Wpł. RDITT-17.08.2023

Wrocław 04.08.2023

Prof. dr. hab. inż. Czesław Smutnicki
Politechnika Wrocławska

Recenzja rozprawy doktorskiej

Tytuł: Metoda oceny zabezpieczeń komponentów sieci przemysłowej na przykładzie sterowników przemysłowych.
Autor: mgr inż. Dariusz Rogowski
Promotor: dr hab. inż. Andrzej Białas, prof. Łukasiewicz-EMAG

Przedmiot oceny

Przedmiotem oceny jest rozprawa doktorska z dziedziny nauk technicznych w dyscyplinie informatyka techniczna i telekomunikacja mgra. inż. Dariusza Rogowskiego pt. „Metoda oceny zabezpieczeń komponentów sieci przemysłowej na przykładzie sterowników przemysłowych" napisana pod kierunkiem dra. hab. inż. Andrzeja Białasa, prof. Łukasiewicz - EMAG. Promotorem pomocniczym był dr inż. Artur Kozłowski. Rozprawa ma całkowitą objętość 185 stron, w tym w szczególności zawiera: 100 pozycji bibliograficznych, 39 tabel, 22 rysunki, słownik pojęć, 3 spisy rzeczy, 2 załączniki. Podstawowo część pracy z bibliografią to 128 stron, dalsza części to załączniki mające interpretację dokumentów oraz ich ocenę. Rozprawa została przygotowana w ramach programu doktoratów wdrożeniowych, mającego na celu połączenie badań naukowych z przemysłem i jednostkami biznesowymi.

Informacje o Autorze rozprawy

W załączonej dokumentacji brak jest danych dotyczących przebiegu kariery zawodowej i naukowej Autora rozprawy. W rozprawie wymieniono istotne doświadczenie projektowe Autora (str. 11) w tematyce zgodnej z rozprawą. W szczególności dotyczy to kierowania częścią projektów KSO3C 2018-2022 dotyczącego wdrożenia certyfikacji standardu CC oraz projektu CyberBEAM 2021-2024 realizowanych w EMAG dla utworzenia docelowo laboratorium badania bezpieczeństwa systemów automatyki i sterowania. Według mojej wiedzy, dotychczas nie realizowano rozprawy w tej tematyce.

Tematyka rozprawy

Tematyka, zakres i przedmiot rozprawy mieści się całkowicie w zakresie dyscypliny informatyka techniczna i telekomunikacja. W rozprawie formalnie nie podano listy słów kluczowych, choć łatwo je zidentyfikować, są to: cyberbezpieczeństwo, standardy, certyfikacja, komunikacja, systemy automatyki i sterowania. Problem badawczy, który autor sformułował wynika z braku metod oceny bezpieczeństwa informatycznego urządzeń IACS (Industrial Automation and Control Systems). Do tego rodzaju urządzeń zalicza się m.in. sterowniki programowalne, interfejsy człowiek/maszyna, systemy wizualizacji, stacje robocze, interfejsy komunikacyjne, zdalne wejścia/wyjścia oraz urządzenia wykonawcze. Traktując

problem szerzej, obejmuje on komponenty różnych typów stosowane w sieci systemów sterowania, występujących jako elementy budujące cały system IACS. Problem dotyczy wielu sektorów publicznych, krytycznych dla funkcjonowania społeczeństwa, takich jak: energetyczny, transportowy, bankowy, finansowy, zdrowia, zaopatrzenia w wodę, infrastruktury cyfrowej. Szereg usług kluczowych w tych sektorach korzysta z systemów nadzoru i sterowania opartych na komponentach IACS. Problem jest niewątpliwie istotny ponieważ, mimo iż dopracowano kryteria CC (Common Criteria for Information Technology for Security Evaluation) oraz metodykę CEM (Common Evaluation Methodology for IT Security Evaluation) dla systemów typowo informatycznych, dotychczas nie udało się ujednolicić metody oceny bezpieczeństwa systemów IACS. Jednym z powodów jest różnorodność produktów IACS obecnych na rynku (wynikająca z polityki producentów urządzeń), braki w standaryzacji oraz duża zmienność produktów w czasie. Dodatkowo, w niektórych obszarach wciąż funkcjonują starsze urządzenia IACS niezapewniające odpowiedniego poziomu bezpieczeństwa. Brak metody oceny, wspólnej dla produktów IT oraz IACS, rodzi potencjalne problemy dla producentów urządzeń IACS, jak i laboratoriów oceniających. Producenci urządzeń IACS, mimo implementowania zabezpieczeń informatycznych, nie mogą uzyskać certyfikatu zgodnie z metodyką CC dla swoich produktów, ponieważ obecnie nie uwzględnia ona wymagań i kryteriów przeznaczonych dla tego typu urządzeń. Natomiast laboratoria, które wdrożyły w swojej działalności metodykę CC, mogłyby ją stosować do oceny urządzeń IACS i w ten sposób poszerzyć ofertę usług oceny bezpieczeństwa o nowy typ produktów, ale nie mogą tego zrobić z tego samego powodu. Rozwiązanie tych problemów mogłoby przynieść korzyści zarówno dla producentów IACS, jak i laboratoriów certyfikujących.

Uważam, że tematyka rozprawy jest aktualna i istotna z praktycznego punktu widzenia, bowiem dotyczy bezpieczeństwa systemów IACS, kluczowych dla funkcjonowania infrastruktury państwa, przedsiębiorstw, wytwórców, firm. W związku z licznymi działaniami hakerskimi kierowanymi ostatnio, nie tylko na obiekty IT, ale także na IACS traktowane jako strategiczne obiekty infrastrukturalne państwa atakowane w wojnie hybrydowej, znaczenie tej tematyki nabrało szczególnego znaczenia. Co więcej, w warstwie aplikacyjnej i industrialnej rozprawy opisano pilotażowe zastosowanie proponowanych rozwiązań w praktyce badań oceny bezpieczeństwa systemów klasy IACS zrealizowane testowo w laboratorium ITSEF Łukasiewicz – EMAG.

Ocena układu rozprawy

Rozprawa rozpoczyna się od dość ogólnie nakreślonego problemu certyfikacji CC dla zabezpieczenia klasycznych urządzeń IT oraz problemu certyfikacji urządzeń IACS (rozdz. 2). Następnie określono szczególne potrzeby i wymagania bezpieczeństwa dla urządzeń IACS (rozdz. 3). Wpierw określono zasoby, zagrożenia i podatności. Wylistowano komponenty, z których budowane są złożone i wielowarstwowe systemy sterowania. Podano kluczowe atrybuty bezpieczeństwa dla systemów IACS wymienione w normie IEC 62443-4-2. Zanalizowano zasoby krytyczne urządzeń IACS i ich znaczenie dla zagrożeń bezpieczeństwa. Omówiono i przeanalizowano obowiązujące standardy i normy bezpieczeństwa komponentów IACS pod kątem możliwości ich implementowania w proponowanej w rozprawie procedurze certyfikacji. Na uwagę w obu rozdziałach i w całości rozprawy zasługuje bardzo dobra znajomość przez Autora obowiązujących norm oraz wyczerpujące ich omówienie. Jest to oczywiste w kontekście roli Autora w projektach zmierzających do utworzeniu laboratorium certyfikacji bezpieczeństwa systemów IACS w EMAG. W kolejnym

rozdziale 4 podano sposób adaptacji wymagań bezpieczeństwa CC w kierunku IACS przy uwzględnieniu norm IEC oraz wymagań SFR (Security Functionality Requirement) i SAR (Security Assurance Requirement). Opis jest bardzo szczegółowy i staranny. Dokłady opis metody oceny dla IACS Autor sformułował w rozdz. 5. Tamże podano rozszerzone wymagania SAR_EXT i SFR_EXT z wykorzystaniem oryginalnych jednostek oceny. W rozdz. 6 przedstawiono walidację zaproponowanej metody oceny dla IACS, ze szczególnym uwzględnieniem oceny dokumentacji, testami funkcjonalnymi i analizą podatności. Pracę podsumowano w rozdziale 7. Każde prezentowane zagadnienie badawcze Autor omawia na tle dotychczasowej wiedzy oraz istniejących i stosowanych rozwiązań w tym zakresie.

Układ rozprawy jest organizacyjnie poprawny. Opisuje kolejno kluczowe elementy prowadzące od sformułowania CC i CEM do autorskiej metody certyfikacji urządzeń IASC. Proponowana metoda jest rozwinięciem kryteriów CC przy uwzględnieniu specyfiki urządzeń automatyki i sterowania. Kolejno rozprawa dokumentuje dokonania Autora w tym obszarze oraz prezentuje wyniki Jego badań eksperymentalnych. Eksperyment w tym przypadku ma postać sformalizowanej procedury testowania bezpieczeństwa systemu IACS zastosowanej w laboratorium ITSEF w Łukasiewicz - EMAG. Struktura pracy, podział na rozdziały i podrozdziały został zrealizowany prawidłowo. W mojej ocenie kompozycja pracy została wykonana nie tylko poprawnie, ale także właściwie z punktu widzenia tematyki rozprawy.

Merytoryczna i formalna ocena rozprawy

Na uwagę zasługuje co najmniej kilka pozytywnych cech rozprawy. Po pierwsze, dostarcza ona wyczerpującego kompendium wiedzy na temat dość specyficznej dziedziny bezpieczeństwa systemów IACS. Odmienność tego zagadnienia w stosunku do innych problemów bezpieczeństwa systemów IT polega na sformułowaniu szczególnych i rozszerzonych wymagań bezpieczeństwa dla systemów automatyki i sterowania. Po wtóre: przegląd problematyki stał się podstawą do sformułowania oryginalnej tezy rozprawy: „Metodyka Common Criteria może być zastosowana do oceny zabezpieczeń komponentów sieci przemysłowych po jej adaptacji do potrzeb i realiów specyficznych dla środowiska operacyjnego tych komponentów". Teza ta została wykazana poprzez zdefiniowanie kryteriów oceny bezpieczeństwa systemów IACS jako rozszerzenie kryteriów norm CC i metodyki CEM, a zrealizowana poprzez uwzględnienie specyficznych wymagań dla systemów IACS występujących w innych normach, w tym IEC 62443. Kryteria te obejmują wymagania na uzasadnione zaufanie do zabezpieczeń, wymagania na funkcjonalność zabezpieczeń oraz precyzują działania ewaluatora, który ocenia te wymagania. Autor rozprawy zidentyfikował problemy badawcze (patrz rozdz. 3, 4) w omawianym obszarze, sformułował zadania badawcze oraz przedstawił je w kontekście istniejących badań nad bezpieczeństwem systemów i urządzeń. Dla postawionych problemów Autor zaproponował pewne konkretne rozwiązanie (rozdz. 5) w formie autorskiej metody oceny urządzenia IACS. Rozwiązanie to ma postać sformalizowanych procedur, według których badane są urządzenia IACS i kolejno oceniane przy użyciu adekwatnych wskaźników. Pozytywnie oceniam fakt, że rozprawa zawiera staranny opis dokumentacji wykorzystywanej w tym procesie certyfikacji (załączniki 1 i 2). Jest to niezwykle istotne z punktu widzenia wiarygodności certyfikacji, powtarzalności oceny i historii zmian. Efektem finalnym badań i działań Autora rozprawy są m.in. sformalizowana procedura testowania bezpieczeństwa, zakres niezbędnych danych wejściowych do oceny, format dokumentacji z badań i ocen ewaluatora, kategoryzacja ocen cząstkowych i końcowych. Finalnie, pozwoliło to również na precyzyjną lokalizację osiągnięć

Autora na tle dziedziny. Autor wykazał także relację każdego zaproponowanego rozwiązania do zidentyfikowanych wcześniej problemów oraz zagadnień badawczych. Odniesiono otrzymane wyniki badań do spełnienia kluczowych norm międzynarodowych.

Praca ma charakter eksperymentalny, a nie teoretyczny. Jest oryginalna z punktu widzenia bezpieczeństwa systemów IACS (doktorat wdrożeniowy). Tworzy pomost pomiędzy naukowym oraz komercyjnym podejściem do zagadnień bezpieczeństwa. W mojej ocenie wykonane badania mają charakter nietrywialny i świadczą o wysokiej wiedzy dziedzinowej doktoranta.

Ocena zastosowanego piśmiennictwa

Rozprawa zawiera 100 pozycji bibliograficznych, głównie anglojęzyczne. W zdecydowanej większości są to dokumenty dotyczące norm międzynarodowych, raporty techniczne z ustaleń dedykowanych komisji EU lub rekomendacje dotyczące standardów publikowane w okresie ostatnich 5-6 lat. Podany okres czasu świadczy o aktualności dokumentów oraz o najnowszych pracach EU w zakresie standaryzacji i certyfikacji dla IACS. Liczba i repertuar „innych niż raporty" publikacji jest nieznacząca, 4 publikacje własne Autora rozprawy, 6 publikacji Promotora rozprawy plus 5-8 publikacji innych autorów. To znaczy że ok. 80% pozycji bibliograficznych to dokumenty standaryzujące i zalecenia EU. Autor rozprawy wykazał się doskonałą znajomością przywoływanych standardów międzynarodowych i krajowych oraz opracowań zespołów zajmujących się opracowaniem zaleceń międzynarodowych. Nie dziwi mnie to, bowiem odpowiada On za akredytowane laboratorium badawcze ITSEF Łukasiewicz EMAG PCA AB 1781 z 2021. Jego znajomość kluczowych dokumentów formalnych jest w tym kontekście jak najbardziej uzasadniona. Można uznać, że jest bardzo dobrze zorientowany w najnowszych dokumentach EU dotyczących tematyki rozprawy. Pozostałe pozycje piśmiennicze (inne niż dokumenty) sugerują, że albo brak jest w literaturze analiz krytycznych proponowanych rozwiązań certyfikacji IACS, albo dokonany przegląd Autora jest niekompletny w tym zakresie.

Ocena celu rozprawy

Teza rozprawy to „Metodyka Common Criteria może być zastosowana do oceny zabezpieczeń komponentów sieci przemysłowych po jej adaptacji do potrzeb i realiów specyficznych dla środowiska operacyjnego tych komponentów". Celem głównym rozprawy było i jest opracowanie metody oceny bezpieczeństwa informatycznego dla przemysłowych systemów automatyki i sterowania IACS bazującej na metodyce CC (ISO/IEC 15408), i CEM (ISO/IEC 18045) z wykorzystaniem norm charakterystycznych dla IACS, a mianowicie IEC 62443. Cel główny wynika bezpośrednio z postawionego problemu badawczego, a jego realizacja umożliwi opracowanie metody oceny uwzględniającej poziomy uzasadnionego zaufania do wykonanej oceny (EAL), a także specyfikę środowiska pracy urządzeń IACS. Do zrealizowania celu głównego wykorzystano wyniki analizy stanu techniki i wiedzy w zakresie obowiązujących metodyk i standardów stosowanych w branży przemysłowej, bieżących projektów badawczych w zakresie certyfikacji cyberbezpieczeństwa oraz wiedzę i doświadczenie autora pracy w stosowaniu standardu CC.

Odpowiednio do celu ogólnego, w rozprawie podano cele szczegółowe, a mianowicie:

1. identyfikacja potrzeb i wymagań bezpieczeństwa charakterystycznych dla branży IACS, na podstawie obecnego stanu techniki i wiedzy, standardów, metod i narzędzi oceny stosowanych w tej branży;
2. adaptacja standardu CC i metodyki oceny CEM do zidentyfikowanych potrzeb i wymagań bezpieczeństwa specyficznych dla urządzeń IACS oraz adaptacja kryteriów i wymagań standardu CC do oceny urządzeń IACS;
3. opracowanie metody oceny bezpieczeństwa, opartej na metodyce CEM, implementującej kryteria i wymagania bezpieczeństwa standardu CC dostosowane do oceny urządzeń IACS;
4. walidacja opracowanej metody w laboratorium ITSEF w trakcie pilotażowej oceny bezpieczeństwa wybranego urządzenia IACS.

Cele szczegółowe są konsekwencją celu ogólnego. Uważam, że zarówno cel ogólny, jak i cele szczegółowe zostały określone nie tylko poprawnie, ale także są istotne z punktu widzenia praktycznego i aplikacyjnego dla wskazanego specyficznego obszaru zastosowań.

Ocena zastosowanych metod badawczych

Dochodzenie do rozwiązania problemu Autor zrealizował zgodnie z metodyką opracowania koncepcji i eksperymentu CD&E (Concept Development and Experimentation) promowaną w ramach NATO (patrz str. 13). Podejście to zaleca tworzenie nowych rozwiązań na bazie doskonalenia już istniejących i sprawdzonych w praktyce poprzez testy i walidacje. Na bazie metodyki CD&E Autor podzielił realizację badań na fazę wstępną, w której zauważył pewne braki i niedogodności istniejących rozwiązań; fazę badań, w której zdefiniował problem badawczy i zaproponował możliwości jego rozwiązania; fazę rozwojową, w której opracował rozwiązanie i wykonał jego analizę; oraz fazę walidacji i ulepszania uzyskanej koncepcji. Po zakończeniu tego procesu nastąpiło ostateczne zatwierdzenie rozwiązania do wdrożenia, po jego użyciu w ocenach pilotażowych. Koncepcję rozwiązania oparto na bazie istniejącej metodyki CC i jej udoskonaleniu poprzez dostosowanie kryteriów oceny bezpieczeństwa do potrzeb charakterystycznych dla rozwiązań IACS. Charakter tego rozwiązania ma postać innowacji technologicznej już istniejącego rozwiązania. Opracowana w ten sposób metoda umożliwi wydawanie certyfikatów bezpieczeństwa jednocześnie zgodnie z normą CC i standardem przemysłowym, co z kolei ma charakter innowacji organizacyjnej. Opracowane rozwiązanie uwzględnia informatyczne i przemysłowe kryteria oceny zabezpieczeń oraz wprowadza pojęcie uzasadnionego zaufania do oceny urządzeń IACS. Sprawdzenie słuszności tej koncepcji rozwiązania odbyło się za pomocą walidacji opracowanej metody za pomocą weryfikacji zdefiniowanych kryteriów oraz na bazie wyników testów uzyskanych w laboratorium bezpieczeństwa informatycznego, w trakcie pilotażowej oceny bezpieczeństwa jednego z urządzeń IACS.

Do realizacji poszczególnych celów szczegółowych Autor rozprawy zastosował następujące metody badawcze (patrz str. 9):

Ad. 1. Dla analizy potrzeb i wymagań bezpieczeństwa oraz standardów przeznaczonych dla urządzeń IACS zastosowano metodę „analizy i krytyki piśmiennictwa".

Ad. 2. Dla adaptacji metodyki CC dla urządzeń IACS oraz opracowania i adaptacji wymagań oceny bezpieczeństwa (cel szczegółowy C2) zastosowano metodę „analizy i krytyki piśmiennictwa" oraz „analizy i konstrukcji logicznej".

Ad. 3. Dla opracowania metody oceny bezpieczeństwa dla urządzeń IACS zastosowano metodę heurystyczną.

Ad. 4. Dla walidacji koncepcji rozwiązania zastosowano metodę eksperymentalną przy pilotażowej ocenie bezpieczeństwa wybranego urządzenia IACS, wybrano programowalny sterownik zabezpieczenia odległościowego. Badania wykonano w laboratorium badawczym ITSEF Łukasiewicz – EMAG przez zespół badawczy laboratorium.

Według definicji (patrz Wikipedia) „metoda analizy i krytyki piśmiennictwa" (inaczej analiza krytyczna, przegląd literatury) jest *metodą badań naukowych* niewykorzystującą badań własnych lecz badania cudze. Ma charakter pomocniczy, i stanowi punkt wyjścia do dalszych badań własnych. Dzięki niej można wykazać luki w obecnym stanie wiedzy czy kierunki dalszej dyskusji naukowej. Tą cechę wykorzystano w rozprawie. Jednocześnie metoda analizy i krytyki piśmiennictwa może występować samoistnie, tworząc nową wiedzę. Metoda analizy krytycznej wspomaga również wykorzystywanie wiedzy, jaka została dzięki tej metodzie zanalizowana, oceniona i zsyntetyzowana. Dwie ostatnie cechy metody nie zostały w rozprawie wykorzystane, choć możliwe jest stworzenie na bazie rozprawy publikacji „przeglądowej" w tej dziedzinie.

W fazach wstępnej i badań, z wykorzystaniem metody analizy i krytyki piśmiennictwa wykonano badanie aktualnego stanu wiedzy w dziedzinie certyfikacji cyberbezpieczeństwa produktów IT oraz IACS, zbadano trendy rozwoju certyfikacji w Europie, jak również zidentyfikowano możliwości i braki istniejących metodyk oceny bezpieczeństwa. Przedmiotem badań były źródła europejskich programów badawczych, a także materiały normatywne metodyki CC i CEM. Umiejscowienie problemu badawczego w kontekście bieżących prac międzynarodowych w zakresie certyfikacji cyberbezpieczeństwa pozwoliło uzasadnić cel główny pracy i umotywować prowadzenie badań w tym kierunku.

W wyniku realizacji celów szczegółowych osiągnięto cel główny w postaci metody oceny bezpieczeństwa, która zawiera następujące elementy (kroki):

a. Sposób oceny dokumentu specyfikacji zabezpieczeń produktu;
b. Sposób oceny dokumentacji użytkownika i dokumentacji projektowej;
c. Sposób oceny środowiska projektowania, wytwarzania i utrzymania produktu oraz cyklu życia produktu;
d. Sposób oceny testów producenta;
e. Sposób wykonywania testów niezależnych przez laboratorium;
f. Sposób analizy podatności produktu w oparciu o wartość potencjału ataku.

Biorąc pod uwagę, że celem rozprawy jest opracowanie *metody* oceny bezpieczeństwa informatycznego dla przemysłowych systemów automatyki i sterowania, to zastosowane działania badawcze dobrano właściwie. Zaproponowano pewną metodę, zanalizowano jej właściwości oraz oceniono jakość metody na drodze eksperymentu. Otwartym pozostaje pytanie, czy zaproponowana metoda jest najlepsza/najkorzystniejsza w zbiorze „potencjalnych" metod tej klasy. Wprawdzie Autor podaje, że wyniku analizy krytycznej i analizy i konstrukcji logicznej zaproponował „najlepszy wariant rozwiązania" oraz „najbardziej odpowiednie rozwiązanie" (str. 75). Ocena taka jest subiektywna bowiem nie zdefiniowano „miary jakości" rozwiązania. Niewątpliwie zmiany rynkowe produktów IACS oraz bardziej staranna analiza zagrożeń atakami spowoduje zmiany w ocenach (a)-(f) zaproponowanej metody co sugeruje naturalną ewolucję w metodzie oceny bezpieczeństwa.

Ocena omówienia wyników badań

Podsumowaniem wyników badań jest rozdz. 7, pt. „Wnioski i uwagi końcowe". Dokonano w nim bilansu osiągnięć Autora rozprawy. Mimo iż omówienie jest wyczerpujące i szczegółowe, jednak w mojej ocenie jest nadmiernie długie (10 stron).

Praktyczne zastosowanie wyników badań

Autor rozprawy jest związany z Łukasiewicz - EMAG kierując kolejno projektami KSO3C 2018-2022 oraz CyberBEAN 2021-2024 w częściach realizowanych przez EMAG (w konsorcjum wchodziły każdorazowo trzy jednostki). W wyniku projektu KSO3C powstały dwa laboratoria badania bezpieczeństwa ITSEF produktów informatycznych zgodnych z CC (w IŁ -PIB i w Łukasiewicz - EMAG) oraz jednostka certyfikująca NASK – PIB. Akredytacja PCA z r. 2021 dla laboratorium ITSEF w Łukasiewicz – EMAG zezwala na wykonywanie badań oceny bezpieczeństwa zgodnie ze standardem CC i zgodnie z poziomem zaufania EAL 1 do EAL 4. Zatem jest to wdrożenie koncepcji certyfikacji CC wymienianej w rozprawie. Rozwinięciem CC i CEM na komponenty automatyki przemysłowej (IACS) oraz Przemysłowego Internetu Rzeczy (IoT, IIoT) jest obecnie realizowany projekt CybeBEAN. Jego celem jest opracowanie programu oceny i certyfikacji bardziej zaawansowanych urządzeń, w tym IASC w sposób opisany w rozprawie. Ponieważ wg stanu na r. 2023 nie wymieniono faktu akredytacji laboratoriów w zakresie koncepcji przedstawionej w rozprawie, traktuję opisaną walidację metody jako pilotażową, a także testową dla poszukiwania różnych rozwiązań w tym zakresie. Wprawdzie laboratorium Łukasiewicz – EMAG uzyskało w r. 2022 akredytację dla badań według standardu IEC 62443-4-2, jednak akredytacje CC i IEC 62443 mają póki co charakter rozłączny. Uważam, że doświadczenia Autora oraz kompetencje ITSEF Łukasiewicz – EMAG umożliwią szybką implementację Jego koncepcji.

Uwagi i komentarze

Lektura rozprawy generuje następującą listę uwag i komentarzy:

1. Od strony redakcyjnej, pożądane jest rozpoczęcie rozprawy od bardzo krótkiego „Streszczenia" (polskie, angielskie) oraz podania słów kluczowych. Faktycznie, takie streszczenia dostarczono jako samodzielne poza rozprawą. Moja uwaga wynika z faktu, że ocenie podlega rozprawa, a nie dokumenty jej towarzyszące.
2. Teza rozprawy Autora, formułując ją w sposób skrócony, to "rozszerzenie CC i CEM poprzez uwzględnienie specyficznych wymagań dla IACS.". Oczywistym alternatywnym (odwrotnym) podejściem jest „adaptacja dla potrzeb IACS tych komponentów z CC i CEM, które są istotne dla oceny bezpieczeństwa". Być może należałoby raczej mówić o „części wspólnej wymagań wynikających z CC i IACS".
3. Istnieją co najmniej dwa oddzielne podejścia do spraw bezpieczeństwa systemów IT: formalne certyfikacja CC i CEM oraz praktyka i doświadczenia funkcjonowania międzynarodowych zespołów CYBER-FORCE różnych firm zajmujących się badaniem incydentów. Nie znalazłem w rozprawie referencji do opinii i doświadczeń takich zespołów w kontekście ważności kryteriów przyjmowanych dla oceny poziomu bezpieczeństwa.

Ogólna wiedza kandydata

W rozprawie omówiono kompleksowo problematykę bezpieczeństwa systemów informatycznych, urządzeń automatyki i systemów sterowania. Doktoranta postrzegam jako jednego z ekspertów w obszarze certyfikacji procedur certyfikacji bezpieczeństwa tych urządzeń. Praca dostarcza dobrą wiedzy i analizę syntezę stanu badań oraz wyczerpujące kompendium wiedzy na wymienione wcześniej tematy. Uważam, że w kontekście pracy, wiedza kandydata jest nie tylko udowodniona rozprawą, ale także wyjątkowo szeroka.

Ważniejsze osiągnięcia zawarte w rozprawie

Za ważniejsze osiągnięcia Autora zawarte w rozprawie uważam:

1: identyfikacja kluczowych problemów bezpieczeństwa w systemach automatyki,
2: zaproponowanie rozwiązań dla postawionych problemów badawczych
3: zaprojektowanie i przeprowadzenie badań empirycznych
4: odniesienie do norm międzynarodowych

Reasumując, pragnę również podkreślić następujące elementy rozprawy:

A: rozprawa analizuje istotną klasę problemów bezpieczeństwa występujących w przemyśle, energetyce, etc.
B: rozprawa zawiera konstruktywne propozycje rozwiązania postawionych problemów badawczych
C: Autor posiada dużą wiedzę i dojrzałość w samodzielnym analizowaniu i rozwiązywaniu trudnych zagadnień bezpieczeństwa i prowadzeniu badań eksperymentalnych.
D: rozprawa łączy badania naukowe z przemysłem, zatem spełnia założenia doktoratu wdrożeniowego

Ocena końcowa

Uważam, że mimo pewnych mankamentów redakcyjnych rozprawa mgra. inż. Dariusza Rogowskiego spełnia wszystkie wymagania stawiane rozprawom doktorskim w aktualnej Ustawie z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki z późniejszymi zmianami. Przedstawione w pracy wyniki stanowią niewątpliwie oryginalne rozwiązanie istotnego problemu naukowego-badawczego. Rozprawa wykazuje także ogólną wiedzę teoretyczną Kandydata w dyscyplinie informatyka techniczna i telekomunikacja oraz umiejętność samodzielnego prowadzenia pracy naukowej.

Wnioskuje o przyjęcie recenzowanej pracy doktorskiej i dopuszczenie mgra. inż. Dariusz Rogowskiego do dalszych etapów przewodu doktorskiego, w tym do publicznej obrony pracy.