wpł. RDITT-17.08.2023
M. Stroiny

Warszawa, 24 lipca 2023 r.

Prof. dr hab. inż. Ewa Niewiadomska-Szynkiewicz
Wydział Elektroniki i Technik Informacyjnych
Politechnika Warszawska
ewa.szynkiewicz@pw.edu.pl

RECENZJA ROZPRAWY DOKTORSKIEJ DLA RADY DYSCYPLINY INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA POLITECHNIKI ŚLĄSKIEJ

Tytuł rozprawy: Metoda oceny zabezpieczeń komponentów sieci przemysłowej na przykładzie sterowników przemysłowych

Autor rozprawy: mgr inż. Dariusz Rogowski

1. Ogólna charakterystyka rozprawy. Cel badań.

Systematycznie wzrastająca liczba oraz złożoność prób działań nieuprawnionych w sieciach teleinformatycznych powoduje konieczność opracowania nowych rozwiązań w zakresie wykrywania i przeciwdziałania potencjalnym skutkom naruszeń bezpieczeństwa w cyberprzestrzeni. W ostatnich latach agencje bezpieczeństwa monitorujące przestrzeń cyfrową zgłaszają wiele incydentów związanych z naruszeniem bezpieczeństwa sieci przemysłowych, w tym funkcjonujących w jednostkach stanowiących infrastrukturę krytyczną państwa. Ich liczba rośnie wraz z rozwojem technologii i przenoszeniem operacji zdalnego monitorowania i sterowania do Internetu. Sprzyja temu integracja rozwiązań automatyki przemysłowej z infrastrukturą teleinformatyczną przedsiębiorstw oraz intensywny rozwój systemów Internetu Rzeczy, w tym bezprzewodowych sieci czujników stanowiących często komponent sieci przemysłowych.

Aby spełnić wymogi bezpieczeństwa w erze Przemysłu 4.0 i utrzymać ciągłość operacji konieczne jest zapewnienie skutecznych działań w celu szybkiego wykrywania i reagowania na incydenty bezpieczeństwa, ale przede wszystkim zabezpieczyć systemy sterowania i automatyki przemysłowej (ang. Industrial Automation and Control Systems) przed atakami komputerowymi oraz próbami nieuprawnionego dostępu. Stąd od dostawców sprzętu i oprogramowania oczekuje się wprowadzania odpowiednich zabezpieczeń oferowanych rozwiązań. Zabezpieczenia te różnią się skutecznością, wydajnością i realizacją. Współcześni odbiorcy oczekują określenia poziomu zaufania do rozwiązania, potwierdzenia jego skuteczności za pomocą testów wykonanych przez niezależną stronę, jaką są akredytowane laboratoria.

Większość funkcjonujących w kraju akredytowanych laboratoriów oceniających bezpieczeństwo systemów sterowania i automatyki przemysłowej stosuje metodyki i standardy uwzględniające atrybuty bezpieczeństwa typowe dla systemów przemysłowych. Rozważane normy nie uwzględniają zazwyczaj zagrożeń cyfrowych, nie formułują kryteriów oceny poziomu zabezpieczeń (pewności) przed incydentami bezpieczeństwa.

Z drugiej strony od pewnego czasu funkcjonuje metodyka wspólnych kryteriów do oceny bezpieczeństwa technologii informatycznych (ang. Common Criteria for Information Technology Security Evaluation - CC), norma ISO/OSI 15408 oraz jej uzupełnienie – metodyka oceny zabezpieczeń informatycznych (ang. Common Methodology for Information Technology Security Evaluation - CEM), norma ISO/OSI 18045, w której zdefiniowane są poziomy uzasadnionego zaufania (ang. Evaluation Assurance Level – EVAL), które definiują kryteria i szczegółowość wykonywanej oceny zabezpieczeń.

Naturalne wydaje się więc połączenie obu podejść i wykorzystanie opracowanych i sprawdzonych standardów i metodyk oceny bezpieczeństwa rozwiązań IT do oceny zabezpieczeń przed zagrożeniami cybernetycznymi rozwiązań IACS. Autor recenzowanej rozprawy doktorskiej podjął to wyzwanie. Przedmiotem badań prezentowanych w recenzowanej rozprawie są metodyki oceny zabezpieczeń informatycznych produktów teleinformatycznych oraz komponentów systemów automatyki przemysłowej, uwzględniające obowiązujące obecnie standardy. Celem jest opracowanie metody oceny zabezpieczeń przed cyberzagrożeniami komponentów sieci przemysłowych bazującej na metodyce Common Criteria. Cel ten był konsekwentnie realizowany, począwszy od szczegółowej analizy norm i metodyk oceny zabezpieczeń produktów IT i IACS, przez identyfikację ograniczeń oraz możliwości w zakresie certyfikacji cyberbezpieczeństwa IT i IACS, projekt i propozycję rozszerzeń i uzupełnień obowiązujących metodyk oraz walidację proponowanego rozwiązania na przykładzie oceny wybranego produktu przemysłowego.

Realizując zadania badawcze związane z osiągnięciem celu rozprawy mgr inż. Dariusz Rogowski sformułował następującą tezę (str. 10):

> „*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.*"

Słuszność tezy została potwierdzona przez wyniki analiz prezentowane w rozprawie. Opracowana przez Doktoranta metoda została również sprawdzona w laboratorium na przykładzie oceny zabezpieczeń wybranego urządzenia przemysłowego, tj. programowalnego sterownika zabezpieczenia odległościowego dla stacji elektroenergetycznych.

Rozprawa została zrealizowana w ramach programu doktoratów wdrożeniowych. Ma więc charakter praktyczny. Rozważania teoretyczne koncentrują się na zdefiniowaniu głównych problemów związanych z certyfikacją i oceną bezpieczeństwa informatycznego komponentów sieci przemysłowych oraz analizą możliwości opracowania metodyki oceny zabezpieczeń, która spełniałaby normy przemysłowe, jak i standardy bezpieczeństwa dla aplikacji informatycznych, przyjmując, że ocena zabezpieczeń jest wykonywana w jednym laboratorium. Głównym rezultatem pracy jest sprawdzona doświadczalnie autorska metoda oceny, która jest wdrożona w utworzonym w macierzystym instytucie Doktoranta laboratorium. Laboratorium ITSEF Łukasiewicz-EMAG (ang. IT Security Evaluation Facility) jest jednym z dwóch licencjonowanych laboratoriów w Polsce, upoważnionych do wykonywania ocen produktów IT zgodnie z Common Criteria. Doktorant osiągnął założony cel oraz potwierdził ogólną słuszność podjętych przez siebie badań. Należy podkreślić, że Doktorant był kluczową osobą odpowiedzialną za utworzenie laboratorium ITSEF Łukasiewicz-EMAG i realizację po stronie EMAG projektu NCBiR KSO3C, w ramach

którego powstawał krajowy program oceny i certyfikacji bezpieczeństwa produktów informatycznych zgodny z Common Criteria.

2. Syntetyczna analiza treści rozprawy. Charakter rozprawy

Zasadniczą część rozprawy podzielono na siedem rozdziałów. Rozdział pierwszy zawiera wprowadzenie w tematykę, stanowi punkt wyjścia dla treści prezentowanych w dalszej części pracy. Formułowany jest problem badawczy, omawiany kontekst i geneza rozważanego zagadnienia. Doktorant formułuje główny cel pracy badawczej oraz cele szczegółowe, a także wymagania wynikające z faktu, iż jest to doktorat wdrożeniowy.

Szczegółowe problemy badawcze C1 – C4, wokół których były skoncentrowane prace obejmowały:

- C1: analizę stanu wiedzy, techniki, standardów, metod i narzędzi stosowanych do oceny zabezpieczeń w celu identyfikacji potrzeb i wymagań bezpieczeństwa charakterystycznych dla systemów IACS,
- C2: określenie możliwego zakresu adaptacji standardu Common Criteria i metodyki oceny CEM do potrzeb i wymagań bezpieczeństwa charakterystycznych dla systemów IACS,
- C3: opracowanie metody oceny bezpieczeństwa systemów IACS bazującej na metodyce CEM i wymaganiach bezpieczeństwa standardu CC,
- C4: walidację metody w laboratorium na ITSEF Łukasiewicz-EMAG na podstawie pilotażowej oceny bezpieczeństwa wybranego urządzenia automatyki przemysłowej.

W rozdziałach drugim i trzecim Doktorant uzasadnia potrzebę podjęcia rozważanego problemu badawczego oraz prezentuje jego usytuowanie na tle aktualnego stanu badań. Na podstawie przeglądu literatury prezentowany jest stan wiedzy w zakresie certyfikacji cyberbezpieczeństwa produktów IT i IACS, w tym trendy rozwojowe certyfikacji w Europie. Omawiane są podstawowe metodyki oceny bezpieczeństwa, ze zwróceniem uwagi na ich ograniczenia. W rozdziale drugim uwaga Doktoranta koncentruje się na dwóch aspektach, tj. europejskich ramach certyfikacji cyberbezpieczeństwa oraz standardzie Common Criteria do oceny bezpieczeństwa, stanowiącego podstawę metody opracowanej w ramach pracy doktorskiej. Na podstawie analizy literatury Doktorant wskazuje na potrzebę opracowania spójnej metodyki oceny bezpieczeństwa urządzeń IACS oraz stwierdza, że wprowadzając odpowiednie rozszerzenia oraz dopuszczalne modyfikacje możliwe jest dostosowanie standardu CC i metodyki CEM do wymagań i potrzeb specyficznych dla komponentów przemysłowych.

Rozdział trzeci stanowi wprowadzenie w problematykę bezpieczeństwa systemów sterowania i automatyki przemysłowej. Doktorant prezentuje komponenty wchodzące w skład typowego systemu IACS, w tym urządzenia i sieci oraz wskazuje na krytyczne zasoby urządzeń i podstawowe zagrożenia. Szczegółowo omawia stosowane standardy i metody oceny bezpieczeństwa w systemach przemysłowych. Końcowym rezultatem przeglądu literatury przedmiotu jest wytypowanie dwóch norm przemysłowych IEC (ang. International Electrotechnical Commission) – IEC 62443-4-1 oraz IEC 62443-4-2 oraz metody TeleTrust jako materiału wyjściowego do badań, których celem jest adaptacja standardu Common Criteria do wymagań bezpieczeństwa w systemach przemysłowych.

Główne wyniki prac badawczych zawierają rozdziały czwarty i piaty. W rozdziale czwartym Doktorant prezentuje autorskie propozycje rozszerzeń standardu CC pozwalające

na dostosowanie tego standardu do specyficznych wymagań systemów IACS. Poprzedza je prezentacja studium porównawczego standardu CC oraz standardów przemysłowych IEC 62443-4-1 i IEC 62443-4-2. Autor zwraca uwagę na fakt, iż w obu przypadkach występują elementy wspólne i wyznacza kierunek działania polegający na rozważaniu każdego czynnika oddzielnie i doskonaleniu normy CC na podstawie odpowiadającej jej normy IEC. Odwzorowuje wymagania fundamentalne FR (ang. Fundational Requirement) zdefiniowane w standardach IEC do klasy wymagań na funkcjonalność zabezpieczeń SFR (ang. Security Functional Requirement) normy CC oraz wymagania normy IEC 62443-4-1 do klasy wymagań na uzasadnione zaufanie do zabezpieczeń SAR (ang. Security Assurance Requirement). Następnie dokonuje adaptacji wymagań standardu CC na potrzeby oceny bezpieczeństwa systemów przemysłowych, wykorzystując m.in. opracowane przez siebie rozszerzenia SFR i SAR, wytwarzane zgodnie z metodyką uszczegóławiania i kolejnych iteracji. Efektem końcowym prac opisanych w tym rozdziale jest przedstawiony zakresu adaptacji standardu CC do potrzeb i wymagań bezpieczeństwa charakterystycznych dla systemów sterowania i automatyki przemysłowej.

Kolejnym kluczowym rozdziałem rozprawy jest rozdział piaty zawierający opis metody oceny bezpieczeństwa systemów IACS. Bazuje on na wynikach badań przedstawionych w rozdziale czwartym. Jako podstawową metodykę oceny dla systemów przemysłowych Doktorant przyjmuje metodykę CEM (ang. Common Evaluation Methodology for IT Security Evaluation), argumentując m.in., że jest to metodyka wspierająca stosowanie standardu CC. Na podstawie krytycznej analizy aktualnego stanu stosowania metodyki CEM w laboratorium ITSEF Doktorant proponuje warianty jej ulepszenia i ostatecznie wskazuje na rozwiązanie, które uważa za najlepsze, czyli wariant wykorzystujący metodykę CEM z zaproponowanymi wcześniej dostosowaniami wymagań standardu Common Criteria. Efektem końcowym opisanym w rozdziale piątym jest autorska metoda oceny wykorzystująca zarówno oryginalne komponenty wymagań SFR i SAR normy CC, jak i komponenty rozszerzone. Rozdział kończy szczegółowy opis trzech głównych etapy metody, tj. ocena dokumentacji, testy funkcjonalne i niezależne oraz analiza podatności.

Wyniki walidacji opracowanej metody oceny bezpieczeństwa systemów przemysłowych zgodnie z poziomem EAL 4 (ang. Evaluation Assurance Level), przeprowadzonej na podstawie oceny pilotażowej programowalnego sterownika w laboratorium ITSEF Łukasiewicz – EMAG, są opisane w rozdziale szóstym. Prezentowane są wszystkie działania oceniające stanowiące wymienione etapy metody, tj. oceny klasy ASE, AGD, ADV, ALC (etap 1), ocena klasy ATE (etap 2) i klasy AVA (etap 3).

Podsumowanie rozprawy zawiera rozdział siódmy. Doktorant formułuje wnioski końcowe wskazując na użyteczność wyników wykonanej pracy badawczej i wkład w rozwój metod oceny bezpieczeństwa systemów przemysłowych, będących w ostatnich latach ważnym wektorem cyberataków. Pokazuje mocne strony rozwiązania, ale też zwraca uwagę na pewne ograniczenia i problemy, które otwierają perspektywę dalszych badań. Autor podkreśla również oryginalność przedstawionego w rozprawie rozwiązania.

3. Ocena analizy źródeł i sposobu sformułowania wniosków wynikających z analizy źródeł.

Ogółem Autor w całej rozprawie odwołuje się do 100 pozycji literatury związanych z tematyką pracy. Przegląd obejmuje opis standardów, aktów prawnych, opis inicjatyw i projektów, w tym trendów rozwojowych certyfikacji w Europie, a także publikacje naukowe z tej tematyki. Doktorant odwołuje się również do materiałów zawierających statystyki zagrożeń cyberprzestrzeni oraz opisy ataków na instalacje przemysłowe, podkreślając w ten sposób wagę i aktualność zagadnienia rozpatrywanego w rozprawie. Zamieszczony przegląd literatury koncentruje się na standardach, aktach prawnych, raportach. Nieco brakuje

szerszego omówienia literatury naukowej poświęconej zagadnieniom oceny i certyfikacji, w tym artykułów w renomowanych czasopismach o wysokich wskaźnikach wpływu. Możliwe, że jest to uzasadnione w przypadku rozważanego obszaru badawczego. Większość publikacji naukowych to prace z lat do 2019 roku. Brakuje publikacji z ostatnich lat.

Doktorant analizuje literaturę głównie w rozdziałach drugim i trzecim. Na podstawie przeprowadzonego studium literaturowego omawia standardy oraz metodyki stanowiące podstawę prowadzonych prac badawczych oraz opracowanej autorskiej metody oceny bezpieczeństwa. Publikacje wykorzystuje również do identyfikacji i wskazania problemów badawczych. Doktorant analizuje i porównuje standardy Common Criteria oraz wybrany standard przemysłowy IEC oraz metodyki oceny bezpieczeństwa. Brakuje nieco bezpośredniego odniesienia się do prac autorstwa innych badaczy, którzy podejmowali próby dostosowania standardów dla produktów informatycznych do potrzeb produktów innych branż, w tym opisu stosowanych metodyk. Byłaby wówczas możliwość porównania metodyki adaptacji przyjętej przez Doktoranta do metodyk zastosowanych przez innych badaczy.

Podsumowując, uważam, że mimo pewnych braków przedstawiona w rozprawie analiza źródeł oraz postawione na podstawie przeglądu wnioski świadczą niewątpliwie o wiedzy Doktoranta w przedmiocie rozprawy. Na szczególną uwagę zasługuje znakomita znajomość norm i metodyk oceny i umiejętność ich wnikliwej analizy i interpretacji. Doktorant dysponuje również dużym doświadczeniem zawodowym w zakresie systemów oceny i certyfikacji. Należy podkreślić, że problematyka certyfikacji, w tym oceny bezpieczeństwa ze względu na intensywny rozwój systemów teleinformatyki, który skutkuje również wzrastającą liczbą cyberzagrożeń, stanowi obecnie dynamicznie rozwijający się nurt badań. W tej sytuacji systemy ocen i certyfikacji oraz stosowane metodyki muszą być na bieżąco dostosowywane do zmieniających się warunków prawnych, administracyjnych i technicznych.

4. Analiza poprawności rozwiązania przedstawionego zadania, poprawność przyjętych założeń i wybranych metod.

Doktorant rozwiązał postawione w pracy zagadnienia. Dokonał wnikliwej analizy obowiązujących norm i metodyk oceny bezpieczeństwa. Wykorzystując wnioski z przeglądu standardów, metodyk, aktów prawnych i literatury naukowej, w tym szczegółowego porównania norm Common Criteria oraz IEC 62443, zaproponował uniwersalny sposób zwiększenia uzasadnionego zaufania do oceny zabezpieczeń przemysłowych i informatycznych. Opracował autorską metodę oceny bezpieczeństwa dla komponentów sieci przemysłowej, która nie wymaga dodatkowej walidacji w myśl ustaleń normy ISO/IEC 17025 określającej wymagania dotyczące kompetencji laboratoriów badawczych i wzorcujących. Wykorzystując wyniki pilotażowej certyfikacji wybranego urządzenia przemysłowego wykazał, że opisane w rozprawie rozwiązanie bazujące na zaproponowanych rozszerzeniach standardu CC oraz przyjęta metodyka oceny mogą być stosowane w procesie certyfikacji, a proponowane podejście do dostosowywania standardów stanowi potencjał dalszego rozwoju metod oceny dla nowych typów produktów i technologii.

Zdaniem recenzenta przyjęte metody badawcze obejmujące przegląd i szczegółową analizę standardów, stosownych aktów prawnych, opisów projektów i inicjatyw w zakresie certyfikacji, dokumentacji ocenianych produktów oraz publikacji naukowych, studium porównawcze i krytyczną analizę standardów i metodyk, iteracyjną adaptację oraz walidację rozwiązania na danych pilotażowej certyfikacji są właściwe dla badanego zagadnienia. Uzyskane wyniki potwierdzają poprawność rozwiązania. Autor w rozprawie doktorskiej

uzasadnia, że zaproponowana metoda może być stosowana do oceny zabezpieczeń komponentów przemysłowych w laboratoriach oceny bezpieczeństwa.

5. **Oryginalność rozprawy, samodzielny dorobek autora, pozycja rozprawy w stosunku do stanu wiedzy prezentowanego w literaturze światowej.**

Rozprawa zawiera nowe oryginalne rezultaty. Najważniejsze zostały wymienione poniżej.

- Ocena możliwość zastosowania standardu Common Criteria do oceny bezpieczeństwa komponentów systemów przemysłowych, wraz ze szczegółowym porównaniem standardów CC i standardów przemysłowych IEC oraz porównaniem metodyki CEM z normą do tworzenia metod oceny najnowszego wydania normy CC i porównaniem zadań zabezpieczeń IACS i CC.
- Odwzorowanie wymagań SFR (tabele 15, 39) i SAR (tabele 24, 36, 37, 38) z normy Common Criteria do wymagań bezpieczeństwa systemów IACS, w tym propozycja komponentów dodatkowych wymagań SFR i SAR (rozszerzeń) umożliwiających stosowanie standardu CC do oceny zabezpieczeń komponentów przemysłowych.
- Metoda oceny bezpieczeństwa dla urządzeń branży automatyki przemysłowej zakładająca zastosowanie, dostosowanych do potrzeb przemysłowych, wymagań Common Criteria w znormalizowanej metodyce oceny CEM, która może być stosowana w różnych laboratoriach oceny bezpieczeństwa komponentów informatycznych i przemysłowych.
- Wyniki wstępnego wdrożenia i walidacji metody na danych z pilotażowej oceny programowalnego sterownika w laboratorium ITSEF Łukasiewicz – EMAG, które potwierdziły, że zaproponowana metoda oceny uwzględnia wszystkie aspekty bezpieczeństwa przemysłowego zapisane w normach IEC oraz pozwala na wykonanie oceny zgodnie z wymaganiami rozszerzonego standardu CC.

Przedstawione wyniki mają istotne znaczenie dla tworzenia nowych metod oceny bezpieczeństwa produktów informatycznych i przemysłowych bazujących na obowiązujących standardach.

6. **Analiza poprawności prezentacji wyników pracy**

Recenzowana rozprawa doktorska liczy 158 stron, zawiera 22 rysunki i 39 tabel. Zasadnicza treść zamieszczona jest na 121 stronach, pozostałe zawierają spis treści, wykazy tabel i rysunków, słownik pojęć i akronimów, bibliografię oraz dwa załączniki. Pierwszy załącznik zawiera opis komponentów wymagań wykorzystanych w metodzie oceny systemów sterowania i automatyki przemysłowej. Drugi to skan elementów sprawozdania z pilotażowej oceny bezpieczeństwa programowalnego sterownika zabezpieczenia odległościowego dla stacji elektroenergetycznych.

Znaczna część pracy jest poświęcona omówieniu norm i standardów. Bardzo dobrym rozwiązaniem było zebranie licznych akronimów i wyjaśnienie ich znaczenia w oddzielnej tabeli. Szkoda, że nie przedstawiono analogicznej tabeli dla rozważanych standardów i metodyk oceny. Większość norm jest opisana w rozdziałach pracy, ale takie zestawienie ułatwiłoby czytanie rozprawy.

Układ pracy nie budzi zastrzeżeń. Autor w jasny sposób przedstawia rozwiązywany problem badawczy i wynikający z niego cel pracy. Wskazuje rodzaje materiałów źródłowych, które obejmują poza publikacjami naukowymi normy i wytyczne organizacji standaryzujących oraz publikowane wyniki międzynarodowych projektów, których celem jest

opracowanie ram oceny i certyfikacji bezpieczeństwa. Prezentacja osiągnięć badawczych pokazuje wyniki kolejnych, zdefiniowane przez Doktoranta, zadań szczegółowych, których rozwiązania składają się na osiągnięcie postawionego celu. Doktorant podaje również metody badawcze wykorzystane do realizacji poszczególnych celów szczegółowych. Ten sposób narracji bardzo dobrze sprawdza się, szczególnie w doktoratach o dużym komponencie praktycznym.

Praca jest zredagowana bardzo starannie, zarówno pod względem językowym, jak i graficznym. Występują drobne błędy językowe i redakcyjne, np. str. 21, 41, 85, 49 (dwa razy FTA_SSL1.1) 99, tabela 11 (czy FRU oznacza usuwanie zasobów?). Niektóre sformułowania mogą nie być oczywiste dla osoby spoza branży (np. str. 102 „utwardzanie produktu", str. 103 „bezpieczeństwo wspomagające strategię ochrony w głąb", str. 108 „testy brzegowe", str. 63 „półformalnie zweryfikowany", str. 65 tabela 19 „NA"). Nie wszystkie komponenty klasy ASE wymienione w tabelach 27 są zamieszczone na rysunku 17 (Czy jest to poprawne?). Wspomniane błędy i braki nie wpływają w sposób istotny na jakość tekstu.

Nie jest do końca jasne, czy wynikiem pracy Autora jest opracowana metoda, czy też metodyka oceny bezpieczeństwa IACS. W tabeli 25 (str. 76) mamy *„Celem głównym metody jest zapewnienie sformalizowanej, unormowanej i wspólnej metodyki do stosowania we wszystkich laboratoriach oceny bezpieczeństwa."* – czy słowo „metody" jest tu uzasadnione? Wydaje się, że słowo „metodyka" lepiej oddaje główny wynik pracy Doktoranta, który proponuje nowy wariant metodyki CEM, gdyż jest ona stosowana dla rozszerzonych wymagań bezpieczeństwa.

7. Słabe strony rozprawy i jej główne wady

Rozprawa doktorska jest, ze względu na liczność przytaczanych standardów, metodyk, praktyk i związanych z tym akronimów, niezbyt łatwa w czytaniu. Autor wykazał się bardzo dużą starannością przekazu. Generalnie jest on jasny pomimo olbrzymiej liczby akronimów, co jest charakterystyczne dla poruszanej tematyki. Niemniej warto było w niektórych miejscach odwołać się do stron zawierających definicje pojęć (nie wszystkie akronimy i pojęcia zostały zdefiniowane w tabeli 35). W niektórych rozdziałach wskazane byłoby przedstawienie dokładniejszych opisów przytaczanych pojęć. Nie jest oczywiste na jakiej podstawie ustalane są wartości zmiennych w tabeli 31 (dlaczego np. mamy dla KT tylko wartości 0, 3, 7, 11). Podobnie, co oznaczają cyfry w tabeli 18? Rysunek 10 nie wyjaśnia dokładnie Praktyk normy IEC 62443-4-1. Warto było podać nie tylko ich definicje, ale też dokładniejsze opisy w tabeli.

Pewnym ograniczeniem zaproponowanego rozwiązania, o którym też wspomina Doktorant w podsumowaniu rozprawy, jest skoncentrowanie się na rozszerzeniu standardu Common Criteria o jedną wybraną normę standardu przemysłowego, tj. IEC 62443. Może to nieco ograniczyć zakres zastosowań opracowanej metody. Niemniej prezentowane w rozprawie podejście do odwzorowywania i rozszerzania standardów może być zastosowane w dalszych pracach, których efektem będzie opracowanie kolejnych metod oceny bezpieczeństwa uwzgledniających też inne normy przemysłowe.

O walidacji opracowanej metody oceny bezpieczeństwa świadczy załącznik zawierający wybrane części raportu z badań wykonanych w laboratorium ITSEF Łukasiewicz – EMAG. Nie jest łatwo stwierdzić, które z prezentowanych wyników badań potwierdzają wykorzystanie metody Doktoranta (chodzi m.in. o wykorzystanie wprowadzonych komponentów rozszerzających). Wskazane byłoby przedstawienie skanów sprawozdania dotyczących wszystkich komponentów IEC, dla których były wprowadzone rozszerzenia SFR (poza zamieszczonymi brakuje CR1.2, CR3.7, CR7.6). Warto było, prezentując raport,

opatrzyć go stosownymi opisami objaśniającymi, nawiązać do tabel pokazujących odwzorowania standardów. Szkoda, ze nie zamieszczono w sekcji 6.2.2 (str. 107) dokładniejszego opisu wykonanych w laboratorium testów oraz przykładu jak zostały przeprowadzone. W zamieszczonym skanie sprawozdania nie widać testów wydajnościowych. Brak takich komentarzy utrudnia recenzentowi zweryfikowanie poprawności i użyteczności rozwiązania.

8. Przydatność rozprawy dla nauk technicznych

Uważam, że przedstawione w rozprawie wyniki wnoszą istotny wkład w dyscyplinę informatyka techniczna i telekomunikacja, a konkretnie w rozwój badań w zakresie certyfikacji bezpieczeństwa systemów. Opracowana autorska metoda oceny bezpieczeństwa systemów sterowania i automatyki przemysłowej jest wdrożona do działalności laboratorium oceny bezpieczeństwa ITSEF Łukasiewicz – EMAG. Została już wykorzystana w zakresie oceny testów funkcjonalnych i niezależnych, które przeprowadzono dla certyfikowanego produktu przemysłowego. Laboratorium ITSEF Łukasiewicz – EMAG uzyskało akredytację PCA oraz było audytowane przez przedstawicieli członków międzynarodowych porozumień SOGIS-IS (Mutual Recognition Agreement of Information Technology Security Evaluation Certificates) oraz CCRA (Arrangement on the Recognition of Common Criteria Certificates). Walidacja opracowanej metody oceny wykonana na danych pilotażowej certyfikacji urządzenia w tym laboratorium potwierdziła poprawność i użyteczność opracowanego rozwiązania.

9. Podsumowanie i wniosek końcowy

Uważam, że rozprawa mgr inż. Dariusza Rogowskiego spełnia wymagania stawiane rozprawom doktorskim, w tym doktoratom wdrożeniowym, przez przepisy ustawy o tytułach i stopniach naukowych. Stawiam wniosek o przyjęcie rozprawy i dopuszczenie do obrony doktorskiej.

podpis