees of Computer Science and Business Management. In December, 2006 he earned a Ph.D. in Computer Science, specialisation - Computer Security at the Faculty of Electronics, Telecommunications and Informatics of Gdańsk University of Technology. Between 2004 and 2008 he worked in the European Commission Joint Research Centre, in the teams dealing with information security and the security of critical networked infrastructures. After his return to the university in 2008, from 2010 to 2012 he was seconded to the European Network and Information Security Agency (ENISA), where among the others he was responsible for coordinating the studies related to the security of industrial control systems and smart grids. His professional interests focus on the security of information systems, information security of critical infrastructures, and the issues relevant to information security management.

Robert Małkowski
Gdańsk University of Technology
e-mail: robert.malkowski@pg.gda.pl
He graduated from the Faculty of Electrical Engineering and Automation of Gdańsk University of Technology in 1999. Four years later he got his PhD. He works as an assistant professor in the Chair of Electrical Engineering of Gdańsk University of Technology His scientific interest focus on wind energy issues, critical electrical energy systems failures, as well as on levels of voltage and reactive power distribution in electric power systems.

Michał R. Wróbel
Gdańsk University of Technology
e-mail: wrobel@eti.pg.gda.pl
Dr. Michał Wróbel is an assistant professor at Gdańsk University of Technology, Faculty Of Electronics, Telecommunications And Informatics. He got the MSc degree in 2002 and PhD in 2011 in Computer Science at the Faculty of Electronics, Telecommunications and Informatics of Gdańsk University of Technology. PhD thesis concerned the security of operating systems. His professional interests focus on the security of ICT systems and software development process management.

This is a supporting translation of the original text published in this issue of "Acta Energetica" on pages 81–87. When referring to the article please refer to the original text.

PL

Badanie sieci świadomości sytuacyjnej dla infrastruktury elektroenergetycznej

Autorzy
Rafał Leszczyna
Robert Małkowski
Michał R. Wróbel

Słowa kluczowe
sieć energetyczna, bezpieczeństwo cybernetyczne, świadomość sytuacyjna, testowanie

Streszczenie
Współczesne systemy elektroenergetyczne są narażone na nowe rodzaje zagrożeń. Są one spowodowane lukami w zabezpieczeniach oraz słabościami architektonicznymi związanymi z szerszym zastosowaniem technologii teleinformatycznych (ICT) w tych systemach. Połączenie sieci elektroenergetycznych z Internetem naraża je na nowego rodzaju niebezpieczeństwa, takie jak ataki APT (ang. *Advanced Persistent Threats*) lub rozproszona odmowa usługi (ang. *Distributed Denial-of-Service* – DDoS). W tej sytuacji zastosowanie tradycyjnych technologii bezpieczeństwa informatycznego staje się warunkiem koniecznym, ale niewystarczającym. Aby przeciwdziałać rozwiniętym i wysoce zaawansowanym zagrożeniom, konieczne jest zastosowanie najnowocześniejszych technologii, np. systemów zarządzania informacjami i zdarzeniami bezpieczeństwa (ang. *Security Incident and Event Management* – SIEM), rozbudowanych systemów wykrywania włamań lub zapobiegania włamaniom (ang. *Intrusion Detection/Prevention Systems* – IDS/IPS) oraz układów Trusted Platform Module (TPM). Niezbędne jest także wdrażanie w infrastrukturze teleinformatycznej sieci świadomości sytuacyjnej, która umożliwia precyzyjne monitorowanie i wykrywanie zagrożeń. W artykule przedstawiono projekt oraz wyniki przeprowadzonych testów sieci świadomości sytuacyjnej (ang. *Situational Awareness Network* – SAN) przeznaczonej dla sektora energetycznego. Celem testów było potwierdzenie doboru komponentów SAN i sprawdzenie ich możliwości operacyjnych w złożonym środowisku testowym. W trakcie przeprowadzonych eksperymentów zweryfikowano poprawne działanie sieci SAN.

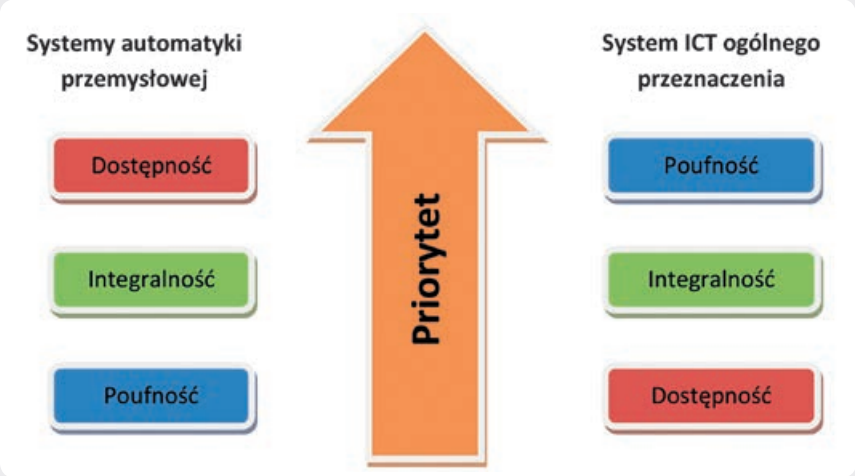
1. Wstęp
Obecnie działające sieci elektryczne coraz częściej wykorzystują technologie teleinformatyczne (ICT), a nawet są podłączane do sieci Internet. To naraża je na zupełnie nowy rodzaj zagrożeń, tzw. cyberzagrożenia, wśród których ataki APT (ang. *Advanced Persistent Threats*) lub rozproszona odmowa usługi (ang. *Distributed-Denial-of-Service* – DDoS) stanowią szczególnie poważne wyzwanie dla ochrony infrastruktury elektroenergetycznej. Najbardziej narażonymi elementami Krajowego Systemu Elektroenergetycznego (KSE) są systemy SCADA w stacjach i rozproszone systemy kontroli (ang. *Distributed Control Systems* – DCS) w elektrowniach.
Do grupy ataków APT należą wrogie, wyspecjalizowane działania, które są uporczywie kierowane na określony podmiot i mają na celu spowodowanie zamierzonych skutków, takich jak na przykład przerwanie zasilania [1, 2]. Z kolei ataki DDoS stanowią próbę opóźnienia, zablokowania lub zaburzenia komunikacji w sieci [3]. Stuxnet [4] był pierwszym powszechnie znanym przykładem złośliwego oprogramowania opracowanego specjalnie do atakowania sieciowych systemów automatyki przemysłowej w obiektach takich jak rurociągi gazowe lub elektrownie. Rozpoznany po raz pierwszy w 2010 r. Stuxnet to tzw. cyberrobak, który może infekować serwery kontroli procesów i programowalne kontrolery logiczne (ang. *Programmable Logic Controller* – PLC) oraz zmieniać procesy fizyczne w celu sabotowania atakowanego obiektu. Późniejsze badania wykazały, że Stuxnet nie był pierwszym zagrożeniem tego typu. W rzeczywistości miał prekursora pod nazwą Flame, który jednak pozostał niewykryty do roku 2012 [5].
Do przeciwdziałania rozwiniętym, wysoce zaawansowanym zagrożeniom konieczne jest zastosowanie nowoczesnych technologii bezpieczeństwa cybernetycznego, takich jak systemy zarządzania informacją i zdarzeniami bezpieczeństwa (ang. *Security Information and Event Management* – SIEM), białe listy aplikacji i układy Trusted Platform Module (TPM) [1, 6]. Opracowywanie i wdrażanie sieci świadomości sytuacyjnej (ang. *Situation Awareness Network* – SAN) z oprogramowaniem SIEM poprawi świadomość sytuacyjną i umożliwi lepsze kontrolowanie i szybsze reagowanie na zagrożenia [7].
Taka sieć świadomości sytuacyjnej jest rozwijana w ramach projektu DEnSeK (ang. *Distributed Energy Security Knowledge*) [8]. Celem projektu jest poprawa bezpieczeństwa i odporności nowej infrastruktury energetycznej na zagrożenia cybernetyczne. Będzie ona platformą wymiany wiedzy o bezpieczeństwie między firmami europejskiego sektora energetycznego. Jej efektem będzie ustanowienie Centrum Udostępniania i Analizy Informacji (ang. *Information Sharing and Analysis Centre* – ISAC) dla europejskiego sektora energetycznego, które umożliwi interaktywne dzielenie się wiedzą i informacjami w czasie rzeczywistym wszystkim zainteresowanym stronom [8].
W artykule przedstawiono wyniki badania sieci SAN przeznaczonej dla sektora energetycznego. Celem badań było potwierdzenie doboru komponentów, sprawdzenie ich możliwości operacyjnych i współpracy w złożonym środowisku testowym.

2. Bezpieczeństwo cybernetyczne infrastruktury elektroenergetycznej
Ze względu na intensywne wykorzystanie technologii teleinformatycznych (ICT) współczesna sieć elektroenergetyczna jest narażona na nowe rodzaje zagrożeń cybernetycznych. Najbardziej narażonymi elementami Krajowego Systemu Elektroenergetycznego są systemy automatyki przemysłowej (ICS), w tym systemy SCADA w stacjach, i rozproszone systemy sterowania w elektrowniach.
Bezpieczeństwo cybernetyczne można zdefiniować jako „zdolność ochrony lub obrony wykorzystania cyberprzestrzeni przed atakami cybernetycznymi" [9] i jest ono nierozerwalnie związane z bezpieczeństwem informacji, tj. stanem informacji, w którym jej poufność, integralność i dostępność są chronione [9, 10].
Przy czym [10]:
- „Poufność to właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana osobom, podmiotom lub procesom nieupoważnionym
- Dostępność to właściwość polegająca na możliwości uzyskania dostępu i wykorzystania na żądanie przez podmiot upoważniony
- Integralność to właściwość polegająca na gwarancji dokładności i kompletności zasobów".

Powyższa definicja ma ogólne zastosowanie do technologii teleinformatycznych. Natomiast systemy automatyki przemysłowej wykazują cechy, które istotnie różnią je od tradycyjnych systemów przetwarzania informacji. Przede wszystkim systemy ICS mają inne priorytety i implikują zagrożenia o znacznie szerszym zakresie i znaczeniu. Systemy automatyki przemysłowej zostały opracowane, aby spełnić wysokie wymagania dotyczące wydajności i niezawodności, które nie są typowe dla konwencjonalnych

This is a supporting translation of the original text published in this issue of "Acta Energetica" on pages 81–87. When referring to the article please refer to the original text.

PL



Rys. 1. Porównanie celów z zakresu zarządzania ryzykiem [11]

środowisk ICT. Jednocześnie wiele systemów tego typu służy do kontroli i monitorowania procesów o krytycznym znaczeniu, takich jak np. produkcja energii jądrowej. Oznacza to, że zagrożenia obejmują wpływ na zdrowie i bezpieczeństwo ludzi, poważne szkody dla środowiska, straty produkcyjne, wpływ na gospodarkę kraju itd.
Powyższe różnice wpływają na wymagania dotyczące ochrony systemów i priorytety dla procesów ochrony. W efekcie cele z zakresu zarządzania ryzykiem dla dwóch typów systemów nie są takie same (zob. rys. 1).
Poniżej opisano najważniejsze różnice między systemami ICT a ICS.

Wymagania dotyczące wydajności

Zazwyczaj systemy ICT ogólnego przeznaczenia nie są systemami czasu rzeczywistego. Często wymagają wysokiej dostępności oraz przepustowości danych, a jednak wysokie czy zmienne opóźnienia przesyłanych danych są dopuszczalne pod warunkiem zachowania ich integralności. Z kolei systemy ICS najczęściej muszą pracować w czasie rzeczywistym, dlatego opóźnienie lub zmienność opóźnienia są niedopuszczalne. Przepustowość nie jest tak istotna, dlatego stosowana infrastruktura komunikacyjna może być ograniczona w tym zakresie. [11]

Wymagania dotyczące dostępności

W większości przypadków przestoje systemów ICS są niedopuszczalne, dlatego redundancja podzespołów jest powszechną praktyką. Co więcej, wielu systemów sterowania nie można łatwo zatrzymać lub uruchomić bez skutków dla produkcji. Oznacza to, że praktyki powszechne w przypadku systemów informatycznych, takie jak ponowny rozruch, są niedopuszczalne. [11]

Wymagania dotyczące zarządzania ryzykiem

W przypadku tradycyjnych systemów informatycznych priorytetami są poufność i integralność informacji. W przypadku systemów ICS priorytetami są bezpieczeństwo ludzi, wpływ na środowisko i sam proces (strata sprzętu/produkcji). Dlatego spośród fundamentalnych cech bezpieczeństwa komputerowego priorytetami dla systemów ICS są dostępność i integralność. [11]

Krytyczne czasowo interakcje maszyna – człowiek

Reakcja systemu ICS na interakcję z człowiekiem jest bardzo ważna. Wymóg uwierzytelniania przy użyciu hasła nie powinien utrudniać ani zakłócać obsługi czynności awaryjnych. [11]

Obsługa systemu

Starsze systemy są narażone na niedostępność zasobów i zaburzenia czasowe. Sieci kontroli często są bardziej złożone, a ich obsługa wymaga innego poziomu wiedzy (np. zwykle zarządzają nimi inżynierowie automatycy). Aplikacje programowe i sprzętowe są trudniejsze w modernizacji, a wiele systemów nie zostało wyposażonych w pożądane zabezpieczenia (np. szyfrowanie, rejestrowanie błędów, zabezpieczenie hasłem itd.), a uwzględnienie ich może być trudne, ponieważ są systemami o ograniczonych zasobach. [11]

Zarządzanie zmianami

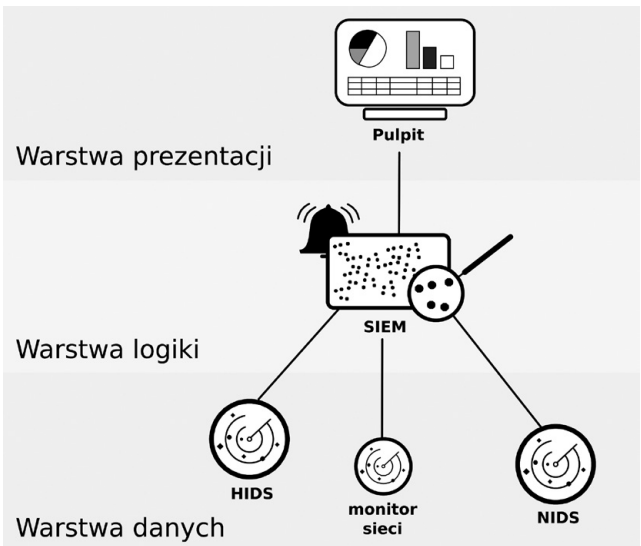
Aktualizacje oprogramowania systemów ICS muszą być dokładnie przetestowane przez dostawcę i użytkownika końcowego przed wdrożeniem, a przestoje systemów ICS często muszą być planowane z wielodniowym lub wielotygodniowym wyprzedzeniem. Co więcej, wiele systemów ICS wykorzystuje starsze wersje systemów operacyjnych, które już nie są wspierane. [11]
Istnieje wiele wyzwań związanych z ochroną systemów automatyki przemysłowej i systemów ITC w infrastrukturze elektrycznej. Zainteresowany czytelnik znajdzie bardziej szczegółowe informacje w [11–14].

3. Systemy zarządzania informacją i zdarzeniami bezpieczeństwa w świadomości sytuacyjnej

Świadomość sytuacyjna

Istnieje wiele definicji świadomości sytuacyjnej (ang. *Situation Awareness* – SA) [15, 16], z których Tadda i Salerno przystosowali definicję Endsleya [17] do zastosowania w dziedzinie cyberbezpieczeństwa:
„Świadomość sytuacyjna to postrzeganie elementów środowiska w zakresie czasowym i przestrzennym, rozumienie ich znaczenia i projekcja ich stanu w bliskiej przyszłości dla potrzeb nadrzędnych decyzji" [10].

Endsley proponuje model odniesienia świadomości sytuacyjnej, który obejmuje następujące poziomy:
- poziom 1: postrzeganie elementów w aktualnej sytuacji
- poziom 2: rozumienie aktualnej sytuacji
- poziom 3: projekcja przyszłego stanu.



Rys. 2. Trójpoziomowa architektura SAN

This is a supporting translation of the original text published in this issue of "Acta Energetica" on pages 81–87. When referring to the article please refer to the original text.

PL

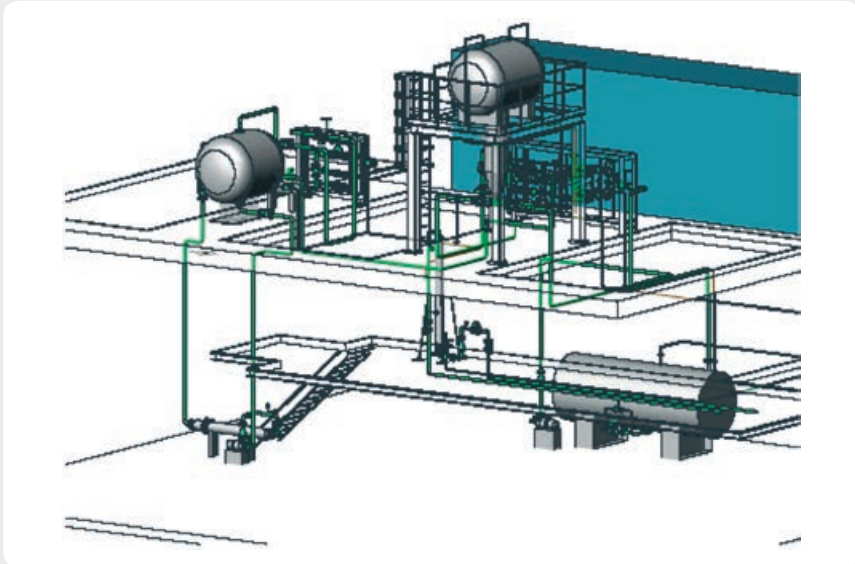
Postrzeganie to najniższy poziom świadomości sytuacyjnej. Dostarcza informacje o stanie i zachowaniu odpowiednich elementów środowiska oraz przedstawia je w przewidzianej formie. Bez prawidłowego postrzegania ważnych elementów środowiska prawdopodobieństwo utworzenia zniekształconego obrazu sytuacji jest znacznie wyższe [16].
Rozumienie sytuacji dotyczy łączenia, interpretacji, zapisu i zachowania informacji. Rozszerza postrzeganie o integrację wielu zestawów informacji i ustalenie ich znaczenia dla obranych wcześniej celów, co umożliwia wyciąganie odpowiednich wniosków. Rozumienie porządkuje spojrzenie na aktualną sytuację poprzez określenie znaczenia obiektów i zdarzeń. Łączy nowe informacje z dotychczasową wiedzą w celu wytworzenia całościowego spojrzenia na ewoluującą sytuację [16].
Projekcja to najwyższy poziom świadomości sytuacyjnej. Jest ona definiowana jako zdolność przewidywania na podstawie rozumienia i postrzegania [16].
McGuinness i Foy [18] rozszerzyli model poprzez dodanie czwartego poziomu, pod nazwą „rozwiązywanie", którego celem jest określenie optymalnej ścieżki do uzyskania pożądanej zmiany stanu dla bieżącej sytuacji. Rozwiązywanie polega na wyborze jednego kierunku działania z podzbioru dostępnych działań [18].
W ramach projektu DEnSeK [19] opracowano panel sterowania (ang. *dashboard*) dla operatorów sieci świadomości sytuacyjnej. To oprogramowanie wizualizuje dane zebrane z rozproszonego zestawu czujników. Podczas przeprowadzonych testów opracowany panel pobierał dane z dwóch źródeł. Pierwsze, analizator sieci Argus, było wykorzystywane do gromadzenia danych o ruchu sieciowym w chronionej sieci. Drugim był OSSIM, kompleksowy system zarządzania informacją i zdarzeniami bezpieczeństwa rozwijany zgodnie z zasadami Open Source. Traktując OSSIM jako warstwę pośrednią, panel mógł być połączony z dużą liczbą czujników, w tym z najpopularniejszymi systemami IDS, takimi jak Snort i Suricata.
W projekcie DEnSeK zaproponowano trójwarstwową architekturę sieci świadomości sytuacyjnej, przedstawioną na rys. 1. Najniższa warstwa, czyli warstwa danych, składa się z czujników, takich jak systemy wykrywania włamań do sieci i hosta, monitory sieci i analizatory. Oprogramowanie OSSIM pracuje w warstwie logiki – gromadzi i przetwarza dane z czujników i przesyła je do warstwy najwyższej. Ostatecznie w warstwie prezentacji przetworzone dane wizualizowane są w formie przystępnego interfejsu operatora.

4. Środowisko testowe

Testy zostały przeprowadzone w Laboratorium Bezpieczeństwa Cybernetycznego (*Security Lab*) należącego do ośrodka rozwojowo-badawczego włoskiej firmy ENEL, w Livorno.
Celem laboratorium jest odtworzenie architektury sieci i głównych elementów kontroli procesu rzeczywistej elektrociepłowni gazowo-parowej. Zostało pomyślane, zaprojektowane i rozwinięte na potrzeby testowania i rozwoju aplikacji z zakresu automatyki procesów. Z punktu widzenia systemu ICT sieć jest podzielona na warstwy w taki sam sposób jak zakład produkcyjny, dlatego występują w niej wszystkie główne elementy sieci przemysłowej kontroli procesów, w tym sterowniki PLC i rozproszone systemy kontroli (ang. *Distributed Control System* – DCS) różnych dostawców.
Z punktu widzenia procesu przemysłowego kontrolowany proces przypomina obiegi wody zimnej i gorącej potrzebne w elektrociepłowni. Ten proces fizyczny jest wyposażony w urządzenia terenowe (czujniki i siłowniki), takie jak ciśnieniomierze, zawory, pompy, falowniki itd. kontrolowane przez sterowniki PLC.
Elektrownia ma dość złożone środowisko, które jest zbudowane z wielu rodzajów systemów, podsystemów i podzespołów, w tym:

- system terenowy, obejmujący wszystkie PLC, RTU i czujniki elektrowni
- system kontroli procesów i pozyskiwania danych (Process SCADA), który zasadniczo kontroluje system terenowy
- sieć kontroli, która obsługuje komunikację w całej elektrowni
- sieć danych, która umożliwia łączenie różnych elektrowni
- sieć biznesowa (biurowa) z typowymi aplikacjami intranetowymi
- strefa zdemilitaryzowana, w której znajdują się serwery do udostępniania danych dotyczących procesów.

Systemy te zostały odtworzone w bezpiecznie odizolowanym (sieci fizycznie oddzielonej od innych sieci) środowisku laboratorium na podstawie urządzeń komputerowych i sieciowych, a także urządzenia SCADA skonfigurowane w fizycznej instalacji hydrologicznej – emulator elektrociepłowni (zob. rys. 2 i tab. 1).
System informatyczny elektrowni został odtworzony z wysoką wiernością. Utworzono identyczne podsieci. Wszystkie kluczowe stacje robocze elektrowni zostały skopiowane w stosunku jeden do jednego. Oznacza to, że każda stacja robocza została odzwierciedlona na jednym komputerze środowiska symulacyjnego. Tylko topologia Intranetu została zredukowana przy użyciu mniejszej liczby stacji, ale odbyło się to bez utraty ogólności. W rekonstrukcji



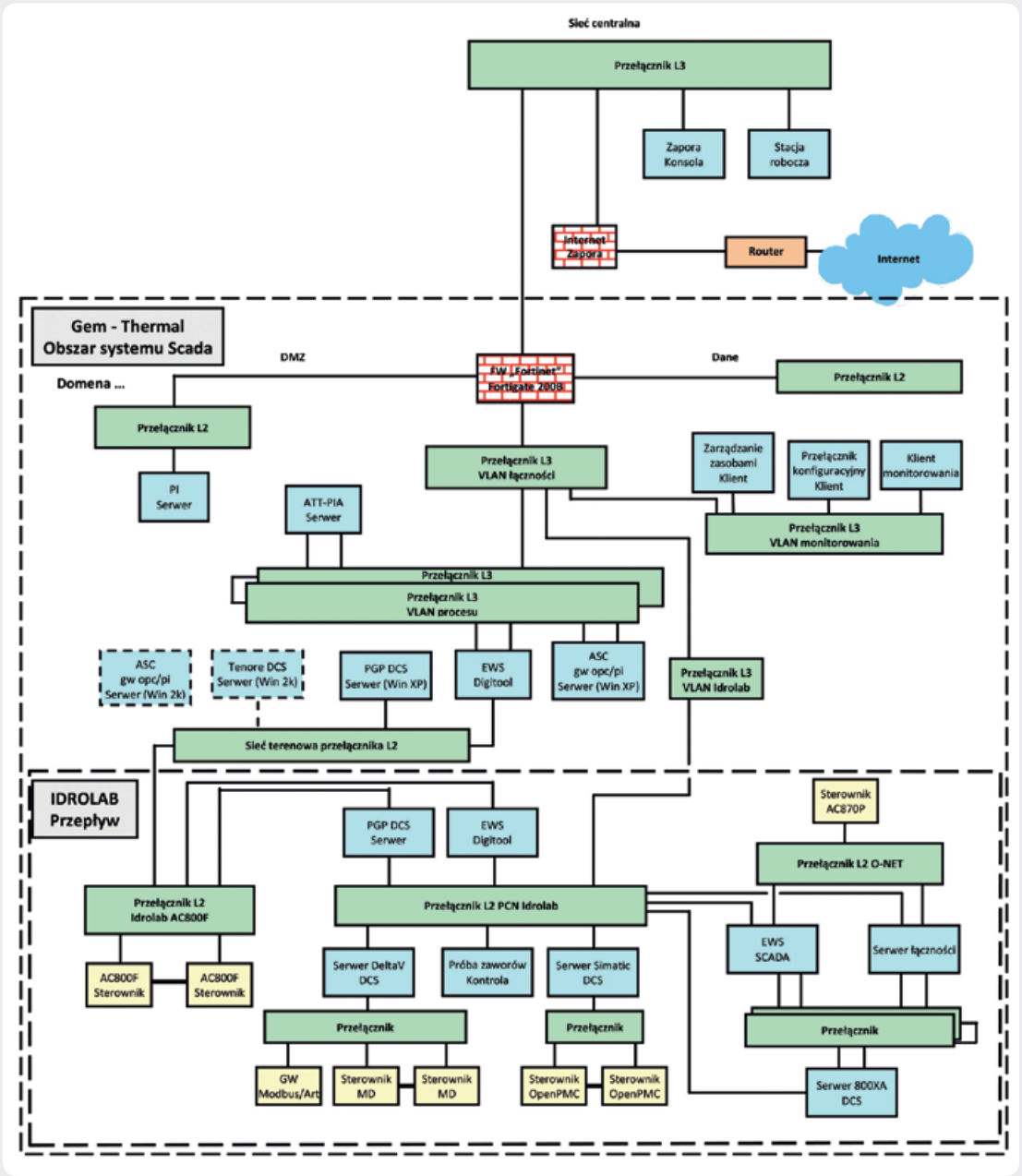
Rys. 3. Emulator elektrociepłowni

Siemens	Emerson	ABB	W terenie
2 x OpenPMC (PLC) 2 x IM157 (łącze DP) 2 x sprzęg DP/PA 2 x ET 200M (szyna aktywna) 1 x SM321 (DI) 1 x SM322 (DO) 2 x SM331 (AI) 2 x SM332 (AO)	2 x Ctrl MD (PLC) 1 x KLD-2 (DP/PA) 1 x KLD-2 (DP/PA)	2 x AC 800F (PLC) 3 x RLM 01 (łącze Y, wtórnik) 1 x konwerter F.O./ RJ45, Ethernet 1 x przełącznik Ethernet 2 x CI 840 1 x RLM 01 1 x łącze mocy DP/PA 2 x LD 800 HSE 1 x konwerter F.O./ RJ45, Ethernet 1 x przełącznik Ethernet	21 PA, DP, FF, 3 Hart, 12 analogowych we/wy

Tab. 1. Podzespoły Emulatora elektrociepłowni

This is a supporting translation of the original text published in this issue of "Acta Energetica" on pages 81–87. When referring to the article please refer to the original text.

PL



Rys. 4. Schemat laboratorium bezpieczeństwa cybernetycznego

wykorzystano takie same adresy sieciowe, zainstalowano takie samo oprogramowanie (z uwzględnieniem poziomu poprawek), zastosowano taką samą konfigurację zapór itd.

Laboratorium jest powszechnie wykorzystywane do wykonywania różnych prób bezpieczeństwa cyberinformatycznego, zwłaszcza w sieci kontroli procesów, które ułatwiają jednostkom bezpieczeństwa korporacyjnego, bezpieczeństwa systemów ICT i innym jednostkom biznesowym ENEL podejmowanie opartych decyzji. Testy bezpieczeństwa obejmują m.in. testy penetracyjne, ocenę luk bezpieczeństwa w działających systemach oraz weryfikację nowych rozwiązań bezpieczeństwa. Ponadto laboratorium jest wykorzystywane do testowania polityk bezpieczeństwa lub wytycznych technicznych przed zatwierdzeniem oraz do testowania poprawek zabezpieczeń przed zastosowaniem w krytycznych środowiskach produkcyjnych w celu zweryfikowania, czy nie spowodują awarii systemów typu SCADA. Również procesy oceny ryzyka wykorzystują informacje z laboratorium, zwłaszcza w kwestii wpływu i skuteczności koncepcji zabezpieczeń, procedur i rozwiązań technicznych.

Wszystkie testy, oprócz scenariusza 4 z konfiguracją 2, zostały przeprowadzone w obszarze zakładu IDROLAB.

Podczas testów zostały wykorzystane trzy komputery jako hosty maszyn wirtualnych. Dwa były wyposażone w system operacyjny Linux, a jeden w system Microsoft Windows.

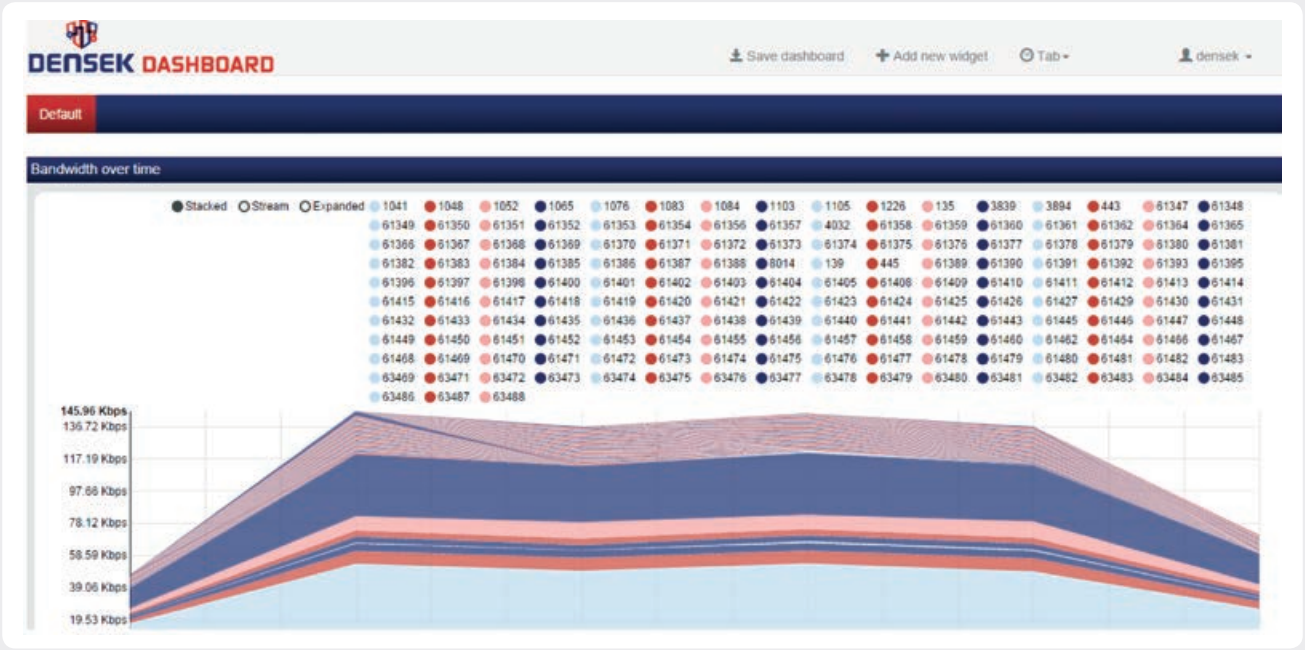
- Windows 7: Intel Core i7-Q720, 8-rdzeniowy, 1,6 GHz, 16 GB RAM
- Linux Mint: Intel Core i5-3317U, 4-rdzeniowy, 1,7 GHz, 8 GB RAM
- Kali Linux: Intel Core i3, 2-rdzeniowy, 1,2 GHz, 4 GB RAM.

5. Proces testowania

Celem wykonywanych testów było zweryfikowanie, czy architektura i wybrane podzespoły wykazują przystosowanie do złożonego środowiska elektrowni. W tym celu opracowano testy integralności. Opracowano pięć przypadków testowych sprawdzających współpracę podzespołów SAN. W testach uwzględniono następujące podzespoły:

This is a supporting translation of the original text published in this issue of "Acta Energetica" on pages 81–87. When referring to the article please refer to the original text.

PL



Rys. 5. Nieczytelna prezentacja danych na panelu

- Argus – analizator sieci
- Snort – system wykrywania włamań do sieci (NIDS)
- OSSIM – system zarządzania informacją i zdarzeniami bezpieczeństwa (SIEM)
- Panel DEnSek – panel sieci świadomości sytuacyjnej.

Do przeprowadzenia testów wykorzystano oprogramowanie typu *open source*, w tym TCPReplay, Oinkmaster i Barnyard2.
W pierwszej części procesu testowania zweryfikowano współpracę między poszczególnymi elementami systemu.
Celem wykonania pierwszych dwóch przypadków testowych było sprawdzenie pracy panelu z analizatorem Argus jako źródłem danych. Podczas tych testów rozpoznano wiele problemów. Wszystkie dotyczyły przetwarzania i wizualizacji dużych ilości danych właściwych dla środowiska elektrowni (np. rys. 4). Wyniki testów pomogły w rozpoznaniu i poprawieniu błędów.
Podczas drugiej fazy testów (przypadki 3 i 4) zweryfikowano integrację IDS Snort i SIEM Ossim. Ponieważ obydwa systemy są dojrzałymi projektami *open source*, ich wdrożenie i skonfigurowanie przebiegło płynnie. Jednak testowanie w środowisku wielkoskalowym pozwoliło rozpoznać problemy z komunikacją między podsieciami. W środowisku produkcyjnym czujniki będą rozproszone po wielu regionach, krajach, a nawet kontynentach. Dlatego ważne jest opracowanie metody komunikacji z centralnym systemem SIEM.
Wreszcie ostatnie testy były poświęcone pełnej integracji SAN. Przetestowano komunikację na wszystkich poziomach SAN (rys. 1). Dane zebrane przez czujniki (Snort) były przesyłane do systemu SIEM (OSSIM). Tam, na podstawie analizy i agregacji, następowało wszczynanie alarmów i powiadamianie panelu. Operator był informowany o wykrywanych zagrożeniach za pośrednictwem widgetów panelu. Testy wykazały, że architektura SAN została zaprojektowana prawidłowo. Choć była pewna ilość problemów i błędów, system wykazał swoją przydatność w złożonym środowisku testowym.

6. Wnioski

Ryzyko związane z atakiem cybernetycznym na polską infrastrukturę energetyczną wzrasta powoli, ale konsekwentnie. Wynika to z jednej strony ze wzrostu uzależnienia gospodarki i społeczeństwa od energii elektrycznej, a z drugiej strony ze stopniowego wdrażania systemów ICT w sektorze energetycznym. Sieć świadomości sytuacyjnej wspomaga monitorowanie infrastruktury oraz wczesne wykrywanie zagrożeń w celu ograniczenia ich wpływu. W ramach projektu DEnSeK opracowano i wdrożono trójpoziomową platformę SAN. Testy integracji przeprowadzone w złożonym i rozległym laboratorium bezpieczeństwa cybernetycznego ENEL wykazały, że architektura i podzespoły systemu zostały właściwie dobrane, a system pracuje według założeń.

Bibliografia

1. Aillerie Y. i in., Smart Grid Cyber Security (2013).
2. Yan Y. i in., A Survey on Cyber Security for Smart Grid Communications. *IEEE Commun. Surv. Tutorials.* 14, 998–1010 (2012).
3. Wang W., Lu Z., Cyber security in the Smart Grid: *Survey and challenges. Comput. Networks.* 57, 1344–1371 (2013).
4. Falliere N., Murchu L.O., Chien, E., W32. Stuxnet Dossier (2011).
5. Kushner D., The real story of stuxnet. *IEEE Spectr.* 50, 48–53 (2013).
6. Carcano A. i in., A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems. *IEEE Trans. Ind. Informatics.* 7, 179–186 (2011).
7. Khurana H. i in., Smart-grid security issues. *IEEE Secur. Priv.* 8, 81–85 (2010).
8. DEnSeK (Distributed Energy Security Knowledge) – project website [online], http://www.densek.eu/.
9. Kissel R., NISTIR 7298 Revision 2 Glossary of Key Information Security Terms (2013).
10. ISO/IEC: ISO/IEC 27001:2005(E): Information technology – Security techniques – Information security management systems – Requirements (2005).
11. Stouffer K., Falco J., Scarfone K., NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security, (2011).
12. ENISA: Protecting Industrial Control Systems – Recommendations for Europe and Member States. ENISA (2011).
13. ENISA: Smart Grid Security: Recommendations for Europe and Member States (2012).
14. Ericsson G., Managing Information Security in an Electric Utility.
15. Vidulich M. i in., Situation Awareness: Papers and Annotated Bibliography (1994).
16. Tadda G.P., Salerno J.S., Overview of Cyber Situational Awareness [w:] Jajodia S., Liu P., Swarup V., Wang C. (red.) Cyber Situational Awareness, s. 15–35. Springer US, Boston, MA (2010).
17. Endsley M.R., Toward a theory of situation awarenss in dynamic systems, *Hum. Factors.* 37, 32–64 (1995).
18. McGuinness B., Foy L., A Subjective Measure of SA The Crew Awareness Rating Scale – GetInfo. Proceedings of the first human performance, situation awareness, and automation conference, Savannah, Georgia, USA (2000).

19. Leszczyna R., Wrobel M., Security Information Sharing for Smart Grids. Developing the Right Data Model. Accepted for the 9th International Conference for Internet Technology and Secured Transactions (ICITST 2014 (2015).

Rafał Leszczyna
dr inż.
Politechnika Gdańska
e-mail: rafal.leszczyna@zie.pg.gda.pl
Rafał Leszczyna jest adiunktem na Wydziale Zarządzania i Ekonomii Politechniki Gdańskiej. W grudniu 2006 r. uzyskał stopień doktora nauk technicznych w zakresie informatyki ze specjalizacją w dziedzinie bezpieczeństwa komputerów. W latach 2004–2008 pracował we Wspólnym Centrum Badań Komisji Europejskiej, w zespołach zajmujących się bezpieczeństwem informacji i bezpieczeństwem krytycznych infrastruktur sieciowych. Po powrocie na Politechnikę Gdańską w 2008 r., w latach 2010–2012 był oddelegowany do Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA), gdzie odpowiadał między innymi za koordynację badań związanych z bezpieczeństwem systemów automatyki przemysłowej i sieci inteligentnych. Jego zainteresowania zawodowe skupiają się na bezpieczeństwie systemów informatycznych, bezpieczeństwie informacji w infrastrukturze krytycznej oraz kwestiach związanych z zarządzaniem bezpieczeństwem informacji.

Robert Małkowski
dr inż.
Politechnika Gdańska
e-mail: robert.malkowski@pg.gda.pl
Ukończył studia na Wydziale Elektrotechniki i Automatyki Politechniki Gdańskiej w 1999 r. Cztery lata później uzyskał stopień naukowy doktora. Pracuje na stanowisku adiunkta w Katedrze Elektrotechniki Politechniki Gdańskiej. Zakres jego zainteresowań naukowych obejmuje zagadnienia zawiązanie z energetyką odnawialną, zasobnikami energii, awariami katastrofalnymi systemu elektroenergetycznego, jak również poziomami napięć i rozpływem mocy biernej w systemie elektroenergetycznym.

Michał R. Wróbel
Politechnika Gdańska
dr inż.
e-mail: michal.wrobel@zie.pg.gda.pl
Michał Wróbel jest adiunktem na Wydziale Elektroniki, Telekomunikacji i Informatyki Politechniki Gdańskiej. Uzyskał tytuł mgr. inż. w 2002 r. i doktora informatyki w 2011 r. na Wydziale Elektroniki, Telekomunikacji i Informatyki Politechniki Gdańskiej. Jego praca doktorska dotyczyła bezpieczeństwa systemów operacyjnych. Jego zainteresowania zawodowe skupiają się na bezpieczeństwie systemów ICT oraz na zarządzaniu procesem rozwoju oprogramowania.