prof. nzw. dr hab. inż. Désiré Dauphin Rasolomampionona

POLITECHNIKA WARSZAWSKA
Instytut Elektroenergetyki

ul. Koszykowa 75, 00-662 Warszawa

tel. 22 234 73 51 fax. 22 234 56 17
e-mail: desire.rasolomampionona@ ien.pw.edu.pl

Warszawa, 26.01.2018 r.

Recenzja rozprawy doktorskiej pt.:

„ Bezpieczeństwo cyfrowe inteligentnych dystrybucyjnych sieci elektroenergetycznych ”

opracowanej przez mgr. inż. **Roberta Czechowskiego**

promotor: prof. dr hab. inż. Eugeniusz Rosołowski

Podstawą opracowania tej recenzji jest uchwała Rady Wydziału Elektrycznego Politechniki Wrocławskiej z dnia 27.11.2017 r. oraz pismo Pana dziekana Wydziału Elektrycznego prof. dr hab. Waldemara Rebizanta z dnia 29.11.2017 r.

1. Wybór tematu rozprawy

Recenzowana rozprawa doktorska jest rezultatem kilkuletnich badań autora Pana mgr. inż. **Roberta Czechowskiego** nad projektowaniem i eksploatacją bezpiecznych inteligentnych dystrybucyjnych sieci elektroenergetycznych. Jak napisał autor „*Omówione w pracy rozwiązania pozwolą na zwiększenie poziomu bezpieczeństwa z perspektywy zagrożeń oraz potencjalnych ataków*”. Praca jest obszerna, gdyż razem z załącznikami liczy ponad 250 stron.

Inteligentna sieć to szybko rozwijająca się technologia, której celem jest dostarczanie energii elektrycznej od dostawców elektrycznych do domostw za pomocą technologii cyfrowej, przy uwzględnieniu interakcji z urządzeniami gospodarstwa domowego. Celem tej interakcji jest systematyczne zaoszczędzanie energii, zmniejszanie kosztów i zwiększanie niezawodności. Pod pojęciem sieci inteligentnej rozumie się łączenie technologii informatycznej i telekomunikacyjnej z technologią procesów energetycznych, umożliwiające przepływ mocy w dwóch kierunkach, w celu uzyskania bezproblemowego działania w zakresie wytwarzania, przesyłu i dystrybucji energii do końcowego użytkownika energii elektrycznej oraz umożliwienia szerokiego zastosowania energii odnawialnej i pojazdów elektrycznych.
Logiczną konsekwencją rozwoju sieci inteligentnych jest to, że systemy elektroenergetyczne stają się coraz bardziej złożone, a stopień ich niepewności coraz wyższy. Ta sytuacja uzasadnia konieczność przeprowadzenia bardziej aktywnej diagnostyki i monitorowania w czasie rzeczywistym. Dzięki temu stabilność przyszłej sieci energetycznej jest zapewniona, a koszty eksploatacji mniejsze. Jest kilka czynników, od których zależy przyszły rozwój

systemów elektroenergetycznych: 1) integracja odnawialnych źródeł o produkcji losowej jak źródła oparte na energii słonecznej lub wiatrowej; 2) coraz intensywniejsza wymiana energii między różnymi obszarami; 3) duży nacisk na wprowadzenie bardziej konkurencyjnych i wolnych rynków energii elektrycznej.
Wszystkie te czynniki w większym lub mniejszym stopniu wymagają konieczności posiadania systemu telekomunikacyjno-informatycznego, obsługującego większość operacji w systemach elektroenergetycznych w celu wymiany danych, komunikowania się poszczególnych elementów SEE, analizowania i kontrolowania pracy sieci elektroenergetycznej. Ponadto, wraz z rozwojem inteligentnych liczników i urządzeń pomiarowych typu PMU, powstają bardzo duże zbiory danych, które muszą być przekazywane i analizowane w czasie zbliżonym do rzeczywistego. Te różne zadania powinny być wykonywane automatycznie, z wysoką częstotliwością i w krótkich odstępach czasu, aby przyszły SEE mógł sprawnie działać.

Krótki przegląd literatury

Chociaż technologia inteligentnych sieci jest wciąż na wczesnym etapie rozwoju, jej obecne wdrożenie już przyniosło pewne korzyści. Na przykład wielu dostawców energii elektrycznej już w latach 90-tych poprzedniego wieku korzystano z automatycznego odczytu liczników elektrycznych (AMR) [1] w celu zbierania danych. Korzystając z przewodowych lub bezprzewodowych technologii komunikacyjnych, system AMR może zapewniać jednokierunkową komunikację z liczników do czytnika danych (za pośrednictwem bramy). Dlatego w porównaniu z konwencjonalną siecią energetyczną wykorzystanie AMR oszczędza dostawcom usług koszty okresowych wyjazdów do każdej fizycznej lokalizacji mierników w celu odczytania licznika. Istotnym elementem systemu inteligentnych sieci jest *Advanced Metering Infrastructure* (AMI) [2], czyli infrastruktura mierników inteligentnych, która zapewnia dwukierunkową komunikację, umożliwiająca przedsiębiorstwom użyteczności publicznej nie tylko śledzenie zużycia energii elektrycznej przez konsumentów, ale również informowanie konsumentów o najnowszych cenach energii elektrycznej, dzięki czemu odbiorca sam może decydować o swojej konsumpcji energii elektrycznej w czasie rzeczywistym.
Jednym z możliwych rozwiązań umożliwiających uruchomienie tych funkcji w AMI jest wdrożenie statycznej, bezprzewodowej sieci kratowej z wieloma przeskokami, która łączy bardzo dużą liczbę (setki lub nawet tysiące) liczników elektrycznych z bramą, która z kolei jest połączona z centrum nadzoru, gdzie ma miejsce koordynacja wszystkich wyżej wymienionych systemów zarządzania. Chociaż węzły liczników w sieci AMI są nieruchome, jakość łączy bezprzewodowych między dowolną parą mierników jest ogólnie niestabilna i zmienia się wraz z upływem czasu z powodu zakłóceń sygnału. Dlatego, aby spełnić wysokie wymagania AMI dotyczące niezawodności i niskich opóźnień, protokół routingu dla sieci AMI musi mieć zdolność radzenia sobie z częstymi zmianami stanu łącza, zapewniając szybkie i skuteczne metody ponownego obliczania ścieżki routingu, a także w tym samym czasie może tylko spowodować umiarkowane zwiększenie ogólnych kroków wykonania danego protokołu.
Bezpośrednią konsekwencją ewolucji SEE z sieci konwencjonalnych do sieci inteligentnych jest rosnąca podatność SEE na zagrożenia i ryzyko związane z atakami cybernetycznymi na jego funkcjonowanie. Osoba atakująca może, na przykład, wykonać zdalnie złośliwe działania bez fizycznego dostępu do systemu. Ponieważ zakłócanie normalnego działania SEE i systemu telekomunikacyjno-informatycznego jemu towarzyszącego może zakończyć się ogromnymi skutkami finansowymi z jednej strony, a poważnymi skutkami związanymi z bezpieczeństwem systemu, konieczne jest opracowanie skutecznych środków zaradczych na cyberataki. Praktyczną implementację (z pewnymi modyfikacjami) protokołu routingu IPv6 dla sieci o niskiej mocy i stratnych sieciach (ang. *Low Power and Lossy Networks* - RPL) [3]

przedstawiono w artykule [4]. Celem tej operacji jest zapewnienie niezawodnego i niskiego opóźnienia w zakresie routingu dla sieci AMI o dużej skali w sieciach inteligentnych. Błyskawicznemu wzrostowi zastosowań infrastruktury AMI towarzyszą poważne obawy związane z bezpieczeństwem, dotyczące potencjalnych słabości wprowadzanych nowych technologii. Obawy te zostały podsycane przez ostatnie doniesienia prasowe na temat luk w zabezpieczeniach, które można znaleźć w wielu urządzeniach pomiarowych [5][6].

Obecność elementów sieci inteligentnej w domostwach daje potencjalnym cybernapastnikom łatwy dostęp do niektórych elementów SEE. Inteligentna sieć będzie narażona na szeroki zakres zagrożeń bezpieczeństwa [7], której ogromna skala sprawia, że prawie niemożliwe jest zagwarantowanie bezpieczeństwa każdej części tego systemu. Co więcej, jak wcześniej napisano, inteligentna sieć będzie nie tylko rozległa, ale także bardzo złożona. Musi łączyć różne systemy i sieci, od jednostek wytwórczych i sprzętu sieci dystrybucyjnej poprzez inteligentne punkty końcowe i sieci usług komunikacyjnych, które prawdopodobnie są deregulowane i są własnością różnych podmiotów. Można zatem się spodziewać, że różnorodność i złożoność elementów inteligentnej sieci może, oprócz znanych słabości już występujących w systemach połączonych i niezależnych mikrosystemach [8], wprowadzić kolejne, nowe słabości. Autorzy [9] proponują połączyć teorię systemów i bezpieczeństwa cybernetycznego, aby ostatecznie zbudować naukę o bezpieczeństwie cyber-fizycznym.

Aby sprostać wyzwaniu związanemu z budowaniem bezpiecznego AMI, Narodowy Instytut Standardów i Technologii (ang. *National Institute for Standards and Technology* - NIST) oraz grupy użytkowników, takie jak Open Smart Grid [13], opracowały raporty i przedstawiły wymagania, dzięki czemu specjaliści i decydenci polityczni mają możliwość uwzględnienia bezpieczeństwa od samego początku procesu rozwoju. Dokumenty te obejmują zakres od oceny ryzyka [14] po wymogi bezpieczeństwa [15] i uzupełniane są dodatkowymi zasobami, takimi jak publikacje badań naukowych [10]-[12] i metody testowania ataków [16].

W artykule [17] przedstawiono aspekt wykrywania możliwych ataków na infrastrukturę, zwłaszcza w monitorowaniu różnych sieci komunikacyjnych AMI. Wg autorów podstawowym celem jest precyzyjne określenie wymagań wobec wydajnego i kompletnego systemu wykrywania włamań do sieci i hosta. Aby określić cel operacji i konieczne kroki na jego osiągnięcie należy, wg autorów, odpowiedzieć na kilka podstawowych pytań:

- Jaki jest model zagrożenia dla AMI i jak ataki mogą manifestować się w różnych sieciach komunikacyjnych?
- Które komponenty muszą być monitorowane i na jakiej warstwie stosu protokołu?
- Jakie są wyjątkowe ograniczenia AMI, jaką technologię wykrywania należy zastosować i jaką architekturę monitorowania należy wdrożyć?

Ci sami autorzy w kolejnym artykule [18] przedstawili takie stanowisko, że tradycyjne rozwiązania IT oparte na standardowych technologiach wykrywania nadużyć lub anomalii nie są odpowiednie, ponieważ cierpią z powodu niedociągnięć, które są niezgodne z ograniczeniami i wymogami monitorowania AMI. Na przykład brak informacji o bieżących atakach na AMI oraz potrzeba wykrywania nieznanych ataków uniemożliwia korzystanie z rozwiązań opartych na sygnaturach. Z drugiej strony potrzeba szybkiego zrozumienia podstawowych przyczyn ataków i konieczności wykrywania ukrytych zagrożeń ogranicza stosowanie rozwiązań opartych na wykrywaniu anomalii. Autorzy [18] uważają, że należy wprowadzić czujnik wykrywania włamań oparty na specyfikacji, aby dokładnie monitorować ruch w sąsiedztwie sieci AMI. Poleganie na specyfikacjach zamiast na sygnaturach ataków lub profilach statystycznych pozwala wykrywać nieznane zagrożenia, a umożliwia jednocześnie zdobywanie szczegółowych informacji o wykrytych, szkodliwych próbach włamania się do systemu. Niestety technologie wykrywania prób włamania oparte na specyfikacji mają dwa dotkliwe i istotne ograniczenia. Po pierwsze, opracowanie specyfikacji jest procesem kosztownym i żmudnym. Po drugie, specyfikacje są często bardzo trudne do oceny i

weryfikacji. Ścisła kontrola protokołów komunikacyjnych dopuszczonych w AMI oraz jednorodne zachowanie liczników i ruch liczników znacznie zmniejszają skutki wystąpienia pierwszego problemu.

Autorzy [18] proponują następujący krok postępowania :

1. określenie zestawu specyfikacji bezpieczeństwa dla inteligentnych liczników i polityki bezpieczeństwa dla AMI, aby zapobiec zagrożeniu infrastrukturze SEE za pośrednictwem AMI;
2. opracowanie formalnego modelu standardowego protokołu C12.22, który jest protokołem warstwy aplikacji używanym w licznikach do wymiany danych i odbierania informacji nt. konfiguracji licznika;
3. Przeprowadzenie formalnej weryfikacji specyfikacji i operacji monitorowania w warstwie aplikacji, aby zagwarantować, że żaden niewykrywany atak nie naruszy polityki bezpieczeństwa;
4. Opis prototypowej implementacji, przetestowanej w emulowanym, ale realistycznym środowisku AMI.

Oprócz infrastruktury AMI, celem ataków cyberprzestępców mogą się stać również inne elementy SEE jak centrum nadzoru pracy SEE. Autorzy [19] przedstawili analityczną metodę oceny odporności centrum nadzoru SEE i powiązanych z nim systemów komputerowych na cyberataki. Autorzy przedstawili model drzewa ataku służącego jako podstawę do oceny odporności. Potencjalne scenariusze włamań mogą zostać określone przy różnych kombinacjach prób wejścia do systemu, naruszając zasady bezpieczeństwa. Niedozwolone wejście do systemu może pozwolić intruzowi na wykorzystanie możliwości sterowania SCADA do podejmowania niepożądanych działań, powodując poważne uszkodzenia w pracy SEE. W artykule [16] pokazano systematyczne procedury oceny wskaźników słabości SEE pod kątem cyberbezpieczeństwa. Autorzy przedstawili kompleksowe badanie cyberbezpieczeństwa infrastruktury krytycznej SEE. Zaproponowano kontrolę nadzorczą i ramy bezpieczeństwa danych zgromadzonych z następującymi czterema głównymi komponentami: 1) monitorowanie w czasie rzeczywistym; 2) wykrywanie anomalii; 3) analiza możliwych skutków ewentualnego ataku; oraz 4) strategie łagodzenia skutków ataku. Rozwiniętą wersję tego artykułu opublikowano w [20].

W artykule [21] przedstawiono wykorzystanie inteligentnej sieci w celu umożliwienia **koordynacji wielu źródeł mocy biernej** umieszczonych w systemie dystrybucyjnym w pobliżu użytkownika końcowego w celu uzyskania ogólnosystemowego układu regulacji napięć. Kładziono szczególny nacisk na zgodność metody regulacji mocy biernej z zawartością dokumentu normalizacyjnego X.800, określającego architekturę bezpieczeństwa modelu OSI [22] i usługi, zagwarantują bezpieczeństwo systemów i ich danych. Norma X.800 identyfikuje kilka kluczowych usług: poufność danych, uwierzytelnianie, integralność danych, kontrola dostępu, nieodrzucanie i dostępność.

Fakt, że systemy SCADA/EMS są teraz połączone i zintegrowane z systemami zewnętrznymi, stwarza nowe możliwości, ale i również zagrożenia [23]. **Te nowe kwestie zostały podkreślone w grupach roboczych CIGRÉ** JWG D2/B3/C2.01 "Bezpieczeństwo systemów informacyjnych i intranetowych w systemach elektroenergetycznych" [24] i D2.22 " Bezpieczeństwo informacji w systemach elektroenergetycznych" [25].

Istotnym osiągnięciem naukowym [26] jest **nowy algorytm wykrywania anomalii w stacji**, który może być wykorzystywany do systematycznego wydobywania złośliwych "śladów" ingerencji zewnętrznej do sieci komunikacji SEE. Autorzy określili współczynnik wpływu (ang. *impact factor*) służący do oceny, w jaki sposób przerwy w zasilaniu mogą wpłynąć na pracę SEE. Proponowana metoda wykrywania anomalii opiera się na systematycznym wydobywaniu śladów włamań, które można wywnioskować z wiarygodnej analizy zdarzeń w postaci włamań w sieci komputerowej stacji.

Kolejnym ciekawym artykułem jest opracowanie autorów [27], w którym proponują **nową architekturę, SGDIDS, której celem jest poprawa cyberbezpieczeństwa inteligentnej sieci** poprzez wykorzystanie hierarchicznego i rozproszonego systemu wykrywania włamań w bezprzewodowej sieci kratowej, a także znalezienie optymalnego routingu dla inteligentnej sieci komunikacyjnej. Bezpieczeństwo poprawia się poprzez klasyfikację danych włamań za pomocą algorytmów SVM i AIS.

Koncepcyjne, warstwowe ramy do ochrony automatyk SEE przed cyberatakami przedstawiono w artykule [28]. Artykuł jest dosyć szeroko znany i często cytowany. Wg autorów należy uwzględnić następujące czynniki: 1) zadbać o bezinwazyjną integrację nowych systemów z istniejącymi systemami; 2) opracować odpowiednią strukturę pod względem modularności, skalowalności, rozszerzalności i łatwości zarządzania; 3) zapewnić kompatybilność z "Mapą drogową dotyczącą polityki bezpieczeństwa systemów automatyki w sektorze energetycznym" [29] oraz architekturą przyszłej inteligentnej sieci [30]-[32].

W artykule [33] przedstawiono **podsumowanie słabych punktów i potencjalnych cyberataków na systemy komunikacji w sieciach inteligentnych** oraz główne wyzwania związane z bezpieczeństwem cybernetycznym w systemach komunikacji inteligentnych sieci. Analizuje również istniejące rozwiązania w zakresie bezpieczeństwa cybernetycznego w komunikacji inteligentnych sieci. Artykuł [34] został opracowany w podobnym duchu jak [33], gdyż omawia zagadnienia związane z doborem odpowiednich komponentów systemu i związanych z nimi zagrożeń cybernetycznych, przy wdrażaniu inteligentnych sieci.

Jeden z najbardziej dotkliwych ataków w skali globalnej jest atak nazywany „sfałszowaną redystrybucją obciążeń (ang. *Load Redistribution* - LR) [35]. Jest to **specjalnego rodzaju atak polegający na wstrzyknięciu fałszywych danych o rozdziale obciążeń w SEE**. Skutki ataków LR na działanie systemu elektroenergetycznego może objawiać się natychmiastowo lub z opóźnieniem. Autorzy [35] udowodnili, że najbardziej szkodliwy atak można zidentyfikować za pomocą modelu optymalizacyjnego max-min typu napastnik-obrońca. Z minimalnym wysiłkiem obliczeniowym można wykorzystać rozkład Bendera do rozwiązania problemu bezpośredniego ataku LR. Skuteczność tej metody została potwierdzona przez rozwiązanie zagadnienia opartego na metodzie Karush-Kuhn-Tucker (KKT), opisanego we wcześniejszej pracy w/w autorów [36].

Udział dostawców usług informatycznych i telekomunikacyjnych w procesie wymiany danych SEE wprowadza nowy zestaw zagrożeń bezpieczeństwa dla inteligentnej sieci [37]. Wg autorów należy najpierw zidentyfikować wyzwania dotyczące bezpieczeństwa cybernetycznego w zakresie świadczenia usług telekomunikacyjnych w inteligentnej sieci. Autorzy kładli nacisk na dwa główne problemy bezpieczeństwa związane ze świadczeniem usług i potencjalne rozwiązania. Pierwszym z nich jest **utworzenie bezpiecznej procedury komunikacji między dostawcą energii elektrycznej, konsumentami i usługodawcami**. Drugim problemem jest **określenie poziomu zachowania prywatnośc**i, ale związanego z określeniem odpowiedzialnej struktury uwierzytelniania wśród jednostek inteligentnych, bez polegania na zaufanej stronie trzeciej.

Z tego przeglądu literatury widać jak istotne jest zagadnienie bezpieczeństwa cyfrowego systemu elektroenergetycznego połączone ze złożoną strukturą przyszłych sieci elektroenergetycznych. Jest to zagadnienie, którym się interesuje wiele ośrodków badawczych na Świecie.

Podsumowując ten punkt należy stwierdzić, że prowadzenie przez Pana mgra inż. **Roberta Czechowskiego prac w obszarze badawczym omówionym powyżej, należy uznać za celowe**.

5. Teza rozprawy

Autor w rozprawie postawił następujące tezy:

"*uwzględnienie nowoczesnych metod bezpieczeństwa cybernetycznego w procesie projektowania i eksploatacji układ w teleinformatyki i automatyki elektroenergetycznej, ograniczy skutki zamierzonych i przypadkowych ataków na obiekty elektroenergetyczne i przyczyni się do zwiększenia bezpieczeństwa pracy systemu elektroenergetycznego. W pracy rozwijana jest koncepcja realizacji tego zadania w oparciu o następujące przesłanki: 1 rozwój inteligentnych sieci elektroenergetycznych dzięki coraz to większej integracji z systemami ICT przyczynia się do sprawniejszego zarządzania tymi sieciami, ale zwiększa podatność tych sieci na ataki, 2 wdrożenie i stosowanie polityki bezpieczeństwa jest najważniejszym elementem w planowaniu strategii bezpieczeństwa dedykowanej systemom elektroenergetycznym, 3 stosowanie indywidualnych i nieszablonowych rozwiązań bezpieczeństwa opartych na technice cyfrowej (certy kowanych i opartych na otwartych protokołach), zapewnia najwyższy możliwy do osiągnięcia poziom bezpieczeństwa systemu. Przedstawione powyżej tezy, jednoznacznie określają opisane w rozprawie zagadnienie cyberbezpieczeństwa. Na uwagę należy jednak zwrócić, że stosowanie zbyt skomplikowanych mechanizm w zabezpieczeń, powoduje z czasem, że osoby sprawujące nad nimi nadzór same zaczynają je w pewien sposób omijać, co często prowadzi do powstawania luk w polityce bezpieczeństwa (teza 4)*". (str. 12-13 pracy)

W pracy Autor konsekwentnie dąży do udowodnienia tez posługując się metodami analitycznymi, symulacji komputerowej oraz badaniami eksperymentalnymi na modelach laboratoryjnych, jako sposobem weryfikacji wyników.

W celu udowodnienia tak postawionych tez, autor wybrał następujący układ rozdziałów pracy:

- W rozdziale 1: autor omawia kwestie bezpieczeństwa cyfrowego systemu elektroenergetycznego, zasady projektowania i jego eksploatacji. W tym rozdziale zawarto również opis pewnych elementów związanych z składowymi inteligentnej automatyki kontrolno-pomiarowej. Rozdział zawiera również informacje nt. procedury, jaką należy rozpocząć w przypadku wystąpienia cyberzagrożenia, począwszy od rozwiązania na poziomie organizacyjnym, czyli uświadomienia personelu danego operatora podmiotu energetycznego o odpowiedzialności, a skończywszy na „*wdrożeniu dokumentów określających w sprecyzowany i jasny sposób zasady postępowania*".
- Modele poszczególnych logicznych obszarów funkcjonowania sieci, zależności i funkcje wszystkich aktorów (uczestników), konstrukcja sieci inteligentnych z punktu widzenia ich logicznej struktury wraz z uwzględnieniem ich podziału na role oraz funkcje w systemie są omawiane w rozdziale 2. Autor przedstawia również poszczególne elementy sieci inteligentnych, którymi są: „*sieci przesyłowe, dystrybucyjne oraz sieci niskiego napięcia nie zapominając o systemach mikro-generacji, magazynowania energii i inteligentnych instalacjach domowych zintegrowanych z systemem operatora*". Na końcu tego rozdziału autor omawia „*zależności interfejsów i kanałów komunikacyjnych stanowiących o: roli, priorytecie i wymaganym czasie odpowiedzi poszczególnych elementów, koniecznych do efektywnego zarządzania rozległymi systemami elektroenergetycznymi*".
- Kolejny rozdział 3 jest poświęcony modelom, którymi doktorant się posługiwał do osiągnięcia celów doktoratu. W zależności od przeprowadzonych badań, korzystano z różnego stopnia skomplikowania modeli sieci, „*o różnym obszarze funkcjonowania w infrastrukturze inteligentnych sieci elektroenergetycznych*". W tym rozdziale zawarto również „*opis stanowisk laboratoryjnych, procedurę testową, symulacje oraz wyniki*

badań następujących modeli: modele sieci rzeczywistej inteligentnego opomiarowania". Opracowane modele, zgodnie z opisem przedstawionym przez autora rozprawy, służą do „*oceny bezpieczeństwa i zagrożeń oraz ich skutków dla poszczególnych rodzajów badanych zakłóceń i celowych ataków*" z jednej strony, a z drugiej strony do „*przeprowadzenia analizy dla bardzo dużej liczby wariantów scenariuszy awarii systemu oraz analizy działań zmierzających do samoczynnego i automatycznego przywrócenia do funkcjonowania sieci nie objętej awarią*".

- Kompleksową analizę poszczególnych rodzajów ataków na systemy informatyczno-telekomunikacyjne SEE, w tym: zagadnienia szacowania ryzyka, proces analizy i oceny prawdopodobnego wystąpienia zagrożeń, przedstawiono w rozdziale 4. Autor omawia również „*konsekwencje różnych scenariuszy ataku, uwzględniając atak na pojedynczy obiekt składowy, systemu jak i ataki związane ze zmianą nastawień układów automatyki i zabezpieczeń*". Autor przedstawia praktycznie wszystkie możliwe formy ataków począwszy od „*ataków na sieć szkieletową, teleinformatyczne centrum operatora*", a skończywszy na „*atakach w sieci niskiego napięcia*".
- Rozdział 5 jest z kolei poświęcony „*aktualnym zagadnieniom i problemom spotykanym przy projektowaniu inteligentnych sieci elektroenergetycznych*". Autor przedstawia również : „*rozwiązania i metody mogące pomóc w zwiększeniu bezpieczeństwa sieci inteligentnych*", „*najczęściej spotykane problemy występujące w modernizacji istniejących i projektowaniu nowych sieci elektroenergetycznych wykorzystujących układy automatyki cyfrowej i rozwiązania telekomunikacyjne, opartych o technologię IT*".
- Całość zamyka rozdział poświęcony wnioskom, podsumowaniu oraz załączniki.

Tezy sformułowane przez autora można moim zdaniem uznać za **oryginalne i w pełni udowodnione**. Autor zajmował się szczególnie trudnym zagadnieniem, w tym:

- identyfikacja potencjalnie wrażliwych , tzn. podatnych na ataki, elementów sieci, także samą analizę wzorców ataku,
- opracowanie wytycznych i strategii, oraz przeprowadzenie ich praktycznej implementacji, której celem jest zwiększenie niezawodności działania i bezpieczeństwa konwencjonalnych sieci energetycznych i nowo utworzonych sieci inteligentnych,
- zastosowanie teleinformatycznych środków ochrony w rozległym systemie elektroenergetycznym celem poprawienia ich efektywności i niezawodności.

W tym celu Autor opracował odpowiednie modele sieci inteligentnych wraz z ich elementami składowymi oraz przetestował. Tymi modelami są:

1. Model nr 1 rzeczywisty Smart Metering BPL[1] (1),
2. Model nr 2 rzeczywisty Smart Metering PLC[2] (2),
3. Model nr 3 rzeczywisty Smart Metering PLC[3] (3),
4. Model nr 4 sieci dystrybucyjnej opartej o technologie ICT (4).

[1] bez separacji sieci od zakłóceń zewnętrznych
[2] bez separacji sieci od zakłóceń zewnętrznych instalacja w budynku
[3] bez separacji sieci od zakłóceń zewnętrznych instalacja sieci miejskiej

Wszystkie modele przedstawione i zbadane w ramach tej pracy umożliwiają coraz to dokładniejsze poznanie mechanizmów ich funkcjonowania transmisji i związanej z komunikacją kwestii bezpieczeństwa cyfrowego.

Jest to niebagatelne osiągnięcie naukowo-badawcze, gdyż na podstawie ww. literatury widać wyraźnie, że zagadnienie jest aktualne, a rozwiązanie zaproponowane przez autora jest ważnym osiągnięciem w tej dziedzinie.

3. Waga podjętego zagadnienia naukowego

W moim odczuciu **rozprawa uzupełnia aktualny stan wiedzy,** pokazując w jaki sposób można szczegółowo zbadać wpływ włamań cybernetycznych na pracę SEE.

- Model nr 1 przedstawiony w rozprawie umożliwia zaobserwowanie utraty i prób ponownego nawiązywania połączenia przez liczniki energii elektrycznej wyposażonych w moduły komunikacyjne.
- Model nr 2 odzwierciedla problem dynamicznej zmiany topologii sieci z uwzględnieniem funkcji urządzeń stanowiącej o ich hierarchii w sieci.
- Model określony jako trzeci umożliwia określenie wpływu najczęściej spotykanych zakłóceń na komunikację cyfrową w sieci rzeczywistej.
- Model ostatni, czwarty służy do analizy cyberbezpieczeństwa. Ten model odzwierciedlał rzeczywistą infrastrukturę teleinformatyczną.

Znaczenie rozprawy dla nauki można określić na podstawie następujących umiejętności, które doktorant zademonstrował w tej pracy:

- umiejętność obserwacji badanego modelu celem sklasyfikowania poszczególnych zakłóceń i ich wpływu na pogorszenie warunków zapewniających komunikację,
- umiejętność sformułowania i zamodelowania problemu dynamicznej zmiany topologii sieci z uwzględnieniem funkcji urządzeń stanowiącej o ich hierarchii w sieci,
- umiejętność sformułowania i zamodelowania oraz określenia wpływu najczęściej spotykanych zakłóceń na komunikację cyfrową w sieci rzeczywistej,
- umiejętność pokazywania w jaki sposób komponenty teleinformatyczne wzajemnie na siebie oddziaływają, oraz w jakim stopniu ich relacje mają wpływ na poziom cyberbezpieczeństwa i skalę potencjalnie możliwej penetracji sieci przez atakującego.

Do cennego dorobku autora można również zaliczyć opracowanie kilku uzupełniających się modeli, pozwalających na systematyczne ujęcie zagadnienia cyberbezpieczeństwa i jego znaczenia dla normalnej pracy SEE.

4. Warsztat naukowy

Autor rozprawy wykazuje dobrą orientację w obszarze zagadnień telekomunikacyjno-informatycznych. Recenzowana praca ma charakter analityczno-eksperymentalny. Duża staranność przy opracowaniu modeli do badań świadczy o **dogłębnym zrozumieniu także od strony modelowania zjawisk zagadnień z przedstawionego obszaru badawczego**. Należy wyrazić opinię, że recenzowana praca stanowi cenny dorobek naukowy w tym obszarze, jest jak najbardziej aktualnym ujęciem prezentowanej tematyki, zawiera wiele oryginalnych treści, sformułowań i wartościowych wyników, co tylko potwierdza dobre przygotowanie doktoranta do samodzielnego prowadzenia w przyszłości prac naukowych i badawczych.

Pan mgr inż. **Robert Czechowski** zajmuje się tym obszarem badawczym od wielu lat, uczestniczył w projekcie międzynarodowym ERA-NET, o czym świadczą jego liczne autorskie i współautorskie publikacje w kraju i za granicą.

5. Oryginalne osiągnięcia

Do elementów nowości, stanowiących oryginalne i najważniejsze rezultaty rozprawy i osiągnięcia jej autora, zaliczam następujące:

- zbudowanie modelu celem sklasyfikowania poszczególnych zakłóceń i ich wpływu na pogorszenie warunków zapewniających komunikację,
- sformułowanie i zamodelowanie problemu dynamicznej zmiany topologii sieci z uwzględnieniem funkcji urządzeń stanowiącej o ich hierarchii w sieci,
- sformułowanie i zamodelowanie oraz określenie wpływu najczęściej spotykanych zakłóceń na komunikację cyfrową w sieci rzeczywistej,
- pokazywanie w jaki sposób komponenty teleinformatyczne wzajemnie na siebie oddziaływają, oraz w jakim stopniu ich relacje mają wpływ na poziom cyberbezpieczeństwa i skalę potencjalnie możliwej penetracji sieci przez atakującego.

6. Uwagi polemiczne, dyskusyjne i redakcyjne

6.1. Uwagi o charakterze ogólnym

Po przeczytaniu rozprawy doktorskiej nasunęły mi się uwagi krytyczne, które powinny być przedmiotem dyskusji w czasie obrony pracy doktorskiej tj.:

1. Str. 68. Pan stwierdza, że „*Jeśli budowę systemu automatycznej kontroli i nadzoru powierzy się całkowicie zewnętrznym firmom informatycznym, to efekt będzie taki, że automatyzacja będzie realizowana, jednak nikt się nie będzie na tych sieciach i systemach elektroenergetycznych znał całkowicie, ani elektrycy ani informatycy.*" Jest to dosyć śmiała teza. Proszę wyjaśnić. Wszystko wg. mnie zależy od dokładności dokumentacji technicznej. Bardziej ryzykowne stwierdzenie jest to, że *strona trzecia zna szczegóły*, ale jak Pan wcześniej napisał najwięcej zagrożeń może pochodzić od wewnątrz, czyli od ludzi pracujących w firmie i znający ją, a nie od zewnątrz.
2. Str. 85. „*W wyniku obserwacji wskazań aplikacji dostawcy B i C nie stwierdzono sygnalizacji przerw w komunikacji pomiędzy licznikami a koncentratorem danych, co zgodnie z przyjętym kryteriami oznacza, że nie zanotowano przerw w komunikacji koncentrator licznik w żadnym przypadku.*"
   A dalej doktorant pisze: „*Jak wynika z przebieg w, napięcia w układzie zasilania fazy L2 i L3 nie są symetryczne i są znacznie odkształcone od przebieg w sinusoidalnych które można zaobserwować w przypadku fazy L1 (podobnie jak w poprzednim etapie).*" Jak to wytłumaczyć? Jak częstotliwość jest znacznie poniżej częstotliwości nominalnej, a na dodatek parametry elektryczne są zniekształcone, dopiero wtedy otrzymuje się dobrą komunikację urządzeń?? Proszę o wyjaśnienie.
3. Str. 86. W tym etapie (1) Załączone są źródła światła: żarowe, LED, świetlówki kompaktowe i lampa biurkowa o mocy 40W ze sterowaniem dotykowym; czas obserwacji 1 godzina. Zaobserwowano, że „*napięcia w układzie zasilania fazy L1, L2 i L3 nie są zniekształcone i można przyjąć, że są symetryczne i nie odbiegają od przebieg w sinusoidalnych. Przebieg prądowy dla fazy L1 jest natomiast mocno odkształcony.*" Podobnie jak w poprzednim przypadku - jak to wytłumaczyć? Jeden z prądów jest mocno zniekształcony,

dopiero też wtedy otrzymuje się dobrą komunikację urządzeń?? Proszę o wyjaśnienie.

4. Uważam, że ta praca dotyczy tylko częściowo bezpieczeństwa elektronicznego. W dużej mierze więcej uwagi poświęcono modelom wykorzystywanym w zagadnieniach związanych z określeniem stanu włączenia lub wyłączenia urządzeń elektrycznych (ang. *Non-Intrusive Load Monitoring Systems*), które są jednym z głównych problemów inteligentnych systemów pomiarowych (literatura [38]-[40]).

6.2. Uwagi szczegółowe i redakcyjne

Praca doktorska liczy łącznie 252 strony. Spis literatury zawiera 120 pozycji podzielonych na ogólne pozycje, ustawy i zarządzenia, raporty oraz literaturę internetową, przy czym doktorant ma w sumie 13 własnych autorskich i współautorskich pozycji w ogólnych pozycjach i jedną pozycję w części „Raporty".

1. Doktorant pisze o pięciu modelach, natomiast, ja zauważyłem cztery.

1. Na stronie 49 doktorant pisze: „*Analiza przepływu mocy opiera się na nich i stanowi popularna metoda oceny dystrybucji zasilania i poziomów napięcia w sieci*." Rozumiem, że chodzi o obliczenie rozpływów mocy i różnorakie regulacje?
   Oraz
   „*Nowoczesne zarządzanie siecią elektroenergetyczną zakłada użycie infrastruktury teleinformatycznej, która sama polega na odpowiednim źródle zasilania."* Skąd to zasilanie? Nie z sieci? Jakieś baterie?

2. Str. 50. Nie rozumiem tego zdania „*Sieć elektroenergetyczna oznacza obecny stan systemu ewoluującego w Smart Grid*". Potem jest stwierdzenie „*Symulacja układów elektrycznych jest w inżynierii tradycyjną dyscypliną, która nakreślą różnicę między dynamiczną i statyczną analizą systemu elektroenergetycznego*." Tylko nie wiem dlaczego ten kawałek jest w „*przypływie płatności*"?

3. Na str. 34 napisano „*Jak pokazują doświadczenia, nawet bardzo dobrze zabezpieczone systemy (np. bankowe które za sprawą swej specyfiki, uchodzą za najlepiej zabezpieczone), nie są systemami których nie można przełamać. Stosowanie jakichkolwiek zabezpieczeń jest zdecydowanie lepsze, od niezastosowania ich w ogóle, gdyż nawet jeżeli nie uniemożliwią, to przynajmniej w znacznym stopniu utrudnią i ograniczą nieautoryzowany dostąp do inteligentnej sieci osobom nieupoważnionym ze średnią wiedzą i umiejętnościami. Warto zwrócić uwagę, że nawet słabe zabezpieczenia w znacznym stopniu uniemożliwiają przeprowadzenie skutecznego ataku osobom, które takiego dostępu nie powinny mieć w ogóle.*"
   Potem we wprowadzeniu do rozdziału 3 znowu „*Doświadczenia z sektora IT pokazują, że nawet bardzo dobrze zabezpieczone systemy, jak systemy bankowe które za sprawą swej specyfiki uchodzą za najlepiej zabezpieczone nie są systemami, których nie można przełamać. Słuszne jest też przeświadczenie, że stosowanie jakichkolwiek zabezpieczeń jest zdecydowanie lepsze, niż nie stosowanie ich w ogóle. Zastosowane zabezpieczenia, nawet jeśli nie uniemożliwią, to przynajmniej w znacznym stopniu utrudnią i ograniczą nieautoryzowany dostęp do inteligentnej sieci osobom nieupoważnionym, ze średnią wiedzą i umiejętnościami. Warto zwrócić uwagę, że nawet słabe zabezpieczenia przyczynią się w znacznym stopniu do utrudnienia przeprowadzenia skutecznego ataku osobom, które nie powinny mieć dostępu do informacji zgromadzonych w systemie.*"
   Trochę się różnią te dwa kawałki tekstu, niemniej mówią o tym samym??

4. Str. 67. Pisanie czegoś w rodzaju „*Obecnie spotykane oprogramowanie przeznaczone do symulacji inteligentnych sieci i system w elektroenergetycznych tylko w części realizuje poszczególne obszary ochrony cyfrowej. Dowodzą tego liczne publikacje, na przykład: [33], [17], [53].*” może doprowadzić do pewnej frustracji. Powinno się podać przynajmniej krótki opis tego, co czytelnik powinien wiedzieć o treści tych artykułów i co ma wspólnego z myślą przewodnią, którym jest sformułowanie „*spotykane oprogramowanie przeznaczone do symulacji inteligentnych sieci i system w elektroenergetycznych tylko w części realizuje poszczególne obszary ochrony cyfrowej*”, zwłaszcza, że dalej autor pisze „*Ponieważ zakres badań przedstawionych w temacie jest szeroki, trudno jest określić, czy funkcje danego symulatora zrealizują wybrane cele analizy danego segmentu systemu i sieci inteligentnej. W związku z powyższym, analiza algorytm w i technik bezpieczeństwa cyfrowych układ w kontrolno/pomiarowych i urządzeń metrologicznych* ***może być realizowana jedynie w obrębie danego obszaru.***” No i tutaj powstaje pytanie Co to jest to słynne „realizowanie tylko jedynie w obrębie danego obszaru.”?
5. Str. 73. „*Natężenie występowania tych zjawisk jest proporcjonalne do mocy lamp zainstalowanych w danej sieci oświetleniowej, jednak przede wszystkim, zależy ono od stopnia odkształcenia prądu. Kolejnym przeprowadzonym testem był test z wykorzystaniem urządzenia o dużym zapotrzebowaniu na moc, przekształcającego energię elektryczną na cieplną. Wyniki badań testowanego modelu można znaleźć również w artykułach [21][43].*” Ale nie ma tutaj informacji nt. tego (1) gdzie wcześniej można znaleźć wyniki tych badań?? (2) zmuszenie recenzenta do poszukiwania tych artykułów, celem komentowania wyników znajdujących się w pracy jest co najmniej niestosowne. Można byłoby chociaż dołączyć artykuły jako załączniki do tego maila, który doktorant do mnie wysłał.
6. Str. 73. „*Urządzeniami, które w największym stopniu wpływają na komunikację PLC, to urządzenia zasilane poprzez przekształtniki: prostowniki, falowniki, przemienniki częstotliwości.*” Nie jest to nic odkrywczego. Urządzenia te generują bardzo dużo różnych, wyższych harmonicznych. Każdy energetyk dobrze o tym wie.
7. Str. 74. Rys. 3.4. Bardzo słaba legenda rysunku. Opis znajdujący się w poprzednim akapicie (Model rzeczywisty Smart Metering PLC (model nr 2)) ani razu nie odnosi się do któregokolwiek elementu znajdującego się na rysunku (K1..K3, 3k, 4k itp). Gorzej – w tabeli odnoszącej się do Rys. 3.4 (tak przypuszczam, bo o powiązaniu też nie ma ani słowa) są zupełnie inne symbole (7P-716). Brak również komentarzy tych nowych symboli.
8. Str. 78. Tab. 3.3. „*Dla przykładu, ruch w testowanej sieci PLC dla 10 licznik w i trzech koncentratorów w okresie jednego miesiąca wynosi ok. 65-70 tyś.*” Rozumiem, że to jest suma poszczególnych pozycji w kolumnie „Liczba zdarzeń”? bo komentarz bardzo trudno powiązać z poszczególnymi rubrykami tabeli 3.3.
9. Str. 78. Bardzo trudno się śledzi ten opis tabeli. Np. napisał pan „*W przypadku licznika 3p-313 można stwierdzić, że praktycznie pracował on w trybie terminala (nie uwzględniając 2 zdarzeń, w których pełnił rolę switch'a) a*” . Ja tam widzę 6 zdarzeń!!
10. Str. 78-79. „*Głównym powodem, dla którego zdecydowano się przedstawić procedurę testową jest chęć pokazania, że testy braku dostępności urządzeń pod wpływem zakłóceń, należy odróżnić od analizy zakłóceń w dynamicznie zmieniającej się trasie sieci PLC to dwa zupełnie odmienne zagadnienia.*” Zastanawiałem się, gdzie w całym tym wywodzie i opisie można znaleźć potwierdzenie tego stwierdzenia, ale niestety

nie znalazłem ☹ . To samo dotyczy stwierdzenia „*Oprócz przedstawionych powyżej wniosków z przeprowadzonych badań, można stwierdzić, że istnieje ścisły związek pomiędzy kształtowaniem się sieci złożonych (ang. Complex Networks), a wewnętrznym mechanizmem działania i zachowania systemu elektroenergetycznego.*”

11. Str. 78. Tutaj również jest stwierdzenie „*Przedmiotowy model sieci może służyć do symulacji zachowania systemu w trakcie normalnej jego pracy, jak również może stanowić bezcenne źródło informacji nt. zachowania systemu na skutek zaistnienia awarii systemowej, bądź celowego ataku na system osób trzecich. Model symulacyjny może również ukazać charakterystykę sieci złożonej w przypadku nagłego wzrostu lub spadku napięcia oraz może być inspiracją do wdrażania nowych pomysł w przyczyniających się do zwiększenia bezpieczeństwa i stabilności całego systemu elektroenergetycznego*”. Czy chodzi o to, że przeprowadzone ataki lub sytuacje awaryjne będą miały podobne skutki jak te zdarzenia przez Pana symulowane i opisane w tym rozdziale? Bo o tym nie ma tu mowy?
12. Str. 79. Kolejne stwierdzenie „*Model symulacyjny może również ukazać charakterystykę sieci złożonej w przypadku nagłego wzrostu lub spadku napięcia oraz może być inspiracją do wdrażania nowych pomysł w przyczyniających się do zwiększenia bezpieczeństwa i stabilności całego systemu elektroenergetycznego*”. Na podstawie przeprowadzonych badań nie widzę przesłanek do takich stwierdzeń.
13. Str. 80 „*Eksperyment porównawczy właściwości komunikacyjnych licznik w inteligentnych był realizowany w ramach cyklicznej konferencji dotyczącej AMI jednego z dostawców energii elektrycznej.*” Na razie wszystko jest OK. Potem jest napisane „*Procedura badawcza została rozpoczęta w grudniu 2015 r. i została zakończona w lutym 2016 r.*”. To wszystko w ramach JEDNEJ, cyklicznej konferencji, rozciągającej się w czasie ???
14. Str. 82. Pan napisał „Przedstawione w rozprawie analizy i wyniki badań Modelu nr 3 zostały przedstawione dla poszczególnych etapów opisanych w Procedurze testowej (4)” Ale gdzie to jest ?
    Jest straszny problem z oznaczeniami:
    Str. „*W przypadku liczników producenta D zaobserwowano wskaźnik skuteczności transmisji poniżej 95% a dodatkowo stwierdzono sygnalizacji braku komunikacji pomiędzy koncentratorem a licznikiem jednofazowym zainstalowanym najdalej od koncentratora (złącze ZL4 przedstawione na Rys. 3.7).*”
    Po pierwsze, bardzo słabo opisany jest ten rysunek 3.7.
    - Są tam stosowane trzy symbole Tr – transformator??
    - Potem są oznaczenia liczników : A1-3F itp., czyli jak pan napisał to są symbole - oznaczenie producenta (A), numer kolejnego urządzenia (x), typ urządzenia liczba faz (yF). Ale potem już na rysunku tego nie widać. Tam są inne oznaczenia: Nie wiem czy te złącza ZL i Wh (prawdopodobnie licznik energii?? Watogodziny)???
    - Potem pan się odwołuje do symboli A, B, które raz oznaczają **sieci** „zmiana konfiguracji poprzez zamianę położenia dwóch wybranych liczników pomiędzy sieciami A i B,”, a raz są **przedziałami czasowymi** „w następujących przedziałach czasowych: A - 14-16 grudnia 2015 r., 07 stycznia i 16 lutego 2016 r., B - 22-26 stycznia 2016 r., C - 8-16 lutego 2016 r., D - 07-14 stycznia 2016 r. i 8 lutego 2016 r.”

- Potem jest mowa o **aplikacji** C i D???? Znowu inne znaczenia mają te duże litery. Pogmatwanie z poplątaniem !!!!

15. Str. 84. Jest takie stwierdzenie „*W przypadku liczników producenta D zaobserwowano wskaźnik skuteczności transmisji poniżej 95% a dodatkowo stwierdzono sygnalizacji braku komunikacji pomiędzy koncentratorem a licznikiem jednofazowym zainstalowanym najdalej od koncentratora (złącze ZL4 przedstawione na Rys. 3.7)*”, ale nie ma nigdzie wytłumaczenia co to spowodowało?? Tylko odległość??, bo przypuszczam, że pod kątem instalacji nie ma różnicy między ZL4 a pozostałymi złączami ZLx (x=1..3).
16. Jest takie stwierdzenie „*nie stwierdzono sygnalizacji przerw w komunikacji pomiędzy licznikami a koncentratorem danych, co zgodnie z przyjętym kryteriami oznacza, »e nie zanotowano przerw w komunikacji koncentrator licznik w żadnym przypadku. dodatkowo stwierdzono sygnalizacji braku komunikacji pomiędzy koncentratorem a licznikiem jednofazowym producenta D zainstalowanym najdalej od koncentratora.”.* Też nie ma próby wytłumaczenia skąd ten brak komunikacji ….
17. Str. 87. Jeżeli chodzi o Badanie nr 6 (Etap 4b – źródło światła : lampy sodowe), z opisu wyników badań wynika, że dosyć dużo jest zjawisk niekorzystnych, niemniej nie ma odniesienia do samych stosowanych źródeł (lampy sodowe i ich właściwości fizyczne), nie ma również próby interpretacji uzyskanych wyników. Jest oczywiście lakoniczne stwierdzenie „*Zarejestrowane w tym kroku badawczym przebiegi prąd w dość istotnie odbiegały od przebieg w sinusoidalnych. Zaburzenia generowane przez zastosowane odbiorniki mogły stanowić przyczynę zaistniałych przerw w komunikacji koncentrator liczniki.*” Jest to rozprawa doktorska. Nie może być tak, że uzyskuje się jakieś wyniki, a nie ma nawet próby interpretacji skąd to się wzięło.
18. Str. 88. Mam podobne uwagi jak i poprzednio: stwierdza doktorant „*Jak wynika z przebieg w napięcia pokazanych na rysunkach w Rozdziale 8 Załączniki 7.45, 7.46, 7.47, napięcia w układzie zasilania są odkształcone. Przebieg prądowy dla fazy L1 (Rys. 7.48) jest mocno odkształcony*.”
19. Str. 92-93. Słaby opis tabeli 3.15-3.16. Nie chce mi się już tego komentować …
20. Str.94. Stwierdza pan, że „*Jakość komunikacji oraz stabilność połączenia zależy od typu obciążenia sieci. Przy obciążeniu czysto rezydencyjnym nie zachodzą większe zakłócenia w pracy sieci, zaś w przypadku obciążenia sieci urządzeniami w których {brakuje tu przecinka} występuje komutacja prąd w np. inwertery i falowniki zawsze będzie dochodzić do zniekształceń przebieg w napięciowych wynikających z niestandardowych przebieg w prądów.*” Ale przy komentarzach poszczególnych przypadków nie widać opisu tych zjawisk.
21. Str. 94 Dalej „*Najczęstsze przyczyny błędów komunikacji mogą występować w przypadku obciążeń sieci urządzeniami wywołującymi nieregularne, odkształcone przebiegi prądów, a zwłaszcza przebiegi, w których występują krótkie czasy narastania i opadania prądów (impulsy prądowe typu szpilki).*” Czy do nich należy te ostatnie przypadki, w których występuje najwięcej błędów komunikacji? Proszę nawiązać do konkretnych wyników uzyskanych podczas badań!
22. Str. 94. Nie wiem dlaczego tutaj nagle się pojawia ten kawałek tekstu „*Termin zaburzenie elektromagnetyczne oznacza zjawisko elektromagnetyczne (przyczynę), które może powodować zakłócenie, czyli skutek w postaci*

degradacji funkcji pracy urządzenia. Zaburzeniami elektromagnetycznymi są wszelkie sygnały elektryczne wytwarzane:

- *bezpośrednio przez zmiany prąd w i napięć w przewodach zasilających, sygnałowych oraz łączących źródło emisji z otaczającym środowiskiem albo,*
- *pośrednio na skutek promieniowania elektromagnetycznego w wolnej przestrzeni przez pola bliskie (składowe elektryczne i magnetyczne) oraz dalekie (elektromagnetyczne) [103].*"
  Czy to ma coś wspólnego z wcześniej przeprowadzonych badań???

23. Dalej na stronie 95 jest taki tekst „*Zaburzenia powodowane emisją pożądaną eliminuje się racjonalną gospodarką widmem elektromagnetycznym przez odpowiedni przydział częstotliwości lub pasm roboczych. Natomiast zaburzenia wywołane emisją niepożądaną powinny mieć tak określone maksymalne poziomy transmisji, aby nie zakłócały pracy innych obiektów w miejscu ich zainstalowania.*" Również i w tym przypadku nie widzę powiązania tego tekstu z przeprowadzonymi badaniami i ich komentowanymi wynikami.
24. Str. 99-109. Cały temat „*Opis stanowiska laboratoryjnego (model nr 4)*" dla mnie wygląda na instrukcję obsługi programu, bo nawet rysunki 3.8-3.14 są bardzo słabo napisane, i tak na prawdę oprócz próby zrozumienia powiązań logicznych między poszczególnymi komponentami, nie bardzo wiadomo na koniec tego punktu, o co nam chodziło i co tutaj właściwie uzyskaliśmy. Proszę o szersze wyjaśnienie.
25. Str. 136. Stwierdzenie „*Zastosowanie technologii cyfrowych, znacznie poprawia wydajność systemu elektroenergetycznego, jednak może wiązać się z podatnością tego systemu na cyberataki. Obecnie szacuje się, że zagrożenia wynikające z nieautoryzowanej ingerencji w system teleinformatyczny i tym samym naruszenie cyberbezpieczeństwa, są znacznie większe niż te wynikające z fizycznego ataku.*"
  Lub jeszcze
  „*Nowy model sieci inteligentnej, za sprawą nowej architektury, wymagać będzie bardzo istotnych zmian w kwestii zarządzania systemem elektroenergetycznym*"
  O tym już wcześniej była mowa, a nawet kilkakrotnie …
26. Str. 128-141. Mnie się wydaje, że cały ten rozdział 4 „*Analiza ryzyka i ocena zagrożeń*"można było dać przed rozdziałami opisującymi testy (rozdział 3) . To są tylko tyko rozważania teoretyczne i opis ryzyk występujących w systemach elektroenergetycznych.
27. Str. 155-156 „*W systemie Linux można przypisać odpowiedni poziom krytyczny nice process by ten proces był dla systemu najważniejszy w wczas opóźnienie nie powinno przekraczać 50ms (pod warunkiem, że jądro systemu zostanie odpowiednio skompilowane tak zwanego czasu rzeczywistego). W przypadku systemu Windows, nie dostarcza on znacznik w czasu odbioru i wysyłania pakietów na poziomie gniazda sieciowego, bez czego nie ma mowy o jakiejkolwiek precyzji.*" Proszę doprecyzować to stwierdzenie.
28. Ogólnie, zarówno w podsumowaniach jak i wnioskach, rzadko kiedy autor nawiązuje do zawartości treści podsumowanej. Odnoszę wrażenie, że znowu wraca do części teoretycznej.

Praca zawiera 6 rozdziałów.

Zamieszczone w pracy rysunki są wykonane z należytą dbałością i są dostatecznie czytelne wraz z ich podpisami (z wyjątkiem niektórych).

Układ redakcyjny pracy pozostawia niestety wiele do życzenia, gdyż zawiera bardzo dużo błędów redakcyjnych. Zestawienie błędów został przekazany doktorantowi w oddzielnym pliku.

Zastosowanie środowiska programowego LATEX do edycji pracy doktorskiej świadczy o umiejętnościach Autora do profesjonalnego opracowywania większych i złożonych opracowań naukowych i technicznych.

Powyższe uwagi mają charakter dyskusyjny i nie umniejszają wartości naukowej oraz znaczenia praktycznego recenzowanej rozprawy. **Błędy redakcyjne obniżają w istotny sposób ocenę tej pracy (załączam większość z nich w ostatniej części tej recenzji).** Niemniej moja generalna ocena rozprawy jest pozytywna.

7. Wniosek końcowy

Recenzowana praca przedstawiona przez **mgr. inż. Roberta Czechowskiego** pt. „**Bezpieczeństwo Cyfrowe Inteligentnych Dystrybucyjnych Sieci Elektroenergetycznych**”, niezależnie od uwag podanych w niniejszej recenzji, stanowi poważny i samodzielny wkład doktoranta do obszaru badawczego dotyczącego bezpieczeństwa, zarówno fizycznego, jak i cybernetycznego sieci inteligentnych.
Autor wykonał kompleksowe badania teoretyczne oraz eksperymentalne, wykazał się umiejętnością formułowania i rozwiązywania trudnych i aktualnych problemów naukowych.

Autor wykazał się także umiejętnością pozyskiwania środków na badania (udział w międzynarodowym projekcie naukowym) i umiejętnością współpracy z naukowcami z renomowanych zagranicznych ośrodków naukowych, o czym świadczą jego współautorskie publikacje zagraniczne.

Uzyskane wyniki mają istotne znaczenie zarówno poznawcze jak i aplikacyjne, i mogą być wykorzystywane w dalszych pracach badawczych w dziedzinie rozwiązań informatyczno-telekomunikacyjnych w sieciach inteligentnych.

Biorąc powyższe pod uwagę **stwierdzam, że opiniowana rozprawa doktorska mgr. inż. Roberta Czechowskiego odpowiada wymaganiom sprecyzowanym w Ustawie z dnia 14 marca 2003 o stopniach naukowych i tytule naukowym oraz wytycznych Centralnej Komisji ds. Stopni i Tytule Naukowym. Wnoszę więc o dopuszczenie jej autora do publicznej obrony.**

8. Literatura

[1] R. Fischer, N. Schulz, and G. H. Anderson, Information Management For an Automated Meter Reading System, Proceedings of the 62nd American Power Conference, April 2000.

[2] S. Karnouskos, O. Terzidis and P. Karnouskos, An Advanced Metering Infrastructure for Future Energy Networks, IFIP/IEEE 1st International Conference on New Technologies, Mobility and Security, May 2007.
[3] T. Winter and P. Thubert, RPL: IPv6 Routing Protocol for Low Power and Lossy Networks, draft-ietf-roll-rpl-04.txt, October 2009.
[4] Di Wang; Zhifeng Tao; Jinyun Zhang; Alhussein A. Abouzeid, RPL Based Routing for Advanced Metering Infrastructure in Smart Grid, 2010 IEEE International Conference on Communications Workshops, Year: 2010, Pages: 1 – 6
[5] J. Wright (InGuardians), “Smart Meters Have Security Holes,” http://www.msnbc.msn.com/id/36055667,2010.
[6] “IOActive’s Mike Davis to Unveil Smart Grid Research at Black Hat USA,” IOActive press release, July 28, 2009, http://www.ioactive.com/news-events/DavisSmartGridBlackHatPR.php
[7] US-DOE, NERCH, High-Impact, Low-Frequency Event Risk to the North American Bulk Power System, Jun. 2010.

[8] NIST, Guidelines for Smart Grid Cyber Security, Draft NISTIR 7628, Jul. 2010.

[9] Yilin Mo; Tiffany Hyun-Jin Kim; Kenneth Brancik; Dona Dickinson; Heejo Lee; Adrian Perrig; Bruno Sinopoli, Cyber–Physical Security of a Smart Grid Infrastructure, Proceedings of the IEEE, Year: 2012, Volume: 100, Issue: 1, Pages: 195 – 209.
[10] T. Roosta, D. K. Nilsson, U. Lindqvist, and A. Valdes, "An Intrusion Detection System for Wireless Process Control Systems," Proceedings of the 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS), pp. 866–872, 2008
[11] S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy Theft in the Advanced Metering Infrastructure," Proceedings of the 4th Workshop on Critical Information Infrastructures Security (CRITIS), 2009
[12] M. LeMay and Carl A. Gunter, "Cumulative Attestation Kernels for Embedded Systems," Proceedings of the 14th European Symposium on Research in Computer Security (ESORICS), pp. 655–670, 2009
[13] Open Smart Grid Users Group, http://osgug.ucaiug.org , 2010
[14] AMI-SEC Task Force, "AMI Risk Assessement," http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/0.%20A MI%20Risk%20Assessment/, 2010
[15] Smart Grid Interoperability Panel, Cyber Security Working Group, "Draft NISTIR 7628: Smart Grid Cyber Security Strategy and Requirements" (second draft), http://csrc.nist.gov/publications/ , NIST (National Institute of Standards and Technology), February 2010
[16] M. Carpenter, T. Goodspeed, B. Singletary, E. Skoudis, and J. Wright, "Advanced Metering Infrastructure Attack Methodology" version 1.0, http://inguardians.com/pubs/AMI_Attack_Methodology.pdf, Jan. 5, 2009
[17] Robin Berthier; William H. Sanders; Himanshu Khurana, Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions, 2010 First IEEE International Conference on Smart Grid Communications, Year: 2010, Pages: 350 – 355.
[18] Robin Berthier; William H. Sanders, Specification-Based Intrusion Detection for Advanced Metering Infrastructures, 2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing, , Year: 2011, Pages: 184 – 193.
[19] Chee-Wooi Ten; Chen-Ching Liu; Manimaran Govindarasu, Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees, 2007 IEEE Power Engineering Society General Meeting, Year: 2007, Pages: 1 – 8.
[20] Chee-Wooi Ten; Govindarasu Manimaran; Chen-Ching Liu, Cybersecurity for Critical Infrastructures: Attack and Defense Modeling, IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, Year: 2010, Volume: 40, Issue: 4, Pages: 853 – 865.
[21] Katherine M. Rogers; Ray Klump; Himanshu Khurana; Angel A. Aquino-Lugo; Thomas J. Overbye, An Authenticated Control Framework for Distributed Voltage Support on the Smart Grid, IEEE Transactions on Smart Grid, Year: 2010, Volume: 1, Issue: 1.
[22] International Telecommunication Union, Security Architecture of Open Systems Interconnection for CCITY Applications, Series X: Data Networks and Open System Communication Oct. 1996 [Online]. Available: http://eu.sabotage.org/www/ITU/X/X0800m1e.pdf
[23] Göran N. Ericsson, Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure, IEEE Transactions on Power Delivery, Year: 2010, Volume: 25, Issue: 3, Pages: 1501 – 1507.
[24] G. Ericsson and Å. Torkilseng, "Management of information security for an electric power utility—On security domains and use of ISO/IEC 17799 standard," IEEE Trans. Power Del., vol. 20, pt. 1, pp. 683–690, Apr. 2005.
[25] G. Ericsson, Å. Torkilseng, G. Dondossola, T. Jansen, J. Smith, D. Holstein, A. Vidrascu, and J.Weiss, Security for Information Systems and Intranets in Electric Power Systems Tech. Brochure (TB) 317 CIGRÉ, 2007.
[26] Chee-Wooi Ten; Junho Hong; Chen-Ching Liu, Anomaly Detection for Cybersecurity of the Substations, IEEE Transactions on Smart Grid, Year: 2011, Volume: 2, Issue: 4, Pages: 865 – 873
[27] Yichi Zhang; Lingfeng Wang; Weiqing Sun; Robert C. Green II; Mansoor Alam, Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids, IEEE Transactions on Smart Grid, Year: 2011, Volume: 2, Issue: 4, Pages: 796 – 808.
[28] Dong Wei; Yan Lu; Mohsen Jafari; Paul M. Skare; Kenneth Rohde, Protecting Smart Grid Automation Systems Against Cyberattacks, IEEE Transactions on Smart Grid, Year: 2011, Volume: 2, Issue: 4, Pages: 782 – 795
[29] "Roadmap to secure control systems in the energy sector," U.S. Dept. Energy, U.S. Dept. Homeland Security, Energetics Incorporate, Tech. Rep., Jan. 2006.
[30] "Smart grid system report," U.S. Dept. Energy, Tech. Rep., Jul. 2009.
[31] "Smart grid system report— Annex A and B," U.S. Dept. Energy, Tech. Rep., Jul. 2009.
[32] "'Grid 2030'"—A national vision for electricity's second 100 years," U.S. Dept. Energy, Tech. Rep., Jul. 2003.
[33] Ye Yan; Yi Qian; Hamid Sharif; David Tipper, A Survey on Cyber Security for Smart Grid Communications, IEEE Communications Surveys & Tutorials, Year: 2012, Volume: 14, Issue: 4, Pages: 998 – 1010.
[34] Jing Liu; Yang Xiao; Shuhui Li; Wei Liang; C. L. Philip Chen, Cyber Security and Privacy Issues in Smart Grids, IEEE Communications Surveys & Tutorials, Year: 2012, Volume: 14, Issue: 4, Pages: 981 – 997.
[35] Yanling Yuan; Zuyi Li; Kui Ren, Quantitative Analysis of Load Redistribution Attacks in Power Systems, IEEE Transactions on Parallel and Distributed Systems, Year: 2012, Volume: 23, Issue: 9, Pages: 1731 – 1738.
[36] Y. Yuan, Z. Li, and K. Ren, "Modeling Load Redistribution Attacks in Power Systems," IEEE Trans. Smart Grid, vol. 2, no. 2, pp. 326-333, June 2011.
[37] Daojing He; Chun Chen; Jiajun Bu; Sammy Chan; Yan Zhang; Mohsen Guizani, Secure service provision in smart grid communications, IEEE Communications Magazine, Year: 2012, Volume: 50, Issue: 8, Pages: 53 – 61.
[38] Kowalik R., Nogal Ł., Januszewski M., Rasolomampionona D., Domowe urządzenia elektryczne i ich cechy przydatne w metodach identyfikacji stosowanych w systemach Smart Metering, Przegląd Elektrotechniczny, nr 11/2014, s. 26-28.
[39] Bilski P.: Nieinwazyjna identyfikacja odbiorników energii elektrycznej w pasmie średnich częstotliwości z wykorzystaniem lasu losowego, Mat. konf. SP'2016 (Łagów, 12-16 czerwca 2016).

[40] Bilski P., Wójcik A.: Metody selekcji cech sygnałów prądowo-napięciowych w nieinwazyjnej identyfikacji odbiorników energii elektrycznej, Mat. konf. SP'2016 (Łagów, 12-16.06. 2016).

Warszawa, 26-01-2018 r.