XVII Międzynarodowa Konferencja Naukowa

AKTUALNE PROBLEMY W ELEKTROENERGETYCE APE'15

Jastrzębia Góra, 17–19 czerwca 2015

TESTY PLATFORMY SAN DLA SEKTORA ELEKTROENERGETYCZNEGO

Rafał LESZCZYNA, Michał R. WRÓBEL, Robert MAŁKOWSKI

Politechnika Gdańska, Wydział Elektrotechniki i Automatyki, ul. G. Narutowicza 11/12, 80-233 Gdańsk
tel.: 58 347 1580; e-mail: rafal.leszczyna@pg.gda.pl
tel.: 58 347 2989; e-mail: michal.wrobel@pg.gda.pl
tel.: 58 347 1798; e-mail: robert.malkowski@pg.gda.pl

Streszczenie: Współczesna infrastruktura elektroenergetyczna jest narażona na zagrożenia związane z dużą liczbą nowych luk i słabości architektonicznych wynikających z szerszego wykorzystania technologii informacyjnych i komunikacyjnych (ang. *Information and Communication Technologies* – ICT). Połączenie infrastruktury elektroenergetycznej z Internetem naraża ją na nowe rodzaje ataków, takie jak ataki typu APT (ang. *Advanced Persistent Threats*) czy DDoS (ang. *Distributed-Denial-of-Service*). W tej sytuacji tradycyjne technologie bezpieczeństwa informacyjnego okazują się niewystarczające. W przeciwdziałaniu zaawansowanym zagrożeniom typu APT, czy DDoS, konieczne staje się wykorzystanie najnowocześniejszych technologii, jak systemy SIEM (ang. *Security Incident and Event Management*), rozbudowane systemy IDS/IPS (ang. *Intrusion Detection / Prevention Systems*), czy moduły TPM (ang. *Trusted Platform Module*). Niezbędne jest także opracowanie i wdrożenie rozległej infrastruktury teleinformatycznej wspierającej szeroką świadomość sytuacyjną dotyczącą bezpieczeństwa informacji. W artykule przedstawiono wyniki testów platformy SAN (ang. *Situational Network Awareness*) przeznaczonej dla sektora energetycznego. Celem badań było sprawdzenie poprawności wyboru komponentów SAN, ocena ich wzajemnej współpracy oraz zdolności operacyjnej.

Słowa kluczowe: sieć elektroenergetyczna, bezpieczeństwo cybernetyczne, świadomość sytuacyjna, testowanie.

1. WPROWADZENIE

Zapewnienie skutecznej i efektywnej pracy współczesnej sieci elektroenergetycznej wymaga zastosowania technologii teleinformatycznych wymagających ciągłego połączenia z Internetem. Powoduje to, że współczesne sieci elektroenergetyczne stają się narażone na zupełnie nowe zagrożenia, tzw. cyber-zagrożenia (ang. *cyber-threats*), do których należą mi.n. ataki typu APT (ang. *Advanced Persistent Threats*) czy ataki DDoS (ang. *Distributed-Denial-of-Service*), stanowiące szczególne wyzwanie w zakresie ochrony infrastruktury elektroenergetycznej. Najbardziej narażonymi elementami sektora energetycznego są komputerowe systemy sterowania typu SCADA (ang. Supervisory Control and Data Analysis) w stacjach elektroenergetycznych i systemy typu DCS (ang. *Distributed Control Systems*) w stacjach i elektrowniach [1].

W odróżnieniu od typowych cyberataków, których celem są przypadkowe, bądź tylko ogólnie określone obiekty, ataki typu APT są dedykowanymi atakami ukierunkowanymi na *konkretny obiekt* w celu uzyskania określonego efektu np. przerwy w zasilaniu, wstrzymania procesów regulacyjnych, itp. [2, 3]. Innym rodzajem ataków są ataki typu DDoS. Poprzez wysyłanie dużej ilości zapytań mogą one spowodować np. opóźnienie, blokadę lub uszkodzenie komunikacji w sieci [4].

Wykryty po raz pierwszy w 2010 roku, Stuxnet [5] był pierwszym przykładem szeroko rozpowszechnionego złośliwego oprogramowania, które zostało specjalnie zaprojektowane do ataku na sieciowe systemy sterowania przemysłowego, takie jak gazociągi lub elektrownie. Stuxnet to cyber robak zdolny do zainfekowana serwerów kontroli procesów oraz sterowników (PLC) w celu zmiany przebiegu procesów produkcyjnych, a w konsekwencji do sabotażu docelowego obiektu. Późniejsze badania wykazały, że Stuxnet nie był pierwszym tego typu zagrożeniem. Jego prekursorem był robak o nazwie *Flame*, który pozostał niewykryty aż do 2012 [4].

W celu przeciwstawienia się nowoczesnym, często bardzo wyrafinowanym zagrożeniom, wymagane jest zastosowanie zaawansowanych technologii bezpieczeństwa cybernetycznego. Należą do nich między innymi, systemy SIEM (ang; *Security Information and Event Management*), Białe Listy (ang. *whitelisting*) czy układy TPM (ang. *Trusted Platform Modules*) [2, 5]. Ponadto wdrożenie sieci SAN (ang. *Situation Awareness Networks*) z oprogramowaniem SIEM poprawia tzw. świadomość sytuacyjną i pozwala na lepszą kontrolę oraz szybszą reakcję na zagrożenia [6].

Taka sieć SAN, dedykowana dla sektora energetycznego, rozwijana jest w projekcie DEnSeK (ang. *Distributed Energy Security Knowledge*) [7]. Projekt ten ma na celu poprawę bezpieczeństwa i odporności nowoczesnej infrastruktury energetycznej przed cyber-zagrożeniami. Planowanym efektem projektu jest zbudowanie platformy wymiany wiedzy dotyczącej bezpieczeństwie systemów między przedsiębiorstwami z europejskiego sektora energetycznego oraz utworzenie Europejskiego Centrum Wymiany i Analizy Informacji dla Sektora Energetycznego (ang. *European Energy Information Sharing and Analysis Centre* – ISAC), które pozwoli na interaktywną wymianę informacji pomiędzy wszystkimi zaangażowanymi stronami [7].

W artykule przedstawiono wyniki testów platformy SAN, które miały na celu sprawdzenie poprawności wyboru jej komponentów i zweryfikowanie ich zdolności operacyjnej oraz współdziałania w złożonym środowisku testowym.

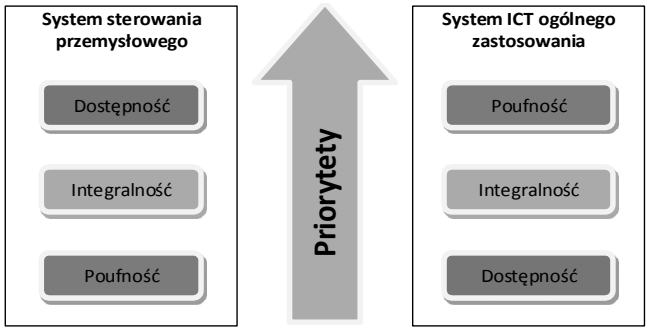
2. CYBERBEZPIECZEŃSTWO W INFRASTRUKRURZE ELEKTROENERGETYCZENJ

Cyberbezpieczeństwo jest definiowane, jako zdolność do ochrony cyberprzestrzeni przed cyberatakami [8] i jest nierozerwalnie związane z bezpieczeństwem informacji tj. takim stanem informacji, w którym zachowana jest jej poufność, integralność i dostępność [8, 9].

Przy czym [9]:

- poufność jest właściwością zapewniającą, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom fizycznym, podmiotom lub procesom;
- dostępność jest właściwością informacji polegającą na możliwości dostępu do niej oraz wykorzystania na każde żądanie uprawnionego podmiotu;
- integralność jest właściwością polegającą na zapewnieniu dokładności i kompletności informacji.

Powyższe definicje odnoszą się do ogólnie pojętych technologii informacyjnych i komunikacyjnych. Natomiast, przemysłowe systemy sterowania (ang. *Industrial Control Systems* – ICS) mają cechy mocno różniące je od tradycyjnych systemów przetwarzania informacji. Można wyróżnić dwa podstawowe czynniki, które odróżniają te systemy. Systemy ICS mają różne priorytety i stwarzają zagrożenia o znacznie szerszym zakresie i skutkach. Przemysłowe systemy sterowania zostały zaprojektowane w celu spełnienia ściśle określonych wymagań odnośnie wydajności i niezawodności, które nie są typowe dla tradycyjnego środowiska teleinformatycznego. Jednocześnie, wiele systemów ICS odpowiedzialne jest za pracę bardzo krytycznych procesów, takich jak np. wytwarzanie energii elektrycznej w energetyce jądrowej. Oznacza to, że istnieje bezpośrednie ryzyko wpływu na zdrowie i bezpieczeństwo ludzi, poważne zagrożenie dla środowiska, straty w produkcji, wpływu na gospodarkę, itd. Różnice te wpływają na sposób, w jaki należy je chronić i jakie priorytety muszą być przypisane w procesie ochrony. W rezultacie cele zarządzania ryzykiem w odniesieniu do tych dwóch rodzajów systemów nie są takie same (patrz rys. 1).



Rys. 1. Porównanie celów zarządzania ryzykiem [10]

Istnieje wiele wyzwań związanych z ochroną przemysłowych systemów sterowania oraz systemów ICT stosowanych w infrastrukturze energetycznej. Więcej szczegółów zainteresowany czytelnik może znaleźć w [11–14].

3. ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI I ZDARZEŃ

Istnieje wiele definicji *świadomości sytuacyjnej* (ang. *Situation Awareness – SA*) [11, 12] spośród których Tadda I Salerno adaptują definicję Endsley'a [13] do dziedziny świadomości sytuacyjnej w cyberprzestrzeni:

Świadomość sytuacyjna jest sposobem postrzegania elementów środowiska w określonym czasie i przestrzeni, rozumieniem ich znaczenia, oraz rzutowaniem (ang. projection) ich stanu na najbliższą przyszłość w celu umożliwienia podejmowania nadrzędnych decyzji. [10]

Endsley dostarcza model odniesienia w świadomości sytuacji, która obejmuje następujące poziomy:

- Poziom 1: Postrzeganie (ang. *perception*) elementów w aktualnej sytuacji;
- Poziom 2: Zrozumienie (ang. *comprehension*) sytuacji bieżącej;
- Poziom 3: Antycypacja (ang. *projection*) przyszłego stanu.

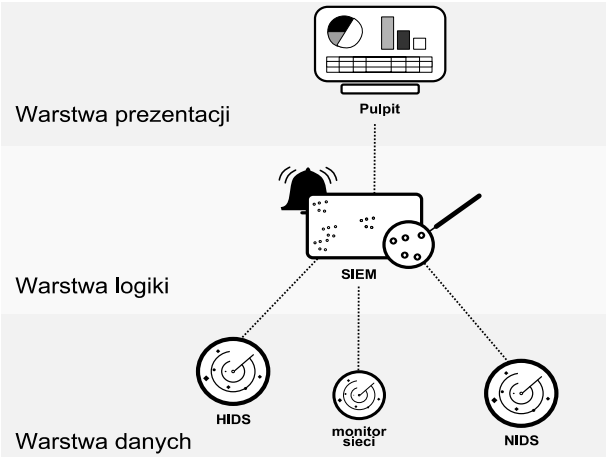
Percepcja jest najniższym poziomem świadomości sytuacyjnej. Dostarcza informacji na temat stanu i zachowania właściwych elementów w środowisku i reprezentuje ją w zrozumiałej formie. Bez prawidłowej percepcji ważnych elementów środowiska prawdopodobieństwo tworzenia zniekształconego obrazu sytuacji, znacznie się zwiększa [12].

Zrozumienie sytuacji związane jest z łączeniem, interpretacją, przechowywaniem oraz wydobywaniem informacji. W ten sposób percepcja zostaje poszerzona o połączenie wielu części informacji i określenie ich związku z wcześniej określonymi celami, co może prowadzić do wyciągnięcia wniosków na temat tych celów. Rozumienie zapewnia ustrukturyzowany ogląd obecnej sytuacji poprzez ustalenie znaczenia obiektów i wydarzeń. Łączy ono nowe informacje z już istniejącą wiedzą w celu wytworzenia pełnego poglądu odnośnie rozwoju sytuacji [12].

Antycypacja jest najwyższym poziomem świadomości sytuacyjnej. Jest ona definiowana, jako zdolność do tworzenia prognoz opartych o wynik zrozumienia (i percepcji) [12].

McGuinness i Foy [16] rozszerzyli ten model dodając czwarty poziom, zwany rezolucją (ang. *resolution*), której celem jest określenie optymalnej ścieżki dla osiągnięcia pożądanej zmiany stanu bieżącej sytuacji. Rezolucja oparta jest na wyborze pojedynczego działania z podzbioru dostępnych działań [14].

W ramach projektu DEnSeK [17] opracowano pulpit nawigacyjny (ang. *dashbard*) dla operatorów systemu świadomości sytuacyjnej (ang. *Situational Awareness Network)*. Oprogramowanie to wizualizuje dane zebrane ze zbioru rozproszonych czujników. W czasie projektowania testów opracowane oprogramowania SAN było przystosowane do gromadzenia danych z dwóch źródeł. Pierwszym z nich był analizator sieci Argus, używany do zbierania danych o aktywności ruchu sieciowego w chronionej sieci. Drugi to OSSIM – kompleksowy i otwarty system SIEM (system zarządzania informacjami i zdarzeniami dotyczącymi bezpieczeństwa). Ponieważ OSSIM w zaprojektowanej sieci SAN pełni rolę warstwy pośredniej, możliwe jest podłączenie do pulpitu nawigacyjnego dużej liczby czujników, w tym np. najbardziej popularnych systemów wykrywania włamań takich jak Snort i Suricata.



Rys. 2. SAN architektura trójpoziomowa

Architektura SAN proponowana w projekcie DEnSeK może być zaprezentowana, jako struktura trójwarstwowa (rys. 2). Najniższa warstwa – warstwa danych składa się z czujników takich jak systemy wykrywania włamań oraz monitory i analizatory ruchu sieciowego. Oprogramowanie

OSSIM pracuje w warstwie logicznej, gdzie gromadzi i przetwarza dane z czujników i przekazuje je do warstwy najwyższej. Wreszcie warstwa prezentacji – pulpit nawigacyjny, po dalszej obróbce wizualizuje dane w formie przyjaznego dla użytkownika interfejsu.

4. ŚRODOWISKO TESTOWE

Testy zostały przeprowadzone w Livorno, w laboratorium cyberbezpieczeństwa, będącego częścią działu badań i inżynierii największego włoskiego koncernu energetycznego, firmy ENEL.

Laboratorium zostało zaprojektowane i zbudowane z myślą o testowaniu i rozwoju aplikacji służących do automatyzacji procesów przemysłowych. Jego celem jest odtworzenie architektury sieci i głównych komponentów sterowania procesami w rzeczywistej elektrowni (układ gazowo-parowy z turbiną gazową). Z punktu widzenia technologii informacyjno-komunikacyjnych, struktura i konfiguracja sieci jest analogiczna do sieci telekomunikacyjnej w elektrowni. Znajdują się tam wszystkie główne elementy sieci sterowania procesami przemysłowymi, w tym sterowniki PLC i rozproszony system sterowania (ang. *Distributed Control System* – DCS) z komponentami od różnych dostawców. W laboratorium odtworzono procesy związane z obiegiem ciepłej i zimnej wody w elektrowni cieplnej. Wszystkie procesy są monitorowane i sterowane przez sterowniki PLC przy użyciu rzeczywistych urządzeń pomiarowych i wykonawczych takich jak czujniki, mierniki ciśnienia, zawory, pompy, falowniki itp.

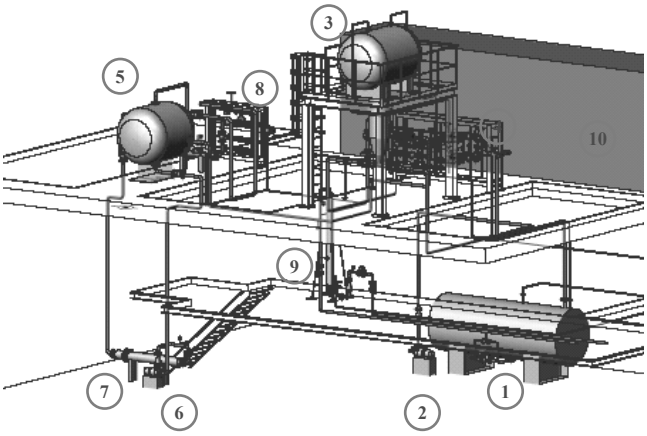
Środowiska informatyczne elektrowni zazwyczaj obejmują kilka rodzajów systemów, podsystemów i podzespołów:

- *System Polowy* (ang. *Field System*), grupujący wszystkie sterowniki PLC, RTU oraz czujniki w elektrowni,
- *Kontrola Procesu i System Akwizycji Danych* (ang. *Process SCADA*), który kontroluje System Polowy,
- *Sieć Sterowania* (ang. *Control Network*), która zapewnia obsługę komunikacyjną w całej elektrowni,
- Sieć Danych (ang. *Data Network*), pozwalająca połączyć różne elektrownie,
- Sieć Biurowa (ang. *Business Network*) z typowymi aplikacjami intranetowymi,
- Strefa Zdemilitaryzowana (ang. *Demilitarised Zone*), gdzie znajdują się serwery służące do udostępniania danych dotyczących procesów przemysłowych w elektrowni.

Systemy te zostały odtworzone w bezpiecznym, odizolowanym (fizycznie odłączonym od innych sieci) środowisku laboratorium bazując na sprzęcie komputerowym i sieciowym oraz urządzeniach SCADA zainstalowanych w fizycznej instalacji hydrologicznej *Fizycznego Modelu Elektrowni* (ang. *Physical Power Plant Emulator*) (patrz rys. 3).

W laboratorium niezwykle wiernie zrekonstruowano system informatyczny elektrowni. Odtworzono identyczne podsieci oraz skopiowano wszystkie główne stacje robocze elektrowni w stosunku jeden do jednego. Oznacza to, że każde ze stanowisk elektrowni znalazło odzwierciedlenie w jednym komputerze środowiska symulacyjnego. Jedynie środowisko intranetu zostało zaprezentowane za pomocą mniejszej liczby hostów. W rekonstrukcji, użyto te same adresy sieciowe, zainstalowano identyczne oprogramowanie (z uwzględnieniem tego samego poziomu „łatek" systemowych), odtworzono te same konfiguracje zapór sieciowych, itp.

Fizyczny Model Elektrowni (rys. 3) odtwarza obieg parowy-wodny typowy dla większości elektrowni cieplnych. Składa się z trzech modułów: M1, M2, M3. M1 jest sekcją hydrauliczną, w której woda przepływa w obiegu zamkniętym (pomiędzy dwoma zbiornikami usytuowanymi na różnych wysokościach), w temperaturze otoczenia. Zbiornik na niższym poziomie przechowuje wodę o ciśnieniu otoczenia. Drugi zbiornik znajduje się nad nim i przechowuje wodę pod ciśnieniem zmieniającym się od 0 do 4 barów. M2 jest innym fragmentem obwodu hydraulicznego, gdzie wymuszany jest przepływ wody w obiegu pomiędzy grzejnikiem (270 kW) oraz zbiornikiem cylindrycznym i jest odparowywana za pomocą pompy. Para mokra jest osuszana w podgrzewaczu (30 kW). Woda przepływającym w tym module pochodzi z M1. M3 jest blokiem turbiny zawierającym trzy zawory regulacyjne rozmieszczone równolegle, przez które przepływa para sucha zmieniając ciśnienie zadawane z poziomu sterowni. Moduł M1 jest „zimną" częścią instalacji, podczas, gdy moduły M2 i M3 razem stanowią część „gorącą" instalacji. Część zimna i ciepła są połączone poprzez wymiennik cieplny, w którym para pochodząca z M3 skrapla się i w postaci ciekłej trafia do zbiornika dolnego M1. Zimna i ciepła część instalacji są funkcjonalnie niezależne, co pozwala symulować trzy różne konfiguracje pracy elektrowni: M1, M2 z M3 lub M1, M2 i M3 razem. Wszystkie opisane dalej testy za wyjątkiem scenariusza 4 z konfiguracją 2 przeprowadzono w tym obszarze laboratorium.



Rys. 3. Składniki Fizycznego Modelu Elektrowni:
1 – zbiornik, 2 – pompa, 3 – zbiornik piezoelektryczny, 4 – obieg recyrkulacyjny, 5 – zbiornik cylindryczny (za nagrzewnicą 30 kW), 6 – pompa podgrzewu, 7 – grzałka 270 kW, 8 – blok turbiny, 9 – skraplacz, 10 – sterownia

Podczas realizacji testów wykorzystano trzy komputery na których uruchamiane były maszyny wirtualne z testowanym oprogramowaniem: (1) Windows 7: Intel Core i7-Q720, 8 cores, 1.6 GHz, 16 GB RAM; (2) Linux Mint: Intel Core i5-3317U, 4 cores, 1.7 GHz, 8 GB RAM; (3) Kali Linux: Intel Core i3, 2 cores, 1.2 GHz, 4 GB RAM.

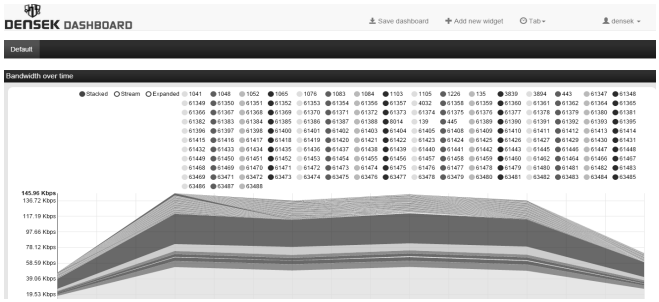
5. PROCEDURA TESTOWA

Celem przeprowadzonych badań było sprawdzenie dopasowania architektury SAN i jej wybranych komponentów do złożonego środowiska elektrowni. W ramach eksperymentu przygotowano testy integralności. Opracowano pięć przypadków testowych w celu zweryfikowania poprawności wzajemnej współpracy poszczególnych składników SAN. Testowano następujące składniki:

- *Argus* – analizator sieci,
- *Snort* – sieciowy system wykrywania włamań,
- *OSSIM* – system SIEM,
- *DEnSek Dashboard* – pulpit nawigacyjny dla operatorów systemu świadomości sytuacyjnej.

W celu przeprowadzenia testów konieczne było wykorzystanie dodatkowego oprogramowania *TCPReplay*, *Oinkmaster* i *Barnyard2*. W pierwszej części procesu testowego

zweryfikowano poprawność interakcji pomiędzy poszczególnymi składnikami systemu. Realizacja dwóch pierwszych przypadków testowych miała na celu sprawdzenie współpracy pulpitu nawigacyjnego z analizatorem Argus, jako źródłem danych. Podczas tych testów zidentyfikowano kilka problemów związanych z procesem przetwarzania i wizualizacji dużej ilości danych specyficznych dla środowiska elektrowni (np. patrz rys. 4), które następnie zostały poprawione przez programistów.



Rys. 4. Nieczytelna prezentacja danych na pulpicie

W drugiej części testowania (przypadki 3 i 4), zweryfikowano integrację systemu wykrywania włamań Snort z systemem SIEM – Ossim. Ponieważ oba systemy są dojrzałymi projektami rozwijanymi w ramach Otwartego Oprogramowania (ang. *Open Source*) ich instalacja i konfiguracja przebiegły sprawnie. Jednak badania w środowisku o dużej skali pozwoliło na identyfikację problemów z komunikacją między podsieciami. W docelowych systemach sensory będą rozmieszczone między różnymi regionami, państwami, a nawet kontynentami. Dlatego niezbędne jest opracowanie odpowiedniej metody komunikacji z centralnym systemem SIEM.

Ostatnie badania były poświęcone pełnej integracji systemu SAN. Przetestowano poprawność komunikacji między wszystkimi warstwami architektury (rys. 2). Dane zebrane przez sensory (Snort) zostały przekazane do systemu SIEM (OSSIM). Tam, po zagregowaniu danych i analizie wygenerowane zostały alarmy, które następnie zostały przekazane do pulpitu nawigacyjnego. W konsekwencji operator został poinformowany o wykrytych zagrożeniach za pośrednictwem elementów graficznych (ang. *widgets*) na pulpicie nawigacyjnym. Testy potwierdziły właściwe zaprojektowanie architektury SAN oraz jej użyteczność.

6. PODSUMOWANIE

Ryzyko związane z cyberatakami w sektorze elektroenergetycznym systematycznie rośnie. Wynika to z jednej strony z rosnącego uzależnienia gospodarki i społeczeństwa od energii elektrycznej, z drugiej strony z coraz większego wykorzystania technologii informacyjnych w sektorze elektroenergetycznym. Systemy świadomości sytuacyjnej wspomagają monitorowanie infrastruktury elektroenergetycznej w celu wczesnego wykrywania zagrożeń i ograniczenia ich skutków. W projekcie DEnSeK opracowano i wdrożono trójwarstwową platformę SAN. Testy integracyjne przeprowadzone w laboratorium cyberbezpieczeństwa ENEL ??udowodniły, że architektura i komponenty systemu są prawidłowo dobrane, a system działa zgodnie z przeznaczeniem.

7. BIBLIOGRAFIA

[1] T. Bayar, "Cybersecurity in the power sector," Power Engineering International, 2014.

[2] Y. Aillerie, S. Kayal, J. Mennella, R. Samani, S. Sauty, L. Schmitt: "Smart Grid Cyber Security," 2013.

[3] Y. Yan, Y. Qian, H. Sharif, D. Tipper: "A Survey on Cyber Security for Smart Grid Communications," IEEE Commun. Surv. Tutorials, vol. 14, no. 4, pp. 998–1010, 2012.

[4] D. Kushner: "The real story of stuxnet," IEEE Spectr., vol. 50, pp. 48–53, 2013.

[5] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. Nai Fovino, A. Trombetta: "A Multidimensional Critical State Analysis for Detecting Intrusions in SCADA Systems," IEEE Trans. Ind. Informatics, vol. 7, no. 2, pp. 179–186, May 2011.

[6] H. Khurana, M. Hadley, N. Lu, D.A. Frincke: "Smart-grid security issues," IEEE Secur. Priv., vol. 8, no. 1, pp. 81–85, 2010.

[7] "DEnSeK (Distributed Energy Security Knowledge) – project website." [Online]. Available: http://www.densek.eu/. [Accessed: 08-04-2014].

[8] R. Kissel: "NISTIR 7298 Revision 2 Glossary of Key Information Security Terms," 2013.

[9] ISO/IEC, "ISO/IEC 27001:2005(E): Information technology – Security techniques – Information security management systems – Requirements." U.S. Government Printing Office, 2005.

[10] K. Stouffer, J. Falco, K. Scarfone: "NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security." 2011.

[11] M. Vidulich, C. Dominguez, E. Vogel, G. McMillan: "Situation Awareness: Papers and Annotated Bibliography," Jun. 1994.

[12] G.P. Tadda, J.S. Salerno: "Overview of Cyber Situational Awareness," in Cyber Situational Awareness, vol. 46, S. Jajodia, P. Liu, V. Swarup, and C. Wang, Eds. Boston, MA: Springer US, 2010, pp. 15–35.

[13] M.R. Endsley: "Toward a theory of situation awarenss in dynamic systems," Hum. Factors, vol. 37, pp. 32–64, 1995.

[14] B. McGuinness, L. Foy: "A Subjective Measure of SA The Crew Awareness Rating Scale – GetInfo," in Proceedings of the first human performance, situation awareness, and automation conference, 2000.

[15] R. Leszczyna, M. Wrobel: "Security Information Sharing for Smart Grids. Developing the Right Data Model," in Accepted for the 9th International Conference for Internet Technology and Secured Transactions (ICITST 2014, 2015.

TESTING SITUATION AWARENESS NETWORK FOR THE ELECTRICAL POWER INFRASTRUCTURE

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 the 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.

Keywords: electric grid, cyber security, situational awareness, testing