**Jacek MALKO, Robert LIS**

Politechnika Wrocławska, Wydział Elektryczny, Katedra Energoelektryki

doi:10.15199/48.2016.01.43

# Cyberbezpieczeństwo systemów zabezpieczeń i sterowania

***Streszczenie.*** *W artykule opisano, postrzegane przez inżynierów i techników zabezpieczeń i sterowania, stojące przed nimi wyzwania związane z zarządzaniem systemami zabezpieczeń i sterowania w obliczu konieczności zarządzania środkami cyberbezpieczeństwa w zakresie zastosowań w skali systemów, podsystemów i elementów. Celem jest objaśnienie problemów zarządzania cyberbezpieczeństwem, poprawy jakości szkolenia rozpoznawania ataków cybernetycznych i dostarczenie wskazówek do interpretacji i stosowania odpowiednich norm i wytycznych.*

***Abstract****. This paper describes, through the eyes of protection and control engineers and technicians, the challenges they face when required to manage cybersecurity applications and process for their systems, subsystems, and components. The objective is to demystify cybersecurity management, improve training to recognize cyber-induced faults, and to provide some guidance to interpret and apply the relevant standards and guidelines. (**Cybersecurity Measures for Protection and Control Systems**).*

**Słowa kluczowe**: cyberbezpieczeństwo, środki dla zabezpieczenia i sterowania
**Keywords**: cybersecurity, measures to protection and control

## Wstęp

Niewiele jest przypadków tak oszałamiającej kariery, jaka przydarzyła się rzeczownikowi „bezpieczeństwo". Wielowymiarowość tego określenia w kontekście socjalnym, ekonomicznym, militarnym, środowiskowym i energetycznym (przy czym ta lista jest daleka od kompletności) wraz z dramatycznymi konsekwencjami niedotrzymania określonych standardów, wzbogaciła się stosunkowo niedawno o nowy wymiar: cyberbezpieczeństwo („cybersecurity"). Wrażliwość systemu energetycznego na ataki terrorystyczne zmusza do pilnych i skutecznych poszukiwań środków zaradczych. „Rosnące ryzyko cyberataków na sektor dostaw energii stwarza dla operatorów systemów IT infrastruktury energetycznej zagrożenia, których nie sposób zlekceważyć" [1,2]. Problem cyberbezpieczeństwa w energetyce stał się „tematem okładkowym" („cover story") specjalnego wydania magazynu Power Engineering Intern. (PEI) koncernu medialnego PennWell [3]. Wagę zagadnienia dostrzeżono również w światowej organizacji CIGRE (Conseil International des Grands Reseaux Electriques), co przejawiło się powołaniem wspólnej grupy roboczej (Joint Working Group B-5/D2), skupiającej reprezentantów Komitetów Studiów „Zabezpieczenia i Automatyka" (SC B5) i „Systemy Informacyjne i Telekomunikacja" (SC D2). Wyłonieni przez Komitety Narodowe CIGRE specjaliści z 16 krajów (od Australii po Zjednoczone Królestwo) pod kierunkiem Dennisa Dolsteina z USA opracowali ważny dokument – Technical Brochure 603 „Zastosowanie i Zarządzanie Cyberbezpieczeństwem – Środki dla Zabezpieczenia i Sterowania" [4,5]. Na przeszło 120 stronach tekstu przedstawiono – zgodnie z autorską deklaracją, wyzwania na które napotykają się inżynierowie, odpowiedzialni za systemy zabezpieczeń i sterowania w obliczu konieczności zarządzania środkami cyberbezpieczeństwa w zakresie zastosowań w skali systemów, podsystemów i elementów. W porównaniu z klasycznym zakresem odpowiedzialności i działań personelu środowisko cechuje się wysoką dynamiką i zagrożeniami cybernetycznej natury [4]. Istotne jest zastrzeżenie definicyjne: termin „cyberbezpieczeństwo", użyty w Broszurze ma odmienne znaczenie od terminu „bezpieczeństwo" w kontekście zastosowań industrialnych, nie uwzględniającego bezpieczeństwa systemów informacyjno-komunikacyjnych, tworzących infrastrukturę zabezpieczeń i sterowania (P&C) [4].

Aczkolwiek inżynierowie, odpowiedzialni za zabezpieczenia i sterowanie są nieodzownymi uczestnikami zespołów, pracujących na rzecz bezpieczeństwa systemu elektroenergetycznego, to ich pierwszoplanowa rola polega na niezawodnym realizowaniu zaaprobowanej polityki bezpieczeństwa, współpracującej z systemami automatyki użytkowanych, dedykowanych technologii. Broszura stara się znaleźć odpowiedź na następujące problemy:

- szkolenia w zakresie cyberbezpieczeństwa dla wykrycia błędów, powodowanych przez systemy „cyber";
- nauka, zaczerpnięta z dobrze opisanych ataków na podobne systemy operacyjne;
- trudności wynikające przy interpretowaniu i stosowaniu odnośnych standardów i zaleceń;
- ograniczenia wynikające z pracy ciągłej („24/7"), mechanizmów kompensacyjnych dla zapewnienia systemów wykonawczych oraz urządzeń inteligentnej elektrowni w warunkach ograniczonych zasobów, a także:
- zarządzanie środkami udostępnienia oraz wykorzystanie wyposażenia sterującego, dostępu do danych oraz zasobów sieciowych.

## System P&C – zabezpieczenie i sterowanie

Przedsiębiorstwo elektroenergetyczne (PE) musi rozważyć szeroki zakres problemów eksploatacyjnych w celu zarządzania stabilnością swych systemów oraz zapewnienia w sposób niezawodny dostaw energii klientom. Broszura nie zajmuje się tymi wszystkimi problemami, co będzie zadaniem przyszłych grup zadaniowych, które podejmą się zastosowań i zarządzania mechanizmami cyberbezpieczeństwa dla systemów sterowania i pobierania danych (SCADA) oraz sterowaniem w sieci w procesach eksploatacji SEE.

Broszura Techniczna skupia się zasadniczo na mechanizmach cyberbezpieczeństwa, stosowanych dla zabezpieczania składników majątku i ochrony systemu, konfiguracji systemów zintegrowanej ochrony oraz sterowaniem lokalnymi stacjami wraz z automatyzacją. Personel odpowiedzialny za systemy P&C wymaga skonfigurowania oraz zdalnego dostępu i wykorzystania mechanizmów sterowania elementami P&C i sieci. Co więcej - od inżynierów P&C wymaga się konfigurowana i utrzymywania w gotowości mechanizmów sterowania dla lokalnych dojść do urządzeń poprzez stacje lokalne (LAN) lub porty komunikacyjne urządzeń. Opracowanie rozważa również nowoczesne układy zabezpieczeń, łącznie z wykorzystaniem sieci komunikacyjnych o dużych prędkościach, oraz dostęp i stosowanie urządzeń sieciowych (takich jak routery i przełączniki). Celem

niniejszej Broszury jest doradztwo inżynierom-specjalistom od zabezpieczeń, technikom-ekspertom oraz zarządzającymi systemami P&C. Wszyscy oni są zaznajomieni z technicznymi środkami cyberbezpieczeństwa i mają dostęp i możliwość korzystania z systemów P&C. Mierzone charakterystyki weryfikują prawidłowość nastaw poziomu cyberbezpieczeństwa. Nastawy te mają być zdolne do spełnienia trzech zasadniczych wyzwań:

- zarządzanie zdarzeniami,
- zarządzanie wrażliwością, modularnością oraz konfiguracją,
- bezpieczeństwo stosowania.

Równie ważne są możliwości sterowania jakościowego cyberbezpieczeństwem oraz konieczność opisania założeń, na których opiera się zarządzanie technicznymi aspektami sterowania.

Narodowa architektura cyberbezpieczeństwa wymaga podejścia całościowego (holistycznego) oraz traktowania w kategoriach systemowych. Ocena architektury jest niezbędna dla rozmieszenia organów sterowania w odpowiednich miejscach i uzyskania ogólnej akceptacji podejmowanych działań. Powszechną polityką jest umieszczanie architektury cyberbezpieczeństwa w funkcjonalnej architekturze systemu. Takie podejście obejmuje sterowanie rozproszone i funkcjonalność zabezpieczeń. Co więcej – nowe schematy zabezpieczeń mogą być wprowadzane w stacjach i centrach sterowania.

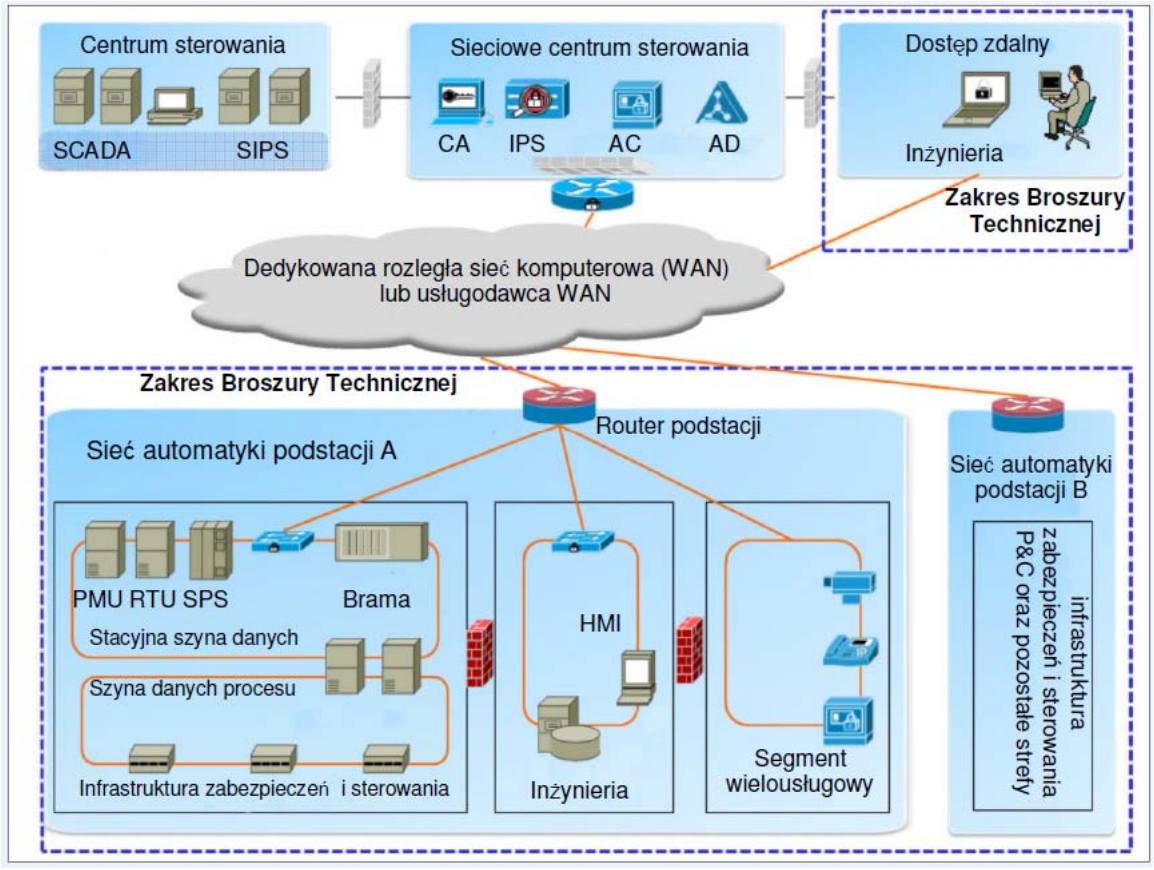
Rysunek 1 uwzględnia cztery zasadnicze przypadki w odniesieniu do P&C:

- automatyka stacji,
- relacje stacja-do-stacji,
- relacje stacja-centra sterowania,
- zdalne wywoływanie działań.

Podstawowym elementem składowym (zgodnie z założeniami TB 603) jest stacja elektroenergetyczna, zawierająca sieć automatyki. Logiczna segmentacja prowadzi do wyodrębnienia fragmentów sieci, umożliwiając oddzielenie obwodów poszczególnych klas zastosowań (np. SCADA, obwody dla celów bieżącej eksploatacji, „engineering"), współpracujących z wirtualnymi sieciami obszaru lokalnego (VLANs). Ponadto „ściany ogniowe" strefowe zapewniają wzmożone cyberbezpieczeństwo obwodów peryferyjnych. Na rys. 1 sieć automatyki stacji składa się z trzech segmentów (stref):

- P&C, który zgodnie z zaleceniami IEC 61850 dzieli się na szyny stacji i szyny procesowe,
- „engineering",
- segment wielousługowy.

Charakterystyki techniczne urządzeń sieciowych (łączników, routerów oraz ścian ogniowych) umożliwiają osiągnięcie elastyczności oraz rozbudowę architektury cyberbezpieczeństwa. W razie potrzeby architekturę rozbudować można o większą liczbę segmentów/stref w oparciu o nowe funkcje i związane z tym modyfikacje polityk.




Rys.1. Architektura narodowa, przyjęta w Broszurze Technicznej TB 603. Objaśnienia do rysunku: SIPS- System Integrity Protection Schemes - system ochrony integralności systemu, CA - Certificate Authority - centrum certyfikacji, IPS - Intrusion Prevention System – system zapobiegania włamaniom, AC – Access Control – kontrola dostępu, AD - Active Directory – usługa katalogowa (hierarchiczna baza danych), PMU – Phasor Measurement Unit - synchrofazorowy system pomiarowy, RTU – Remote Terminal Unit – zdalne moduły transmisyjne, SPS – Special Protection Schemes – schemat systemu ochrony, P&C – Protection and Control, infrastruktura zabezpieczeń i sterowania, HMI - P&C Human-Machine Interface - interfejs człowiek-maszyna

Tabela 1. Cyberataki i środki przeciwdziałania

| Kategoria ataku | Typ ataku | Możliwe konsekwencje | Środki przeciwdziałania |
|---|---|---|---|
| Blokada | Niemożność świadczenia usługi: zalew strumieni danych P&C, przekroczenie zasobów systemowych lub nakładanie się na komunikację P&C. | Utrata dostępu do danych P&C | Peryferyjne ściany ogniowe, sterowanie routerami sieci P&C, zwielokrotnianie zasobów, rozproszony pakiet filtrujący z filtracją dynamiczną i zagregowane sterowanie ograniczeniami |
| | Zakłócanie: interferencja elektromagnetyczna lub nakładanie się sygnałów o tym samym paśmie częstotliwości dla sygnałów bezprzewodowych | Utrata dostępu do danych P&C | Zastosowanie środków przeciwdziałającym zakłóceniom, aktywne przeciwdziałanie zakłóceniom, klatka Faradaya<br>UWAGA: Klatka Faradaya lub ekran Faradaya jest obudową utworzoną przez materiał przewodzący lub siatkę z takiego materiału. Taka obudowa blokuje zewnętrzne pola elektryczne (statyczne i niestatyczne |
| | Nielegalne oprogramowanie i rozpowszechnianie wirusów, robaków, koni trojańskich, programów szpiegowskich i innych programów, nakładających się na P&C składowych systemu | Utrata dostępu do danych P&C, utrata poufności danych | Programy antywirusowe, peryferyjne programy ogniowe, kontrola ruchu sieciowego poszczególnych aplikacji z wykorzystaniem technologii białej listy „whitelisting”.<br>Uwaga 1: Zwracać uwagę na pojawiające się duże zmiany i procedury zarządzania zawierające stosowanie „whitelisting”.<br>Uwaga 2: Stosowanie „whitelisting” powoduje ryzyko odmowy wykonania uprawnionych działań P&C przy zmianie kodu tych aplikacji (np. w wyniku zastosowania łatek systemowych („patching”)). |
| | Fuzzing: wprowadzenie nieuprawnionych, nieoczekiwanych lub losowych danych, interferujących o komunikację P&C | Utrata integralności i dostępności danych | Peryferyjne ściany ogniowe i wykrywanie ingerencji zewnętrznych |
| Naśladownictwo i modyfikowanie | Spoofing: wykrycie osoby lub autoryzowanego użytkownika P&C lub programu P&C dla uzyskania autoryzowanego dostępu | Utrata poufności i integralności danych | Kontrola identyfikacji na bazie P&C, dostęp „z klucza”, bezpieczeństwo IP, podpis cyfrowy |
| | Tampering: celowe uszkodzenie lub fałszowanie danych P&C | Utrata integralności danych | Funkcje „hash”, cykliczna kontrola redundancji, kody identyfikujące P&C |
| | Klonowanie: powtórzenie i ponowny zapis ważnych danych P&C jako równoważnego zbioru | Utrata poufności danych P&C | Uniemożliwienie fizykalne procesu klonowania w P&C |
| | „Replay”: zapis i przechowywanie uprzednio wysłanych danych P&C dla ich powtórzenia lub opóźnienia bieżącej sesji | Utrata poufności danych P&C | Znaczniki czasu w P&C, synchronizacja czasowa, liczby pseudolosowe, identyfikatory sesji, liczby seryjne |
| Pozyskanie zbiorów | „Skimming”: szybkie odczytywanie przesyłanych komunikatów P&C dla zbioru danych | Utrata poufności danych P&C | Encryption and Steganography<br>UWAGA: steganografia jest nauką i sztuką zapisywania ukrytych komunikatów w plikach komputerowych w taki sposób, by nikt - oprócz nadawcy i uprawnionego odbiorcy - nie podejrzewał istnienia tego komunikatu – jest to forma zapewnienia bezpieczeństwa przez zatajenie. |
| | Podsłuch: pozyskiwanie wymienianych komunikatów P&C | Utrata poufności danych P&C | Encryption: potwierdzenie autentyczności na bazie P&C oraz agregacja zatajonych danych P&C (CDA) |
| | Analiza przepływu danych i monitorowanie wymiany danych P&C dla określenia wzorów przepływu | Utrata poufności danych P&C | Wykrywanie nielegalności i niewłaściwych zachowań w sieci P&C |
| Prywatność | Zindywidualizowany: pozyskanie wiedzy o lokalizacji użytkownika P&C, preferencje, zachowania i inne informacje prywatne | Utrata poufności danych P&C | Próbki zagregowane, anonimowe przepływy danych P&C, CDA i zaawansowany podpis cyfrowy.<br>PRZYKŁAD podpisy niewidoczne, grupowe i kołowe |
| | Grupowy: wykrycie funkcjonalnych odpowiedzialności organizacyjnych P&C, uprawnień i szpiegostwo | Utrata poufności danych P&C | Selektywne ujawnianie, niszczenie danych P&C |

**Cyberataki i przeciwdziałanie w systemach P&C**

Broszura (TB 603) wiele uwagi poświęca typom cyberataków, ich możliwym konsekwencjom oraz środkom przeciwdziałania ze strony personelu P&C. Z tego względu celowe jest dokonanie oceny typowych ataków w oparciu o powtarzalne wzorce, z wyodrębnieniem czterech kategorii tych ataków (Tab. 1)

**„Dziesięć przykazań”**

Przegląd cech i uwarunkowań cyberataków daje się sprowadzić do 10 następujących rekomendacji:

1. Zakres i poziom ochrony przeciw cyberatakom winien odpowiadać specyfice i być odpowiedni dla składników majątku zabezpieczeń i sterowania, narażonym na ryzyko. Nie istnieje jedno uniwersalne rozwiązanie, a dostosowanie do specyficznych cech w oparciu o analizę ryzyka daje właściwy kontekst, wynikający ze struktur organizacyjnych i polityk.
2. Mechanizmy cyberbezpieczeństwa winny zapewniać zdecydowane, proste i skalowalne oraz łatwe w zarządzaniu środki, będące częścią normalnych obowiązków personelu P&C.
3. O ile jest to wykonalne w oparciu o ocenę ryzyka układu przetwarzania energii inteligentne urządzenia elektroniczne i ich aplikacje muszą mieć zdolność do wzajemnej komunikacji z wykorzystaniem otwartych bezpiecznych protokołów w rodzaju opisanych w dokumencie IEC62351.
4. Wszystkie urządzenia P&C muszą być zdolne do zapewnienia własnej polityki cyberbezpieczeństwa (lub też zapewnić ochronę kompensacyjną) przy niezabezpieczonej sieci.
5. Personel P&C na każdym stanowisku pracy, łącznie z kontrolowanymi procesami oraz stosowanymi środkami cyberbezpieczeństwa, musi dysponować zadeklarowanymi i transparentnymi poziomami zaufania dla przeprowadzenia każdej wymiany danych.
6. Inteligentne urządzenia elektroniczne P&C muszą mieć zdolność do działania (dwukierunkowo) na odpowiednim poziomi autoryzacji dla dostępu do systemów i danych.
7. Poza obszarem sterowania P&C, uwierzytelnienie, autoryzacja i odpowiedzialność wymagająca zwrócenia bacznej uwagi na wiarygodność transmisji danych przez zewnętrzne interfejsy.
8. Zgodnie z wymaganiami IEC62351 dostęp do danych P&C jest poddany kontroli.
9. Prywatność danych (oraz cyberbezpieczeństwo dowolnego składnika majątkowego P&C o dostatecznie dużej wartości) wymaga segregacji wykonywanych czynności oraz ich uprzywilejowania, wymuszonych przez silny mechanizm kontroli dostępu (RBAC).
10. Przy przechowywaniu, w stanach przejściowych lub podczas użytkowania lub niewłaściwej obsługi stosowane mechanizmy muszą zapewnić bezpieczeństwo danych P&C.

***Autorzy***: *prof. dr hab. inż. Jacek Malko, Politechnika Wrocławska, Wydział Elektryczny, Katedra Energoelektryki, Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, dr hab. inż. Robert Lis, Politechnika Wrocławska, Wydział Elektryczny, Katedra Energoelektryki, Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, E-mail: Robert.Lis@pwr.edu.pl.*

LITERATURA

[1] Malko J., Wojciechowski H.: Sektor energetyczny i cyberbezpieczeństwo. *Nowa Energia*, nr 1 (43) 2015

[2] Amanowicz M.: Cyberbezpieczeństwo krajowego systemu elektroenergetycznego - świadomość sytuacyjna w warunkach zagrożeń, XVIII seminarium "Automatyka w elektroenergetyce", Energotest, 22 - 24. 04. 2015

[3] Bayar T.: Cybersecurity in the power sector. *Power Eng. Intern*. Vol. 22, Iss. 9, Oct. 2014

[4] CIGRE Joint Working Group: Application and Management of Cybersecurity Measures for Protection and Control. JWG B5/D2, Paris, Dec. 2014

[5] CIGRE JWG B5/D2.46: Technical Brochure 603 „Application and Management of Cybersecurity” *Electra* No 278, Febr. 2015