KATEDRA ENERGOELEKTRYKI WYDZIAŁU ELEKTRYCZNEGO
POLITECHNIKI WROCŁAWSKIEJ

STRESZCZENIE ROZPRAWY DOKTORSKIEJ

BEZPIECZEŃSTWO CYFROWE INTELIGENTNYCH DYSTRYBUCYJNYCH SIECI ELEKTROENERGETYCZNYCH

mgr inż. Robert Czechowski

PROMOTOR
Prof. dr hab. inż. Eugeniusz Rosołowski, prof. zw.

Promotor pomocniczy
dr inż. Piotr Pierz

Politechnika Wrocławska

Wrocław
21 listopada 2017

Streszczenie

W pracy opisano zagadnienia związane z projektowaniem i eksploatacją bezpiecznych inteligentnych dystrybucyjnych sieci elektroenergetycznych. Przedstawiono perspektywy rozwoju tych sieci w przyszłości uwzględniając kwestie ich bezpieczeństwa cyfrowego. Zaprezentowano składowe modelu inteligentnego systemu elektroenergetycznego odpowiedzialne za cyfrową komunikację, monitoring oraz sterowanie tych sieci. Omówione w pracy rozwiązania pozwolą na zwiększenie poziomu bezpieczeństwa z perspektywy zagrożeń oraz potencjalnych ataków.

Rozdział 1 (Polityka Bezpieczeństwa Inteligentnych Sieci Elektroenergetycznych) przedstawia wstęp do koncepcji elektroenergetycznych sieci inteligentnych (w tym sieci inteligentnego opomiarowania) oraz pozwala zrozumieć często niedocenianą rolę polityki bezpieczeństwa, szczególnie istotną dla zapewnienia ochrony systemów o znaczeniu krytycznym. Szczegółowo zostały omówione kwestie bezpieczeństwa cyfrowego systemu elektroenergetycznego, zasady projektowania i jego eksploatacji. Wyszczególniono również składowe inteligentnej automatyki kontrolno-pomiarowej. Przedstawiono rozwiązania na poziomie organizacyjnym, poczynając od świadomości i odpowiedzialności pracowników zatrudnionych u danego operatora energii elektrycznej, a kończąc na wdrożeniu dokumentów określających w sprecyzowany i jasny sposób zasady postępowania w przypadku wystąpienia incydentu bezpieczeństwa.

Rozdział 2 (Logiczna architektura Smart Grid) wyjaśnia jak skonstruowane są sieci inteligentne z punktu widzenia ich logicznej struktury wraz z uwzględnieniem ich podziału na role oraz funkcje w systemie. W rozdziale przedstawiono modele poszczególnych logicznych obszarów funkcjonowania sieci oraz wyjaśniono na czym polegają zależności i funkcje wszystkich aktorów (uczestników). Omówiono dokładnie sieci przesyłowe, dystrybucyjne oraz sieci niskiego napięcia nie zapominając o systemach mikro-generacji, magazynowania energii i inteligentnych instalacjach domowych zintegrowanych z systemem operatora. Przedstawiono również zależności interfejsów i kanałów komunikacyjnych stanowiących o: roli, priorytecie i wymaganym czasie odpowiedzi poszczególnych elementów, koniecznych do efektywnego zarządzania rozległymi systemami elektroenergetycznymi.

Rozdział 3 (Badania i symulacje) przedstawia pięć modeli sieci o różnym stopniu skomplikowania i obszarze funkcjonowania w infrastrukturze inteligentnych sieci elektroenergetycznych. W rozdziale zaprezentowano opis stanowisk laboratoryjnych, procedurę testową, symulacje oraz wyniki badań następujących modeli: modele sieci rzeczywistej inteligentnego opomiarowania (modele 1-3), wraz z uwzględnieniem testów stabilności i statystykami zdarzeń logicznych, model teoretyczny infrastruktury teleinformatycznej (oparty o dane rzeczywiste), odzwierciedlały wspieranie procesów kontrolno-sterujących oraz wymianę i agregacja danych (model 4), model infrastruktury ICT zaprojektowany w oprogramowaniu CySeMoL[4], mający na celu analizę potencjalnych zagrożeń, które mogą wynikać z ataków cybernetycznych przeciwko infrastrukturze informatycznej systemów sterowania i pomiarowych, oraz referencyjny model sieci dystrybucyjnej ATP-EMTP[5] (model 5). Wybrane model umożliwiają pomiar wskazanych przez użytkownika przebiegów chwilowych prądów napięć, mocy i energii oraz wybranych parametrów mechanicznych. Na podstawie analizy poszczególnych modeli możliwa jest ocena bezpieczeństwa i zagrożeń oraz ich skutków dla poszczególnych rodzajów badanych zakłóceń i celowych ataków. Modele pozwalają również na przeprowadzenie analizy dla bardzo dużej liczby wariantów scenariuszy awarii systemu oraz analizę działań zmierzających do samoczynnego i automatycznego

[4] CySeMoL ObjectModeler 2.3

[5] ATPDraw 6.2

przywrócenia do funkcjonowania sieci nie objętej awarią. Poddane analizie modele umożliwiają pozyskanie materiału badawczego w celu dokładniejszej i wielokryterialnej analizy ataków zgodnie z przyjętymi scenariuszami.

Rozdział 4 (Analiza ryzyka i ocena zagrożeń) poświęcony jest zagadnieniom szacowania ryzyka, w tym procesowi analizy i oceny prawdopodobnego wystąpienia zagrożeń. W rozdziale poruszono również konsekwencje różnych scenariuszy ataku, uwzględniając atak na pojedynczy obiekt składowy, systemu jak i ataki związane ze zmianą nastawień układów automatyki i zabezpieczeń (przesterowaniem wartości progowych), które mogą doprowadzić do zapaści systemu elektroenergetycznego i w efekcie doprowadzić do wielkoobszarowych awarii systemowych (tzw. Blackout-ów). Rozdział szczegółowo przedstawia potencjalne możliwe formy ataku, poczynając od ataków na sieć szkieletową, teleinformatyczne centrum operatora, a kończąc na atakach w sieci niskiego napięcia, w której stosowane są inteligentne liczniki energii elektrycznej, koncentratory, urządzenia aktywne sieci teleinformatycznej oraz media transmisji danych.

Rozdział 5 (Techniczne aspekty bezpieczeństwa Smart Grid) przedstawia aktualne zagadnienia i problemy spotykane przy projektowaniu inteligentnych sieci elektroenergetycznych. Przedstawiono rozwiązania i metody mogące pomóc w zwiększeniu ich bezpieczeństwa. Rozdział przedstawia również najczęściej spotykane problemy występujące w modernizacji istniejących i projektowaniu nowych sieci elektroenergetycznych wykorzystujących układy automatyki cyfrowej i rozwiązania telekomunikacyjne, opartych o technologię IT. W rozdziale omówiono najważniejsze zagadnienia i problemy spotykane podczas eksploatacji obecnych (klasycznych) systemów i sieci elektroenergetycznych tj.: promieniowanie elektromagnetyczne, zmienne kształtowanie trasy przesyłu informacji, synchronizacja czasu, układy i systemy redundantne czy też problemy związane z kradzieżą energii elektrycznej. Przedstawiono algorytmy detekcji anomalii, nadużyć oraz włamań wraz z regułami filtracji ruchu sieciowego opartych na wcześniej zdefiniowanych regułach. Omówiono również zasady komunikacji i autoryzacji użytkowników i urządzeń w każdym obszarze systemu elektroenergetycznego. Zaprezentowano dedykowane rozwiązania dostępne na rynku, które są w stanie nie tylko wykryć, ale także skutecznie odeprzeć atak, co bezpośrednio przyczyni się do zwiększenia bezpieczeństwa całego systemu.

Rozdział 6 (Wnioski i uwagi końcowe) jest podsumowaniem przeprowadzonych badań symulacyjnych oraz analiz otrzymanych wyników. Celem pracy jest udowodnienie, że główną rolą wdrożenia systemu detekcji ataku docelowo jest informowanie o tym administratora systemu w celu podjęcia przez niego działań mających na celu minimalizację negatywnych skutków powstałych w wyniku przeprowadzenia udanego ataku. Dodatkowo poruszono otwarte problemy naukowe, a także określono możliwe kierunki dalszych badań i zmian projektowych zmierzających do poprawy bezpieczeństwa w systemach elektroenergetycznych.

Przeprowadzone badania pozwolą na identyfikację potencjalnie „wrażliwych", tzn. podatnych na ataki, elementów sieci także samą analizę wzorców ataku. Opracowanie wytycznych i strategii, pozwoli na ich praktyczną implementację zwiększyć niezawodność działania i bezpieczeństwo już wykorzystywanych sieci energetycznych i tych, które jeszcze nie zostaną utworzone. Zastosowanie teleinformatycznych środków ochrony w rozległym systemie elektroenergetycznym w znacznym stopniu poprawi ich efektywność i niezawodność, co w odniesieniu do bezpieczeństwa energetycznego całego kraju ma kluczowe znaczenie. Cyfrowa wymiana informacji nierozerwalnie będzie towarzyszyć ewolucji inteligentnych sieci elektroenergetycznych, a ich bezpieczeństwo będzie priorytetem zarówno dla systemów przesyłowych, jak i dystrybucyjnych.

21.11.2017

R Gerlowski