Politechnika Śląska
Wydział Automatyki, Elektroniki i Informatyki

Dariusz Rogowski

METODA OCENY ZABEZPIECZEŃ KOMPONENTÓW SIECI PRZEMYSŁOWEJ NA PRZYKŁADZIE STEROWNIKÓW PRZEMYSŁOWYCH

Rozprawa doktorska
napisana pod kierunkiem
Dra hab. inż. Andrzeja Białasa
Dra inż. Artura Kozłowskiego

Gliwice, 2023

Serdecznie dziękuję promotorom
Andrzejowi Białasowi, Arturowi Kozłowskiemu i Markowi Sikorze
za motywację i wsparcie, na które mogłem zawsze liczyć
podczas prowadzenia badań i pisania pracy doktorskiej

Składam wyrazy wdzięczności dla zespołu laboratorium ITSEF
Patrycji, Jackowi, Marcelowi, Rafałowi i Tomkowi
za sprawnie przeprowadzoną pilotażową ocenę bezpieczeństwa

Szczególne podziękowania składam
rodzicom, Alinie i Marianowi
oraz córce Ani,
których nieustające wsparcie, nie tylko duchowe,
sprawiało, że nie traciłem wiary.

Spis treści

1. Wstęp

Systemy sterowania i automatyki przemysłowej oraz ich komponenty są coraz częściej przedmiotem cyberataków. Dzieje się tak z powodu postępującej integracji rozwiązań przemysłowych z infrastrukturą teleinformatyczną przedsiębiorstw, która, połączona z Internetem, umożliwia zdalny monitoring i zarządzanie przemysłowymi systemami sterowania (ang. Industrial Control System, ICS). Ponadto, współczesne urządzenia automatyki zbudowane są z podobnych elementów do tych, które stosuje się przy budowie rozwiązań informatycznych (ang. Information Technology, IT), zarówno sprzętowych, sprzętowo-programowych, jak i w postaci oprogramowania, co naraża je na zagrożenia i ataki, które są typowe dla rozwiązań informatycznych.

Dlatego też przedsiębiorstwa wykorzystujące w swojej działalności systemy sterowania i automatyki przemysłowej (ang. Industrial Automation and Control Systems, IACS) są coraz bardziej zainteresowane ich ochroną przed zagrożeniami i atakami za pomocą różnego rodzaju zabezpieczeń. Jednakże zabezpieczenia mogą być różnej jakości, efektywności i mogą być implementowane na różne sposoby. Nasuwa się wtedy pytanie, co sprawia, że do jednych zabezpieczeń i produktów mamy większe zaufanie, a do innych mniejsze? Odpowiedzią może być ocena produktu i jego zabezpieczeń wraz z dokumentacją wykonana przez niezależną i zaufaną trzecią stronę, np. akredytowane laboratorium oceny bezpieczeństwa IT, które zweryfikuje deklaracje producenta za pomocą odpowiednich badań i testów.

Obecnie istnieją standardy i metodyki określające wymagania bezpieczeństwa dla IACS, które jednak skupiają się głównie na atrybutach bezpieczeństwa typowych dla rozwiązań przemysłowych. Standardy te nie stosują metodyk oceny i kryteriów, które wykorzystuje się podczas oceny produktów informatycznych, jak i nie stosują tzw. uzasadnionego poziomu zaufania, inaczej pewności (ang. assurance), do wykonanej oceny zabezpieczeń.

Standardem, który stosuje pojęcie „assurance” w praktyce oceny bezpieczeństwa, jest metodyka „Wspólnych Kryteriów do oceny bezpieczeństwa technologii informatycznych” (ang. Common Criteria for Information Technology Security Evaluation) [1], [2], [3]. Metodyka opisana jest w międzynarodowym standardzie ISO/IEC 15408 [4], [5], [6] i skrótowo nazywana Common Criteria (CC). Standard CC uzupełniony jest przez metodykę oceny zabezpieczeń informatycznych CEM (ang. Common methodology for Information Technology Security Evaluation) [7], która z kolei jest opisana w normie ISO/IEC 18045 [8]. W metodyce CEM zaufanie do oceny zabezpieczeń mierzy się za pomocą poziomów uzasadnionego zaufania (ang. Evaluation Assurance Level, EAL), które definiują rygoryzm i szczegółowość przeprowadzanej oceny i użytych w niej kryteriów.

Do tej pory, zgodnie z metodyką CC, oceniono i certyfikowano wiele różnego typu produktów informatycznych, jednak wśród nich brakuje urządzeń z branży automatyki

przemysłowej. Nasuwa się pytanie, jaki jest powód tego stanu rzeczy? Dlaczego nie ocenia i nie certyfikuje się tego typu produktów zgodnie z metodyką CC?

Wydaje się, że odpowiedź naturalnie wynika z tego, że metodyka CC została opracowana głównie w celu oceny produktów IT i dlatego nie zawiera wymagań i kryteriów przeznaczonych do oceny produktów IACS. Można zatem postawić kolejne pytanie, czy można w jakiś sposób dostosować, uzupełnić lub udoskonalić tę metodykę tak, aby spełniała wymagania i odpowiadała także na potrzeby oceny bezpieczeństwa charakterystyczne dla tego typu produktów? A jeśli tak, to czy dałoby się ją zastosować do oceny bezpieczeństwa tych produktów za pomocą odpowiednio przygotowanej metody oceny?

Uzyskanie odpowiedzi na te pytania jest głównym celem, który postawił sobie autor niniejszej pracy doktorskiej.

1.1. Problem badawczy

Problem badawczy pracy wynika z braku metody oceny bezpieczeństwa informatycznego przeznaczonej dla urządzeń IACS. 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. Problem zatem można potraktować szerzej, nie ograniczając się do jednego typu komponentu, a jego rozwiązanie obejmie wiele typów komponentów stosowanych w sieci systemu sterowania, występujących jako elementy budujące cały system IACS.

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.

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.

Producenci uzyskaliby możliwość oceny zabezpieczeń zarówno zgodnie z wymaganiami informatycznymi, jaki i przemysłowymi, i to w jednym i tym samym laboratorium, a co więcej zgodnie z zadeklarowanym poziomem EAL. Natomiast laboratoria mogłyby poszerzyć swoją ofertę usług oceny o nowy typ produktów na bazie już stosowanej metodyki CEM.

Rozwiązanie problemu badawczego będzie stanowić podstawę rozwoju dziedziny informatyki w zakresie certyfikacji i oceny bezpieczeństwa informatycznego, ponieważ nie tylko poszerza zakres zastosowań o urządzenia IACS, ale stanowi także bazę do rozwoju metod dla innych specyficznych typów produktów lub technologii.

1.2. Cele i przedmiot pracy

Celem głównym pracy jest opracowanie metody oceny bezpieczeństwa informatycznego dla przemysłowych systemów automatyki i sterowania bazującej na metodyce CC.

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.

Zdefiniowano następujące cele szczegółowe pracy, tożsame z zagadnieniami badawczymi, które umożliwią osiągnięcie celu głównego:

- C1 – analiza problemu badawczego pod kątem identyfikacji potrzeb i wymagań bezpieczeństwa charakterystycznych dla branży IACS, na podstawie obecnego stanu techniki i wiedzy, standardów, metod i narzędzi oceny stosowanych w tej branży;
- C2 – analiza problemu pod kątem określenia możliwego zakresu adaptacji standardu CC i metodyki oceny CEM do zidentyfikowanych potrzeb i wymagań bezpieczeństwa specyficznych dla urządzeń IACS oraz adaptacji kryteriów i wymagań standardu CC do oceny urządzeń IACS;
- C3 – rozwiązanie problemu badawczego poprzez opracowanie metody oceny bezpieczeństwa, opartej na metodyce CEM, implementującej kryteria i wymagania bezpieczeństwa standardu CC dostosowane do oceny urządzeń IACS;

- C4 – walidacja opracowanej metody w laboratorium w trakcie pilotażowej oceny bezpieczeństwa wybranego urządzenia IACS.

Przedmiot pracy, uwzględnia realizację powyższych celów i obejmuje swym zasięgiem normy i wytyczne organizacji standaryzacyjnych, projekty badawcze dotyczące budowy ram oceny i certyfikacji bezpieczeństwa, artykuły naukowe opisujące zagrożenia bezpieczeństwa dla rozwiązań przemysłowych, a także narzędzia i metody oceny bezpieczeństwa dla rozwiązań przemysłowych. Materiały źródłowe obejmują m.in.:

- Standardy przemysłowe stosowane do oceny bezpieczeństwa IACS [9], [10], przykładowo: IEC 62443 [11], [12], IEEE 1686 [13];
- Standard Common Criteria oraz metodykę oceny CEM, w tym najnowsze wydanie normy CC (Release 1) z listopada 2022 r. [14], [15], [16], [17], [18];
- Wytyczne NIST (ang. National Institute of Standards and Technology) [19] w zakresie wymagań bezpieczeństwa rekomendowanych dla urządzeń IACS;
- Projekty europejskie realizowane w celu opracowania i ustanowienia europejskich ram certyfikacji i oceny produktów IT (ang. EU Cybersecurity Certification scheme, EUCC) [20] oraz urządzeń automatyki przemysłowej [21].

Do realizacji celów szczegółowych zastosowano metody badawcze, które krótko scharakteryzowano poniżej.

W części pracy dotyczącej analizy potrzeb i wymagań bezpieczeństwa oraz standardów przeznaczonych dla urządzeń przemysłowych (cel szczegółowy C1) została wykorzystana metoda analizy i krytyki piśmiennictwa.

W przypadku analizy problemu w zakresie możliwej adaptacji metodyki Common Criteria dla urządzeń IACS oraz opracowania i adaptacji wymagań oceny bezpieczeństwa (cel szczegółowy C2) zostały wykorzystane metoda analizy i krytyki piśmiennictwa oraz analizy i konstrukcji logicznej.

W celu rozwiązania problemu badawczego w postaci metody oceny bezpieczeństwa dla urządzeń IACS (cel szczegółowy C3) zastosowano metodę heurystyczną.

W celu walidacji koncepcji rozwiązania, opracowaną metodę zastosowano w części dotyczącej testów funkcjonalnych i niezależnych (metoda eksperymentalna) podczas pilotażowej oceny bezpieczeństwa dla wybranego urządzenia IACS (cel szczegółowy C4). Pilotażowa ocena została wykonana w laboratorium badawczym ITSEF Łukasiewicz – EMAG przez zespół badawczy laboratorium.

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

- Sposób oceny dokumentu specyfikacji zabezpieczeń produktu;
- Sposób oceny dokumentacji użytkownika i dokumentacji projektowej;

- Sposób oceny środowiska projektowania, wytwarzania i utrzymania produktu oraz cyklu życia produktu;
- Sposób oceny testów producenta;
- Sposób wykonywania testów niezależnych przez laboratorium;
- Sposób analizy podatności produktu w oparciu o wartość potencjału ataku.

1.3. Teza pracy

Teza postawiona przez autora, która wynika z problemu badawczego i celu głównego pracy brzmi następująco:

„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."

Powyższa teza zostanie uzasadniona w toku realizacji celów szczegółowych oraz walidacji metody w laboratorium na wybranym przykładzie urządzenia przemysłowego, z czego także w konsekwencji wynika cel wdrożeniowy niniejszej pracy doktorskiej.

1.4. Doktorat wdrożeniowy

Celem wdrożeniowym pracy jest zastosowanie opracowanej metody w działalności operacyjnej laboratorium oceny bezpieczeństwa ITSEF Łukasiewicz – EMAG. Wyniki pracy przyczynią się do poszerzenia oferty laboratorium o nowy typ ocenianych produktów w postaci komponentów i urządzeń stosowanych w przemysłowych systemach sterowania. Metoda oceny zostanie ostatecznie wdrożona do działalności operacyjnej laboratorium, po wykonaniu ocen pilotażowych dla co najmniej dwóch produktów i po wprowadzeniu ewentualnych korekt wynikających z analizy wniosków ze zrealizowanych procesów oceny.

Wyniki pracy doktorskiej umożliwią producentom urządzeń IACS ocenę zabezpieczeń zgodnie z normą CC oraz przyczynią się do zwiększenia poziomu zaufania użytkowników do tych urządzeń. Urządzenia systemów sterowania będą posiadać zwiększoną odporność na ataki informatyczne i poprawią tym samym ich konkurencyjność na rynkach krajowym i zagranicznym. Natomiast laboratoria zyskają możliwość stosowania znormalizowanej metodyki CEM do oceny urządzeń przemysłowych, co jest bardzo ważne także w kontekście przyszłego rozwoju działalności laboratorium ITSEF Łukasiewicz – EMAG.

Laboratorium ITSEF Łukasiewicz – EMAG powstało w wyniku realizacji projektu badawczego, pt.: „Krajowy schemat oceny i certyfikacji bezpieczeństwa oraz prywatności produktów i systemów IT zgodny z Common Criteria (KSO3C)", 2018 – 2022, realizowanego

przez trzy jednostki naukowo-badawcze: lidera projektu, Instytut Łączności – Państwowy Instytut Badawczy (IŁ – PIB) oraz Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (NASK – PIB) i Sieć Badawczą Łukasiewicz – Instytut Technik Innowacyjnych EMAG. Projekt został sfinansowany przez Narodowe Centrum Badań i Rozwoju w ramach II programu „CyberSecIdent – Cyberbezpieczeństwo i eTożsamość", nr umowy CYBERSECIDENT/ 3812 82/ II/ NCBR/ 2018 [22]. Doktorant pełnił w projekcie rolę kierownika grupy zadań realizowanych przez Łukasiewicz – EMAG.

W wyniku realizacji projektu został opracowany krajowy program oceny i certyfikacji bezpieczeństwa produktów informatycznych zgodny z Common Criteria. W programie certyfikacji uczestniczą dwa laboratoria ITSEF ustanowione w instytutach IŁ – PIB i Łukasiewicz – EMAG oraz Jednostka Certyfikująca (JC) utworzona w NASK – PIB. Laboratoria ITSEF zostały akredytowane przez Polskie Centrum Akredytacji (PCA) według wymagań normy ISO/IEC 17025 [23] dla laboratoriów badawczych, natomiast Jednostka Certyfikująca według wymagań normy ISO/IEC 17065 [24] dla jednostek certyfikujących wyroby.

Laboratorium ITSEF Łukasiewicz – EMAG uzyskało akredytację PCA nr AB 1781 [25] w marcu 2021 r. Zakres akredytacji obejmuje standard Common Criteria i metodykę oceny CEM i zezwala na wykonywanie badań oceny bezpieczeństwa zgodnie z poziomem uzasadnionego zaufania od EAL 1 do EAL 4.

We wrześniu 2022 r. krajowy program certyfikacji wraz z laboratoriami został poddany audytowi przez przedstawicieli członków międzynarodowych porozumień SOG-IS (ang. Mutual Recognition Agreement of Information Technology Security Evaluation Certificates) [26], [27] oraz CCRA (ang. Arrangement on the Recognition of Common Criteria Certificates) [28], [29]. Porozumienia te są podstawą wzajemnego uznawania certyfikatów bezpieczeństwa wydawanych przez członków tych porozumień. Audyt zakończył się pozytywnym wynikiem, skutkiem czego Polska uzyskała status członka autoryzowanego do wydawania międzynarodowych certyfikatów w ramach tych porozumień. Natomiast laboratoria zostały wpisane przez SOG-IS na listę laboratoriów licencjonowanych (ang. Licensed ITSEF) [30].

Należy tutaj dodatkowo wspomnieć o innym projekcie badawczym, którego dotychczasowe wyniki pozytywnie wpłynęły na realizację doktoratu, jak i będą miały wpływ na wdrożenie rezultatów pracy doktorskiej w przyszłości. Obecnie realizowany jest w Łukasiewicz – EMAG projekt badawczy pt. „System oceny i certyfikacji cyberbezpieczeństwa – lekkie programy certyfikacji (CyberBEAM)", 2021 - 2024. W projekcie doktorant pełni rolę kierownika grupy zadań Łukasiewicz – EMAG. Projekt realizowany jest w konsorcjum z liderem projektu NASK – PIB. Projekt jest finansowany przez NCBiR w ramach programu CyberSecIdent IV (Cyberbezpieczeństwo i e-Tożsamość), nr umowy: CYBERSECIDENT/ 489595/IV/NCBR/2021.

Celem projektu CyberBEAM jest opracowanie tzw. lekkiego, w sensie krótkiego czasu realizacji i niższych kosztów, programu oceny i certyfikacji cyberbezpieczeństwa dla komponentów automatyki przemysłowej (IACS), przemysłowego Internetu rzeczy (ang. Industrial IoT, IIoT) oraz centrów przetwarzania danych (CPD). Dodatkowym celem jest także rozbudowa laboratorium do wykonywania badań zgodnie z opracowanym programem. Łukasiewicz – EMAG odpowiada za opracowanie programu dotyczącego oceny cyberbezpieczeństwa dla IACS i IIoT.

Budowany w projekcie program będzie komplementarny do, uruchomionego w ramach projektu KSO3C, programu certyfikacji zgodnego z Common Criteria. Ponadto, program będzie spełniał wytyczne europejskich programów certyfikacji EUCC [20] oraz przyszłych programów dotyczących certyfikacji IACS, w skrócie ICCS (ang. IACS Components Certification Scheme) [21].

W toku realizacji projektu CyberBEAM, w ramach rozszerzania działalności laboratorium ITSEF, możliwa była realizacja oceny pilotażowej urządzenia IACS. Dzięki uprzejmości producenta, który udostępnił dokumentację i urządzenie do testów, możliwe było wykonanie oceny bezpieczeństwa zgodnie ze standardem przemysłowym IEC 62443-4-2 [12], który został uwzględniony podczas adaptacji wymagań CC w niniejszym doktoracie.

Dzięki temu możliwe było wykorzystanie wyników pilotażu do walidacji metody w części dotyczącej testów funkcjonalnych i niezależnych urządzenia. Wyniki pilotażu, po ich pozytywnej weryfikacji przez PCA podczas audytu laboratorium ITSEF w listopadzie 2022 r., przyczyniły się także do uzyskania przez laboratorium rozszerzenia akredytacji na wykonywanie badań bezpieczeństwa zgodnie ze standardem przemysłowym IEC 62443-4-2.

Rezultaty powyższych projektów badawczych oraz wdrożenie wyników badań niniejszej pracy doktorskiej przyczynią się do zbudowania kompetencji technicznych i poszerzenia oferty oceny bezpieczeństwa obejmującej produkty informatyczne oraz urządzenia stosowane w przemyśle, zgodnie z najnowszymi standardami, politykami i kierunkami rozwoju certyfikacji cyberbezpieczeństwa w Europie.

1.5. Opis pracy

W rozdziale 2 zidentyfikowano problem badawczy, uzasadniono cel główny i motywację podjętych badań. Na podstawie wyników analizy aktualnego stanu techniki i wiedzy w obszarze oceny cyberbezpieczeństwa rozwiązań IT i IACS przedstawiono i zidentyfikowano braki obecnych metod i możliwości adaptacji standardu CC. W wyniku analizy zaproponowano koncepcję rozwiązania problemu badawczego poprzez możliwość udoskonalenia istniejących i sprawdzonych w praktyce metod oceny.

Rozdział 3 przedstawia analizę problemu w kontekście identyfikacji wymagań bezpieczeństwa charakterystycznych dla urządzeń IACS. Wytypowane źródła wymagań IACS

zostaną użyte jako materiał wejściowy do adaptacji wymagań CC, które z kolei zostaną zaimplementowane w opracowanej metodzie oceny. Wyniki badań pozwoliły na realizację celu szczegółowego C1.

Rozdział 4 przedstawia analizę problemu w zakresie określenia możliwego zakresu adaptacji standardu CC i metodyki oceny CEM do urządzeń IACS. Zidentyfikowano podobieństwa pomiędzy standardami przemysłowymi i CC oraz sposób ich wykorzystania do adaptacji wymagań CC. Pokazano wyniki tej adaptacji w postaci odpowiednich zbiorów rozszerzonych wymagań CC, dostosowanych do oceny bezpieczeństwa IACS, które stanowią realizację celu szczegółowego C2.

Rozdział 5 przedstawia rozwiązanie problemu poprzez opracowanie metody oceny bezpieczeństwa dla urządzeń IACS, do której zastosowano zaadaptowane wymagania CC, co umożliwiło realizację celu szczegółowego C3.

Rozdział 6 przedstawia wyniki walidacji rozwiązania włącznie z wykorzystaniem wyników testów wykonanych w pilotażowej ocenie bezpieczeństwa wybranego urządzenia, co stanowi realizację celu szczegółowego C4.

Rozdział 7 zawiera wnioski końcowe, opis wdrożenia wyników w laboratorium ITSEF Łukasiewicz - EMAG oraz dalsze kierunki prac.

2. Identyfikacja problemu badawczego - analiza stanu wiedzy

W rozdziale zidentyfikowano problem badawczy pracy oraz przedstawiono koncepcję jego rozwiązania. Dochodzenie do rozwiązania problemu odbywało się zgodnie z metodyką opracowania koncepcji i eksperymentu (ang. Concept development and experimentation, CD&E) [31] promowaną w ramach NATO. Podejście to zaleca tworzenie nowych rozwiązań na bazie doskonalenia już istniejących i sprawdzonych w praktyce poprzez testy i walidacje.

Na bazie metodyki CD&E realizację badań podzielono na fazę wstępną, w której zauważono pewne braki i niedogodności; fazę badań, w której zdefiniowano problem badawczy i zaproponowano możliwości jego rozwiązania; fazę rozwojową, w której opracowano rozwiązanie i wykonano analizy; aby w końcu przejść do fazy walidacji i ulepszania uzyskanej koncepcji. Na końcu tego procesu nastąpi ostateczne zatwierdzenie rozwiązania do wdrożenia, po jego użyciu w ocenach pilotażowych [31].

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 Common Criteria i CEM.

2.1. Europejskie ramy certyfikacji cyberbezpieczeństwa

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 2016 r. Parlament Europejski przyjął pierwsze prawo dotyczące cyberbezpieczeństwa w postaci dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii [32]. Przyjęta dyrektywa NIS (ang. Network and Information Systems) nakłada na państwa członkowskie obowiązki w zakresie powołania konkretnych instytucji i mechanizmów gwarantujących minimalny poziom krajowych zdolności w dziedzinie bezpieczeństwa. Dyrektywa NIS, m.in. klasyfikuje tak zwanych operatorów usług kluczowych, w przypadku których incydenty bezpieczeństwa teleinformatycznego mogą mieć istotny wpływ na możliwość świadczenia tych usług. Regulacje obejmują następujące sektory: energetyczny, transportowy, bankowy, finansowy, zdrowia, zaopatrzenia w wodę, infrastruktury cyfrowej. Wiele z usług kluczowych korzysta z systemów nadzoru i sterowania opartych na komponentach IACS, dlatego opracowanie metody ich oceny mogłoby stanowić adekwatną odpowiedź na wymagania dyrektywy.

W 2018 r. przyjęto w polskim ustawodawstwie Ustawę o Krajowym Systemie Cyberbezpieczeństwa (KSC) [33], która odpowiada na wymagania postawione w Dyrektywie NIS. W maju 2022 r. Rada i Parlament Europejski osiągnęły porozumienie w sprawie zastąpienia obowiązującej dyrektywy NIS nową dyrektywą NIS2 [34], [35] , która uwzględnia nowe zagrożenia wynikające z postępującej cyfryzacji oraz zwiększającej się liczby nowych rodzajów cyberataków. W związku z tym i w polskiej ustawie KSC będą musiały nastąpić odpowiednie nowelizacje, tym samym powstające programy oceny bezpieczeństwa także będą musiały być zaktualizowane, także metody oceny bezpieczeństwa.

W 2019 r. został ustanowiony przez Radę Europy, tzw. Akt o cyberbezpieczeństwie (ang. Cybersecurity Act, CSA) [36], [37]. Rozporządzenie CSA jest wynikiem prac i inicjatyw, które od kilku już lat podejmowane są w Europie w celu ustanowienia wspólnych ram dla certyfikacji cyberbezpieczeństwa [38]. Rozporządzenie dotyczy Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), nadając jej stały mandat i pełnomocnictwo do regulacji kwestii cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych.

Rozporządzenie określa podstawowe wymagania dla wszystkich programów certyfikacji obowiązujących w Europie. Akt CSA składa się z dwóch części: 1) pierwsza część daje ENISA permanentny mandat oraz szereg nowych obowiązków związanych z wejściem w życie Dyrektywy NIS oraz europejskich ram certyfikacji; 2) druga część dotyczy europejskich ram

certyfikacji cyberbezpieczeństwa dla produktów i usług teleinformatycznych (ang. ICT, Information and Communication Technology), które przewidują wprowadzenie dobrowolnej certyfikacji, jak i obowiązkowej certyfikacji, dla produktów, usług i procesów ICT na trzech poziomach bezpieczeństwa: podstawowym (ang. Basic), istotnym (ang. Substantial) i wysokim (ang. High). Wprowadzone zostaje zatem pojęcie poziomu bezpieczeństwa, które wiąże się ściśle z odpornością produktu na odpowiadający tym poziomom potencjał ataku. Zatem metoda oceny powinna zawierać elementy analizy podatności z uwzględnieniem potencjału ataku i związanym z nimi poziomem bezpieczeństwa produktu.

Agencja ENISA, w ramach swojego mandatu zapewnionego w Akcie CSA, zaproponowała pierwszą, roboczą wersję europejskiego programu certyfikacji cyberbezpieczeństwa (ang. EU Cybersecurity Certification, EUCC) [20]. Wersja programu EUCC powstała w oparciu o metodykę Common Criteria (ISO/IEC 15408) i wymagania międzynarodowego porozumienia o wzajemnym uznawaniu certyfikatów SOG-IS MRA (ang. Senior Officials Group - Information Systems Security Mutual Recognition Agreement) [26], [27]. Laboratorium ITSEF jest obecnie zgodne z wymaganiami CC, dzięki temu jednocześnie jest już przygotowane do wdrożenia regulacji nowego programu EUCC.

W kontekście certyfikacji cyberbezpieczeństwa dla rozwiązań przemysłowych należy przytoczyć wyniki prac grupy tematycznej ERNCIP TG [39] (ang. The European Reference Network for Critical Infrastructure Protection Thematic Group), działającej we Wspólnym Centrum Badawczym (ang. Joint Research Centre, JRC) przy Komisji Europejskiej [40]. Prace tej grupy rozpoczęły się już w 2014 r. i koncentrowały na certyfikacji bezpieczeństwa produktów z branży przemysłowych systemów sterowania i automatyki przemysłowej. Pod koniec 2014 r. grupa wydała swój pierwszy raport [41], w którym przedstawiła rekomendacje dotyczące utworzenia europejskiego programu badania zgodności i certyfikacji cyberbezpieczeństwa komponentów IACS. W ciągu kolejnych lat działalności głównymi zadaniami grupy było opracowanie danych wejściowych oraz wytycznych dla utworzenia europejskich ram oceny i certyfikacji komponentów ICCF (ang. IACS Components Cybersecurity Certification Framework) [21]. W efekcie tej działalności, w roku 2020, grupa opracowała i opublikowała rekomendacje dla wdrażania programów certyfikacji IACS [42]. Programy te, w skrócie nazywane ICCS (ang. IACS Components Certification Scheme), wdrażane wg wypracowanych rekomendacji, będą zgodne z postanowieniami Aktu CSA, czyli będą mogły być stosowane przez europejskie jednostki certyfikujące i laboratoria oceniające zgodność z wymaganiami bezpieczeństwa.

Rekomendacje grupy roboczej ERNCIP wyrażone w raporcie z 2020 r. wskazały, aby pierwszy europejski program certyfikacji dla IACS oprzeć o wymagania standardów przeznaczonych dla rozwiązań informatycznych i zarekomendowała użycie standardu Common Criteria wspieranego rodziną standardów przemysłowych IEC 62443. W raporcie

wskazano na brak zharmonizowanej metodyki oceny dla urządzeń IACS. Zwrócono w raporcie uwagę, że taka metodyka może zostać opracowana np. przez grupę roboczą CEN/Cenelec JTC13 WG3 (Security evaluation and assessment) [43]. Grupa obecnie pracuje nad projektem metodyki oceny cyberbezpieczeństwa dla technologii informacyjnych (ang. Cybersecurity Evaluation Methodology for ICT products), który może stać się podstawą do rozwoju metodyki dla urządzeń przemysłowych.

Ponadto w raporcie rekomenduje się, aby prace nad opracowaniem metodyki prowadzić z maksymalnym wykorzystaniem możliwości ponownego użycia już istniejących standardów. Dlatego też w pracy doktorskiej zbadano możliwość opracowania rozwiązania na bazie udoskonalenia i adaptacji sprawdzonej metodyki oceny CEM z dodatkową implementacją wymagań przemysłowych IEC 62443.

Prace nad europejskimi ramami oraz programami certyfikacji cyberbezpieczeństwa są zaawansowane i należy się spodziewać, że w ciągu następnych kilkunastu miesięcy zostaną opracowane odpowiednie akty wykonawcze, co zostało wyrażone przez przedstawicieli ENISA na konferencji „ENISA Cybersecurity Certification Conference 2022" [44]. Ramy certyfikacji definiują, m.in., że podstawową ich strukturę tworzą jednostki certyfikujące i laboratoria oceniające zabezpieczenia IT (ang. IT Security Evaluation Facility, ITSEF). Jednostki certyfikujące nadzorują i walidują wyniki badań wykonanych przez laboratoria i na tej podstawie wydają certyfikaty. Taka struktura została już zbudowana w Polsce w wyniku realizacji projektu KSO3C.

Najnowsza europejska propozycja regulacji rynku bezpiecznych produktów, tzw. Akt dotyczący cyberodporności [45] (ang. Cyber Resilence Act, CRA), jest projektem rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020 [46] dotyczące nadzoru rynku i zgodności produktów.

W załącznikach [47] do aktu CRA określono, m.in. wymogi bezpieczeństwa dla produktów z elementami cyfrowymi, wymogi dotyczące postępowania w przypadku wykrycia podatności bezpieczeństwa, a także wskazano jakie informacje w kontekście bezpieczeństwa powinny być zawarte w instrukcjach dla użytkowników. W szczególności załącznik nr 3 identyfikuje produkty krytyczne z elementami cyfrowymi, które będą podlegać ocenie zgodności w jednostkach notyfikowanych (np. w akredytowanych laboratoriach oceny bezpieczeństwa).

Wśród tych produktów wymieniono m.in.: systemy sterowania i automatyki przemysłowej (IACS), takie jak: sterowniki (ang. Programmable Logic Controler, PLC), rozproszone systemy sterowania (ang. Distributed Control System, DCS), komputerowe sterowniki numeryczne (ang. Computer Numerical Control, CNC) dla obrabiarek oraz systemy kontroli i akwizycji danych (ang. Supervisory Control and Data Acquisition, SCADA). Opracowanie

metody oceny IACS i jej wdrożenie w laboratorium ITSEF umożliwi prowadzenie ocen bezpieczeństwa także zgodnie z wymaganiami aktu CRA.

Pozostałe załączniki CRA określają warunki deklaracji zgodności UE, zawartość dokumentacji technicznej produktu przekazywanego do oceny zgodności, a także opisują procedury oceny zgodności wykonywane przez jednostki notyfikowane, takie jak ITSEF.

Metoda oceny opracowana w ramach niniejszej rozprawy – po jej wdrożeniu w laboratorium ITSEF Łukasiewicz – EMAG akredytowanym przez Polskie Centrum Akredytacji i autoryzowanym przez europejskie porozumienie SOG-IS oraz światowe porozumienie CCRA (ang. Common Criteria Recognition Arrangement) [28] – umożliwi wprowadzenie do oferty laboratorium nowej usługi oceny cyberbezpieczeństwa przeznaczonej dla produktów przemysłowych. Usługi zgodnej z europejskimi ramami certyfikacji cyberbezpieczeństwa (EUCC), regulacjami Aktu CSA oraz zgodnej z rozporządzeniem Aktu CRA o cyberodporności.

Przegląd projektów badawczych dotyczących certyfikacji cyberbezpieczeństwa w Europie oraz aktualnych trendów i aktów prawnych wykazał, że:

- Brakuje zharmonizowanej metodyki oceny bezpieczeństwa urządzeń IACS;
- Istnieją rekomendacje budowy metodyki oceny IACS w oparciu o istniejące i sprawdzone standardy Common Criteria i IEC 62443;
- Akty prawne UE w zakresie oceny cyberbezpieczeństwa obejmują standardy i metodyki oceny, które już zostały przyjęte i są stosowane w polskim programie oceny IT (KSO3C).

Wyniki analizy wskazują zatem na zasadność postawionego w pracy problemu badawczego i celowość jego rozwiązania. Dotychczas nie opracowano żadnej zharmonizowanej na szczeblu europejskim metodyki oceny IACS, a rekomendacje wykorzystania do jej opracowania metodyki CC są szansą dla autora rozprawy wykorzystania wieloletniego doświadczenia i wiedzy w zakresie CC. W kolejnym rozdziale wykonano analizę, czy faktycznie standard CC i metodyka CEM posiadają potencjał do adaptacji i możliwości zastosowania do innych produktów niż typowo informatycznych.

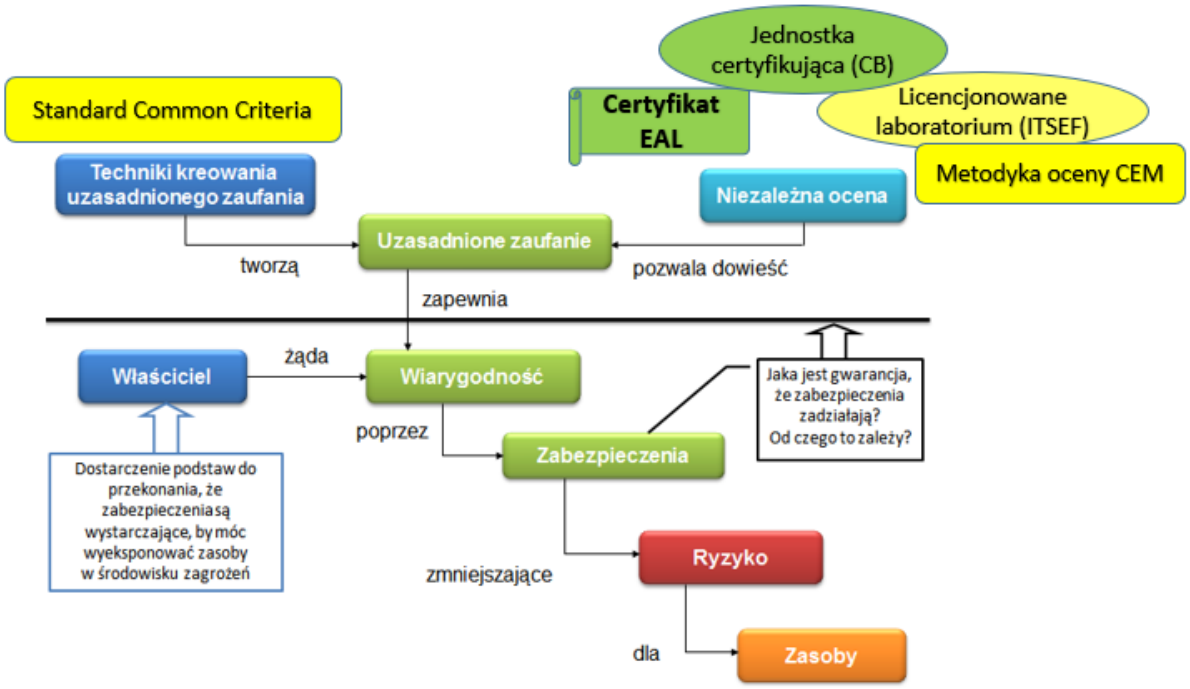
2.2. Standard Common Criteria do oceny zabezpieczeń IT

Rozdział przedstawia analizę problemu badawczego w kontekście uzyskania odpowiedzi czy standard CC jest stosowany do systemów przemysłowych i czy są prowadzone prace w tym kierunku. Za pomocą metody krytyki i analizy piśmiennictwa wskazano źródła, w których wymieniano standard CC w kontekście jego zastosowania do systemów przemysłowych oraz oceniono wynikające z tego rekomendacje. Dodatkowo, na podstawie analizy źródłowych materiałów normatywnych CC, publikacji naukowych oraz wiedzy autora na temat standardu zidentyfikowano możliwy zakres adaptacji CC do wymagań urządzeń IACS.

Ze względu na to, że koncepcja rozwiązania problemu badawczego opiera się na CC i CEM i całość rozprawy doktorskiej skupiona jest w głównej mierze na dokładnej znajomości obydwu metodyk, konieczne jest tutaj krótkie przybliżenie samego standardu i jego podstawowych założeń w celu lepszego zrozumienia zaproponowanego rozwiązania. Natomiast szczegółowe rozwinięcie wykorzystanych w pracy elementów standardu zostało przedstawione w rozdziale 4 ilustrującym sposób jego adaptacji do wymagań przemysłowych.

Model uzasadnionego zaufania (ang. Assurance) według standardu CC został przedstawiony na rysunku 1. Model zakłada, że standard CC jest źródłem technik kreowania zaufania, w których rygorystyczny, kontrolowany proces konstruowania, dokumentowania, testowania, wytwarzania, dostarczania, użytkowania i utrzymywania produktu w całym jego cyklu życia gwarantują, że stosowane zabezpieczenia są poprawne i wystarczające do tego, aby minimalizować ryzyko naruszenia chronionych zasobów produktu informatycznego [48]. W terminologii CC produkty informatyczne są określane jako przedmiot oceny (ang. Target of Evaluation, TOE).

Zaufanie do zabezpieczeń, implementowanych zgodnie z tymi technikami, jest natomiast potwierdzane i uzasadniane w toku procesu niezależnej oceny prowadzonej w akredytowanych i licencjonowanych laboratoriach z wykorzystaniem metodyki oceny CEM.



Rys. 1. Kreowanie uzasadnionego zaufania wg Common Criteria

Waga oceny określana jest za pomocą rygoryzmu definiowanego za pomocą poziomu uzasadnionego zaufania do oceny EAL. Czyli z jednej strony, konstruktor stosuje określone standardem techniki projektowania bezpiecznego produktu, a z drugiej strony, laboratorium

przeprowadza ocenę tego projektu według kryteriów metodyki CEM. Łącząc te dwa procesy w całość można uzyskać zaufanie, które jest uzasadnione, czyli stoją za tym racjonalne, potwierdzone niezależnymi testami i badaniami, przesłanki.

Standard Common Criteria składa się z 3 części. Pierwsza część, oznaczana dalej w pracy CC p.1 [1], zawiera wprowadzenie, opis modelu zarządzania ryzykiem i kreowania zaufania oraz struktur podstawowych dokumentów opracowywanych na potrzeby certyfikacji produktu [49]. Jednymi z podstawowych dokumentów w CC są: zadanie zabezpieczeń (ang. Security Target, ST), który zawiera specyfikację funkcji zabezpieczających dla konkretnej implementacji TOE oraz profil zabezpieczeń (ang. Protection Profile, PP), który zawiera zbiór wymagań bezpieczeństwa dla danego typu (rodziny) produktów IT, niezależny od sposobu implementacji.

Druga część, oznaczana CC p.2 [2], to zbiór wymagań funkcjonalnych na zabezpieczenia (ang. Security Functional Requirements, SFR) wykorzystywane do projektowania zabezpieczeń informatycznych i funkcji zabezpieczających (ang. Security Functions, SF). Natomiast trzecia część, oznaczana CC p.3 [3] zawiera wymagania na zapewnienie zaufania do oceny zabezpieczeń (ang. Security Assurance Requirements, SAR). Powyższe 3 części przeznaczone są m.in. dla projektantów produktów informatycznych, którzy deklarują poziom EAL dla swoich produktów.

Deklarowanym przez projektantów poziomom EAL odpowiadają zbiory komponentów SAR z normy CC p.3 pogrupowane w tzw. pakiety wymagań [50], [51], które pokazano w tabeli 18, rozdz. 4.4). W standardzie CC zdefiniowano 7 poziomów od EAL 1 do EAL 7. Poziomy EAL grupują wymagania SAR do oceny: zadania zabezpieczeń (ST), profilu zabezpieczeń (PP) dokumentacji użytkownika (ang. Guidance documents, AGD), dokumentacji projektowej (ang. Development, ADV), cyklu życia TOE (ang. Life-cycle support, ALC), testowania (ang. Tests, ATE) oraz analizy podatności (ang. Vulnerability assessment, AVA).

Wraz ze zwiększaniem się poziomu EAL następuje zwiększanie się rygoryzmu w stosowaniu procesów projektowania i oceny zabezpieczeń. Można to zilustrować na przykładzie jednego z wymagań, np. dotyczącego analizy podatności AVA (zob. rozdz. 5.3.3). Mianowicie, EAL 1 zapewnia podstawowy poziom zaufania, w którym analiza podatności ogranicza się tylko do wyszukiwania potencjalnych podatności TOE w publicznie dostępnych bazach podatności, np. CVE (ang. Common Vulnerabilities and Exposure) [52]. Natomiast już EAL 3 wymaga, aby analiza podatności wykazała odporność TOE na ataki penetracyjne o podstawowym potencjale ataku (ang. Basic attack potential), a z kolei poziom EAL 4 wymaga wykazania jeszcze wyższej odporności TOE, a mianowicie na podwyższony potencjał ataku (ang. Enhanced-Basic attack potential).

Należy zrozumieć, że poziom EAL nie jest miarą poziomu bezpieczeństwa produktu, który jest oceniany. Poziom EAL jest miarą określającą, jak szczegółowo i z jakim rygoryzmem oceniane są zabezpieczenia tego produktu. Dlatego też wyższy poziom EAL niekoniecznie oznacza, że produkt jest bardziej bezpieczny, ale oznacza zwiększone zaufanie to tego, że produkt i jego zabezpieczenia zadziałają prawidłowo, ponieważ zostały dokładniej przetestowane i ocenione.

Standard CC uzupełniony został przez dokument w postaci metodyki CEM, który służy do oceny czy wymagania bezpieczeństwa zostały prawidłowo zaimplementowane w TOE. Metodyka CEM [5] wprowadza pojęcie tzw. jednostki oceny (ang. Work Unit, WU), która jest synonimem elementarnej czynności, inaczej działania (ang. Action), wykonywanego przez osobę oceniającą w celu wydania werdyktu, czy dane wymaganie CC jest spełnione przez produkt. Osoba oceniająca, którą jest pracownik laboratorium o odpowiednich kompetencjach technicznych, nazywana także często ewaluatorem (ang. Evaluator), może wydawać 3 rodzaje werdyktów: pozytywny (ang. Pass) dla spełnionego wymagania, negatywny (ang. Fail) dla wymagania niespełnionego i nierozstrzygnięty (ang. Inconclusive) w sytuacjach, gdy dowody są niewystarczające do wydania jednoznacznej oceny.

Do tej pory, zgodnie z metodyką CC, oceniono i certyfikowano łącznie ponad 5 tys. różnego typu produktów [53], m.in. procesory i karty inteligentne, zapory sieciowe, systemy operacyjne, bazy danych, urządzenia do podpisu elektronicznego, czujniki biometryczne opisane w artykule [54], czujniki inteligentne [55], [56], tachografy. Jednakże brakuje wśród nich takich produktów, jak np. komponenty systemów IACS, które nie są typowymi produktami informatycznymi, ale mają z nimi wiele cech wspólnych z powodu stosowania do ich budowy typowych podzespołów elektronicznych i oprogramowania.

Standard CC nie jest używany do urządzeń przemysłowych, świadczą o tym takie publikacje, jak ta dotycząca bezpieczeństwa sieci przemysłowych [57], w której autor zaznacza, że CC stosowane są głównie w branży IT. Przeważają publikacje, które sugerują możliwość zastosowania metodyki CC do rozwiązań przemysłowych, jak w artykule [58], ale bez wskazywania koncepcji podejścia do tego problemu. Jedynie programy europejskie takie, jak ERNCIP [41, p. 27], czy też prace agencji ENISA [9], wskazują lub rekomendują zastosowanie metodyki CC do systemów IACS. W artykule [59] zwracam uwagę na prace i wnioski grup ENISA i ERNCIP. Także w publikacji [60] (Table 14.3 List of standards applicable to ICS – Industrial Control Systems) wskazano CC jako standard, który można zastosować do przemysłowych systemów sterowania (ICS).

Widać zatem, że standard CC nie był do tej pory stosowany do urządzeń IACS, mimo że wielu autorów i grup badawczych wskazuje na możliwość jego zastosowania w tej branży. Pozostaje jednak pytanie, czy standard zbudowany jest w oparciu o strukturę, która umożliwia jego dostosowanie do specyficznych produktów lub technologii? Otóż analiza struktury

definiowania wymagań SAR i SFR oraz jednostek oceny WU, wskazuje, że są one zdefiniowane na tyle ogólnym poziomie, aby mogły być, po pierwsze stosowane do szerokiej gamy produktów IT, a po drugie, posiadają możliwość uszczegółowiania parametrów definicji w celu dopasowania ich do konkretnej implementacji produktu.

Standard nakazuje konstruktorom oraz oceniającym stosowanie literalnie zdefiniowanych w CC wymagań. Przede wszystkim w normie podano strukturę budowy wymagań SFR (CC p.2, sec. 7.1.3 SFR component structure), wymagań SAR (CC p.3, sec. 7.1.3 Assurance Component Structure) i jednostek oceny WU (CEM, sec. 7.4 Relationship between CC and CEM structures, sec. 8.2.5 Evaluator verdicts). W trakcie tworzenia własnych komponentów należy je tworzyć dokładnie według przedstawionych struktur.

Jednocześnie dopuszcza się sytuacje, w których nie mogąc dobrać ze standardu odpowiednich wymagań, można te wymagania niejako „dopasować" do potrzeb. Jednakże musi się to odbywać według ściśle określonych reguł. Dopasowanie to odbywa się za pomocą dopuszczalnych w standardzie 4 możliwych operacji na komponentach wymagań:

- Iteracja (ang. Iteration) – pozwala na użycie komponentu więcej niż jeden raz z różnymi wartościami parametrów;
- Przypisanie (ang. Assignment) – pozwala podstawienie wartości dla parametru;
- Selekcja (ang. Selection) – pozwala na wybór jednej lub więcej opcji z listy wyboru dla parametru;
- Uszczegółowienie (ang. Refinement) – umożliwia dodanie szczegółów do wymagania, bez zmiany jego oryginalnego brzmienia.

W przypadku braku możliwości dostosowania wymagania za pomocą operacji, można utworzyć własny komponent dodatkowy, zwany także rozszerzonym (ang. Extended), pamiętając o konieczności stosowania tej samej struktury, jak dla pozostałych komponentów w standardzie. Komponenty rozszerzone dają konstruktorom i oceniającym dużo większe możliwości zastosowania specyficznych wymagań wynikających z typu danego urządzenia. Jednakże wiąże się to z większym nakładem pracy, gdyż taki komponent należy utworzyć od podstaw, a w przypadku komponentów dodatkowych SAR należy także utworzyć skojarzone z nimi jednostki oceny WU.

Norma CC przedstawia sposób tworzenia dodatkowych komponentów w CC p.1, w rozdz. 8.3 oraz aneksie C.4. Ponadto w normie CC p.3 w rozdziale 12.5 „Extended component definition" zawarto wymagania dotyczące oceny komponentów dodatkowych, które należy wykazać w zadaniu zabezpieczeń (ST).

Ponadto jest jeszcze wiele innych dokumentów towarzyszących, które wspierają standard CC w kwestii definiowania komponentów dodatkowych. Między innymi raport techniczny ISO/IEC TR 15446 [61] dotyczący opracowywania zadania zabezpieczeń (ST) oraz profilu zabezpieczeń (PP) przedstawia sposób tworzenia komponentów dodatkowych SAR i zwraca

uwagę na konieczność utworzenia dla nich dodatkowo jednostek oceny dla CEM. W aneksie A do tego samego raportu przedstawiono przykłady komponentów dodatkowych SFR, które można użyć jako wzorcowe podczas tworzenia własnych komponentów rozszerzających katalog wymagań SFR. Ponadto w specjalnym poradniku dla ewaluatorów [62] opisano sposób, w jaki nowe definicje komponentów rozszerzonych będą oceniane przez ewaluatorów, co także stanowi cenne źródło wskazówek podczas opracowywania tych komponentów.

Podsumowując, dotychczas standard CC nie był wykorzystywany do oceny rozwiązań IACS, a jedynie różne źródła i programy badawcze wskazują na taką możliwość.

Standard mimo bardzo restrykcyjnych zasad stosowania pozostawia pewien margines możliwości dostosowania wymagań do specyficznych produktów lub technologii za pomocą dozwolonych operacji na komponentach lub możliwości tworzenia własnych komponentów dodatkowych.

Ponadto, na podstawie własnego, już 20 letniego doświadczenia w pracy nad standardem CC [63], mogę wysnuć wniosek, że standard CC wraz z metodyką CEM mają możliwości dostosowania ich do nowego zakresu wymagań specyficznych dla urządzeń IACS.

Dlatego też, w rozprawie zajmę się sposobem rozwiązania problemu badawczego w oparciu o standard CC i metodykę oceny CEM, modyfikując je w dopuszczalnym zakresie do wymagań i potrzeb specyficznych dla komponentów przemysłowych.

Problem jest ambitny, jednakże zgodnie z metodyką CD&E oraz rekomendacją grupy tematycznej ERNCIP [42, p. 40], wykorzystując i doskonaląc stosowane już w praktyce rozwiązania, jest możliwy do zrealizowania w ramach doktoratu.

Kolejny rozdział rozprawy przedstawia analizę problemu w kontekście określenia przemysłowych wymagań bezpieczeństwa, które będą stanowić dane wejściowe do opracowania dodatkowych lub uszczegółowionych komponentów wymagań SFR i SAR.

3. Badanie potrzeb i wymagań bezpieczeństwa IACS

Rozdział przedstawia analizę problemu badawczego w kontekście określenia potrzeb i wymagań dotyczących bezpieczeństwa przemysłowych urządzeń systemów automatyki i sterowania, wynikających z coraz częstszych ataków, pojawiających się nowych podatności i zagrożeń z nimi związanych. Do określenia wymagań bezpieczeństwa dla systemów IACS, czyli realizacji celu szczegółowego C1, wykorzystano metodę analizy i krytyki piśmiennictwa.

Wykonano badanie wybranych standardów i metod, które zawierają opisy środków ochrony urządzeń przed zagrożeniami, opisy wymagań bezpieczeństwa i zabezpieczeń w celu zmniejszania podatności. Badanie źródeł wymagań miało na celu ustalenie, które z nich mogą stać się materiałem wejściowym i wskazać potencjalny kierunek adaptacji wymagań CC do potrzeb metody oceny bezpieczeństwa.

3.1. Zasoby, zagrożenia i podatności

Międzynarodowe Towarzystwo ds. Automatyzacji ISA (ang. International Society of Automation) [64], które opracowało rodzinę norm IEC 62443, założyło w 2019 r. tzw. Globalny Sojusz Cyberbezpieczeństwa ISA (ang. ISA Global Cybersecuriy Alliance, ISAGCA) [65] w celu promowania działań na rzecz poprawy cyberbezpieczeństwa w automatyce przemysłowej i systemach sterowania. W tym celu ISAGCA prowadzi oficjalny blog [66], w którym porusza m.in. takie zagadnienia, jak analiza ryzyka, badania zgodności cyberbezpieczeństwa przemysłowego, a także udostępnia treści edukacyjne. W jednym z ostatnich wpisów bloga zatytułowanym „Why are cyberattack shifting to ICS?” [67], co można przetłumaczyć „Dlaczego cyberataki przenoszą się do przemysłowych systemów sterowania?”, autorka podaje przyczyny coraz częstszych ataków kierowanych na systemy sterujące elementami infrastruktur, często krytycznych, takich jak: wodociągi, sieci elektroenergetyczne, rafinerie, czy też transport.

Po pierwsze, wiele z tych systemów z racji swojego wieku, a większość z tych systemów została wdrożona nawet ponad dwie dekady temu, zanim jeszcze cyberataki stały się znaczącym zagrożeniem, posiada jedynie proste zabezpieczenia, łatwe do obejścia przez współczesnych hakerów.

Po drugie, celem ataków jest perspektywa uzyskania znacznego zysku ze względu na krytyczne i cenne zasoby, które są pod kontrolą systemów sterowania. Autorka podaje tu przykład niedawnego ataku z 2021 r. na Rurociąg Kolonialny (ang. Colonial Pipeline) [68], biegnący wzdłuż wschodniego wybrzeża Stanów Zjednoczonych. Rurociąg jest wyjątkowo ważny, gdyż zapewnia prawie połowę rocznego zapotrzebowania w produkty naftowe od Teksasu, aż do New Jersey. Atakujący, za pomocą skompromitowanego hasła do sieci VPN, wykradli ok. 100 GB danych firmowych i zażądali za ich zwrot okupu. Władze firmy

zdecydowały o zamknięciu ropociągu na 6 dni, aby zapobiec dalszemu rozprzestrzenianiu się zagrożenia w sieci firmowej, co spowodowało czasowe wstrzymanie dostaw wzdłuż wschodniego wybrzeża. Skutki tej decyzji szybko się rozprzestrzeniły. Linie lotnicze zostały zamknięte z powodu niedoboru paliwa, natomiast stacje benzynowe, mimo że wciąż działały, to i tak miały trudności z zaspokojeniem popytu z powodu natłoku klientów, którzy w panice zaczęli masowo wykupywać paliwo na zapas.

W końcu władze firmy zapłaciły hakerom okup w wysokości 4.4 mln dolarów, z których ostatecznie agencjom federalnym udało się odzyskać ponad połowę z tej sumy. Mimo że firma była mocno krytykowana za legitymizację wrogich działań hakerów, to pozostała przy swojej decyzji mając nadzieję, że skróci to czas przywrócenia ciągłości działania firmy.

Takich przypadków znamy wiele, ale już tylko ten jeden świadczy o powadze zagrożeń i ich możliwych konsekwencjach, jeśli nie będą stosowane odpowiednio silne mechanizmy zabezpieczające. Dla zainteresowanych wymieniam tutaj skrótowo kilka głośnych ataków z ostatnich lat, takich jak: Stuxnet (2008 r.) [69], BlackEnergy (2015 r.) [70], WannaCry (2017) [71], Log4j Apache (2021 r.) [72], czy też przykłady incydentów w publikacji [57, p. 36].

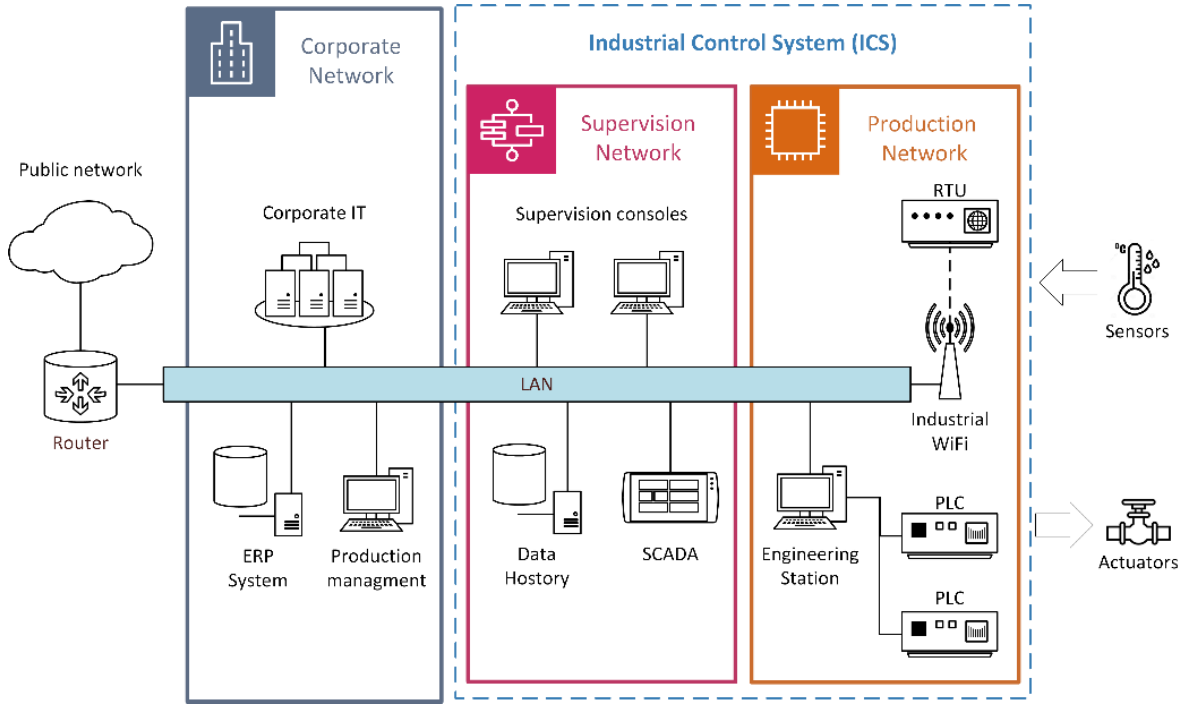
Z wielu podobnych przykładów wynika, że podstawową motywacją hakerów jest chęć zysku, czasem też sabotaż lub zwykła potrzeba rozgłosu. Jednak tym, co łączy je wszystkie, to wartość zasobów oraz ich krytyczność dla ciągłości działania gospodarek, firm, społeczeństw, czy nawet całych państw.

Dlatego też w kolejnej części rozdziału krótko przedstawię podstawowe elementy wchodzące w skład systemu IACS i ich zasoby, w tym krytyczne, a także możliwe podatności, które mogą być przyczyną utraty bądź naruszenia tych zasobów. Znając zasoby i ich lokalizację, a także możliwe luki bezpieczeństwa, jesteśmy w stanie zaproponować efektywne środki zabezpieczające, które z kolei są dokumentowane w standardach bezpieczeństwa, metodach, wytycznych, i które zostaną zidentyfikowane w dalszej części niniejszego rozdziału.

Wiele źródeł i dokumentacji systemów automatyki przemysłowej i sterowania podaje mniej lub bardziej skomplikowane modele struktur tych systemów. Wszystkie te modele można jednak sprowadzić do jednej, wspólnej dla wszystkich, wyjściowej struktury podstawowej, która może stanowić uogólniony model systemu sterowania. Taki przykład podstawowego schematu systemu ICS przedstawiono m.in. w publikacji [60], którego ilustrację pokazano na rys. 2 poniżej.

Model ten składa się z 2 zasadniczych warstw, warstwy sieci korporacyjnej (ang. Corporate network) oraz warstwy sieci ICS. Z kolei warstwa ICS składa się z części zawierającej systemy nadzoru (ang. Supervision network), takie jak SCADA lub bazy danych oraz część produkcyjną (ang. Production network), na którą składają się np. sterowniki PLC. Część produkcyjna steruje urządzeniami wykonawczymi, takimi jak zawory, serwomechanizmy, przekaźniki i odbiera dane z czujników, które umieszczane są w warstwie polowej (ang. Field

area). Z drugiej strony sieć firmowa połączona jest z Internetem, a ta z kolei połączona jest pośrednio z pozostałymi warstwami systemu ICS. Właśnie stąd bierze swój początek jedno z wielu źródeł zagrożeń, czyli połączenie sieci sterowania z siecią publiczną, przez którą mogą następować ataki.



Rys. 2. Przykład podstawowej struktury systemu sterowania [60]

Rysunek przedstawia kilka wybranych typów komponentów ICS stosowanych w sieciach sterowania. W praktyce, ich lista obejmuje pewne typy urządzeń [73] i ogranicza się do kilku podstawowych, z których następnie budowane są złożone i wielowarstwowe systemy sterowania, a są to:

- Sterowniki programowalne (PLC - Programmable Logic Controller);
- Zdalne terminale (RTU – Remote Terminal Unit);
- Inteligentne urządzenia elektroniczne (IED – Intelligent Electronic Device);
- Stacje robocze/inżynierskie (Work/Engineering Station);
- Panele operatorskie (HMI - Human Machine Interface);
- Bazy danych historycznych (Data Historian);
- Bramy komunikacyjne (Communications Gateway);
- Urządzenia polowe (Field devices) – czujniki, zawory, serwomechanizmy, przekaźniki.

Komponenty te posiadają swoje zasoby krytyczne, które definiuje się jako połączenie części składowej urządzenia (ang. Part) oraz atrybutu bezpieczeństwa przypisanego do tej części (ang. Security characteristics) [74].

W bezpieczeństwie IACS rozróżnia się 4 atrybuty bezpieczeństwa: dostępność (ang. Availability, Av), poufność (ang. Confidentiality, C), integralność (ang. Integrity, I), autentyczność (ang. Authenticity, Au). W normie IEC 62443-4-2 [12], powyższe atrybuty bezpieczeństwa definiuje się następująco:

- Dostępność (Av) – zapewnienie terminowego (w wymaganym czasie) i niezawodnego dostępu do informacji i funkcjonalności systemu sterowania oraz możliwości ich wykorzystania;
- Poufność (C) – zapewnienie, że informacja nie jest ujawniana nieuprawnionym podmiotom, procesom lub urządzeniom;
- Integralność (I) – zapewnienie wierności informacji (zachowania jej w niezmienionej postaci) i kompletności informacji;
- Autentyczność (Au) – zapewnienie, że podmiot lub proces jest tym, za kogo/co się podaje, poprzez uwierzytelnienie jego pochodzenia i weryfikację integralności.

Zasób krytyczny charakteryzuje się zatem poprzez wskazanie atrybutu bezpieczeństwa, który ma być zapewniony dla danej części urządzenia. Każdy zasób krytyczny narażony jest na zagrożenia, które mogą osłabiać jego atrybuty bezpieczeństwa.

W ramach jednego urządzenia może występować wiele zasobów krytycznych, które według [74] dzieli się dodatkowo na zasoby krytyczne tego urządzenia i zasoby krytyczne otoczenia, w którym to urządzenie działa.

Zasobami krytycznymi urządzenia nazywa się te jego części, które bezpośrednio realizują funkcje urządzenia, np. w sterowniku PLC może to być np. program użytkownika, który stanowi część cyfrową sterownika. W tym przykładzie można zdefiniować zasób krytyczny jako integralność programu użytkownika, czyli jako kombinację części urządzenia – program użytkownika i atrybutu bezpieczeństwa tej części, czyli integralność (I).

Zasobami krytycznymi otoczenia nazywa się zasoby, które są współdzielone, przechowywane lub przetwarzane przez urządzenie, ale pochodzą z zewnątrz, z jego otoczenia działania. Te zasoby to, np. dane pochodzące od użytkowników, aplikacji lub procesów współdziałających z produktem, np. dane uwierzytelniające dostępu do konfiguracji, konfiguracje połączeń (z adresami źródłowymi i docelowymi, protokołami, portami), których dostępność i integralności należy zapewnić. Na przykład może to być kanał wymiany danych ze stacją inżynierską, który obejmuje interfejs (np. kartę sieciową) i proces komunikacji użytkownika lub administratora bezpośrednio z urządzeniem w celu jego uruchomienia, zarządzania jego konfiguracją lub aktualizacji. W tym przypadku zachodzi potrzeba zapewnienia zasobowi następujących atrybutów bezpieczeństwa: poufności, integralności i autentyczności.

Przykładowe zasoby krytyczne sterownika RTU według profilu zabezpieczeń opracowanego przez grupę ERNCIP [21] wraz z ich atrybutami bezpieczeństwa, prezentuje tabela 1 odpowiednio dla zasobów krytycznych otoczenia i zasobów TOE.

Tabela 1. Krytyczne zasoby urządzenia IACS - przykład

Atrybuty bezpieczeństwa / Elementy	**Av**	**C**	**I**	**Au**
Elementy otoczenia				
1. Interfejs konsoli poleceń procesu	X		X	X
2. Dane uwierzytelniające dostępu do konfiguracji urządzenia	X	X	X	X
3. Dane wymieniane pomiędzy TOE i interfejsem nadzoru	X	X	X	X
4. Dane wymienianie pomiędzy TOE a innym RTU		X	X	X
Elementy TOE				
5. System operacyjny			X	X
6. Oprogramowanie wbudowane		X	X	X
7. Konfiguracja		X	X	X
8. Mechanizm uwierzytelniania użytkownika			X	X
9. Dane poufne użytkownika		X	X	
10. Polityka kontroli dostępu			X	
11. Lokalne dzienniki zdarzeń			X	X

Na początku tego rozdziału wskazano zagrożenia dla systemów IACS, które dotyczą pozyskania lub naruszenia zasobów krytycznych. Ułatwieniem dla zadziałania zagrożeń są potencjalne podatności występujące w systemach IACS. Dlatego też, w kolejnej części rozdziału przedstawiam źródła podatności oraz możliwe sposoby ich niwelowania. Jest to ważne, ponieważ znajomość przyczyn zagrożeń i podatności przekłada się z kolei na zakres prac wielu instytucji, które starają się sformalizować zapis odpowiednich zabezpieczeń, opracowując standardy i wytyczne bezpieczeństwa dla integratorów systemów IACS. Wyniki tych prac będą stanowić źródło wymagań bezpieczeństwa charakterystycznych dla IACS, które zostaną wykorzystane do adaptacji standardu CC.

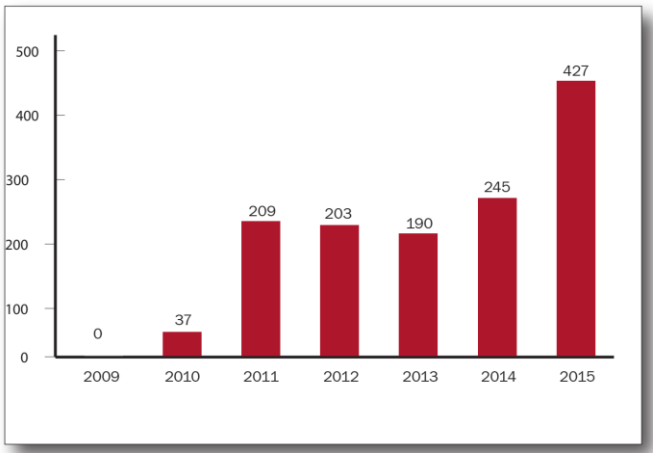
Wagę problemu występowania podatności podkreślają m.in. raporty izraelskiej firmy CyberX [75]. W 2017 r. firma wykonała analizę ryzyka sieci z użyciem autorskich algorytmów analizy ruchu sieciowego (ang. Network Traffic Analysis, NTA) oraz głębokiej analizy pakietów (ang. Deep Packet Inspection, DPI). Łącznie poddano analizie 375 sieci w różnych sektorach przemysłu w USA, Europie i krajach rejonu Azji i Pacyfiku. Badaniem objęto m.in. takie sektory, jak: energetyczny, instytucje użytku publicznego, przemysł farmaceutyczny, chemiczny oraz paliwowy. W raporcie końcowym wykazano następujące główne podatności sieci sterowania w ujęciu procentowym:

- 82% było narażonych na ataki poprzez niezabezpieczone protokoły;

- 76% posiada przestarzałe i nieaktualizowane systemy operacyjne;
- 59% sieci używa haseł przesyłanych jawnym tekstem;
- 50% nie używa oprogramowania antywirusowego na stacjach roboczych;
- 44% posiada co najmniej jedno nieautoryzowane lub nieznane urządzenie;
- 32% sieci przemysłowych jest podłączonych do Internetu;
- 28% wszystkich urządzeń w każdej z sieci zostało ocenionych jako podatne na ataki
- 20% posiadało co najmniej jeden, niekontrolowany punkt dostępowy sieci WiFi;
- 10% sieci ciągle było zainfekowanych złośliwym oprogramowaniem;

Podobne analizy zostały wykonane w latach 2019 i 2020, które wykazały, że wciąż 71% przemysłowych stacji roboczych posiada nieaktualne systemy operacyjne, a 66% nie posiada automatycznej aktualizacji oprogramowania antywirusowego.

Podobne badania wykonał amerykański ICS-CERT (ang. Industrial Control Systems – Cyber Emergency Response Team) dla narodowej agencji cyberbezpieczeństwa [76], w których wykazuje wciąż rosnącą liczbę zgłaszanych podatności (rys. 3).



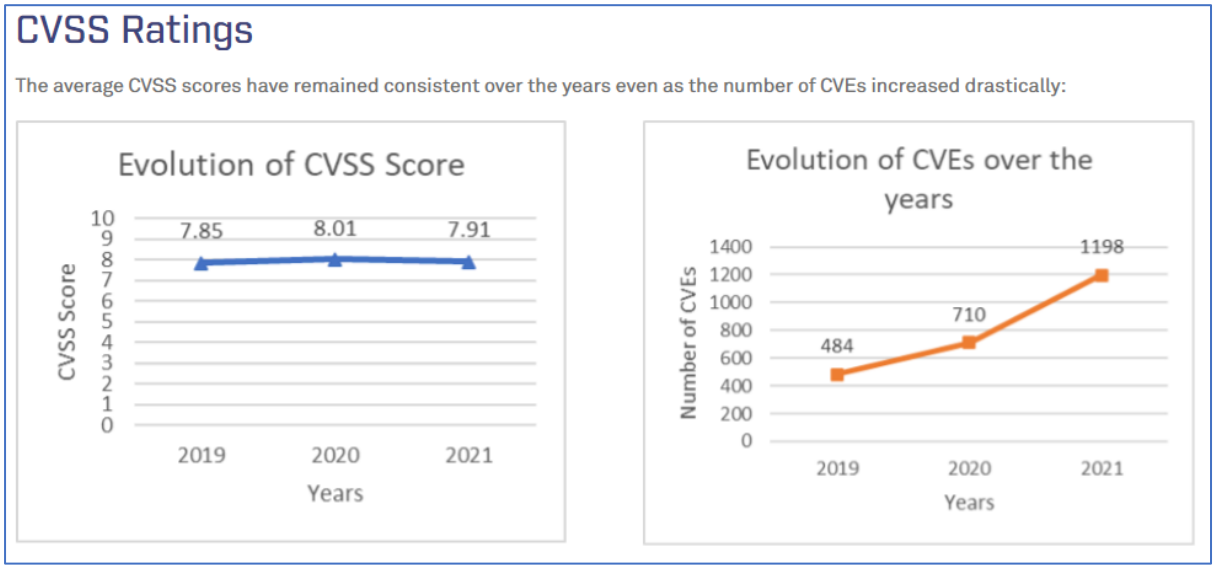
Rys. 3. Liczba zgłaszanych podatności do ICS_CERT, 2009 - 2015

ICS-CERT, w raporcie rocznym z 2015 r. [77], zidentyfikował 6 głównych obszarów występowania podatności:

- Ochrona brzegowa sieci: ryzyko braku detekcji nieautoryzowanej aktywności w systemach krytycznych, słaba separacja pomiędzy sieciami ICS i przedsiębiorstwa;
- Najmniejsza, niezbędna funkcjonalność – dodatkowe, niepotrzebne funkcje zwiększające ryzyko poszerzonego wektora ataku;
- Identyfikacja i uwierzytelnianie – zwiększone ryzyko braku rozliczalności i śledzenia działań użytkowników, utrudnione zabezpieczanie kont zwalnianych użytkowników;
- Fizyczna kontrola dostępu – nieautoryzowany dostęp do urządzeń wykonawczych;
- Audyt, analiza i raportowanie – brak sformalizowanego przeglądu i weryfikacji rejestrów (logów) utrudnia wykrycie ukrytych, nieautoryzowanych użytkowników lub aplikacji;

- Zarządzanie danymi uwierzytelniającymi – ryzyko użycia niezabezpieczonych haseł, skompromitowane hasła mogą zostać użyte do udzielenia zaufanego nieautoryzowanego dostępu do systemów sterowania.

Z kolei grupa doradców bezpieczeństwa VERVE [78] w raporcie „2021 ICS Advisory Report" [79] przedstawiła podsumowanie dotyczące wagi i liczby zgłoszonych podatności na podstawie danych z ICS-CERT oraz z baz podatności CVE i CVSS [80] (ang. Common Vulnerabilities Scoring System).



Rys. 4. Waga i liczba zgłaszanych podatności systemów ICS, raport [79]

Skala oceny podatności CVSS zawiera 5 wskaźników jakościowych z przypisami im przedziałami liczbowymi, które oblicza się wg wzoru zawartego w specyfikacji CVSS (CVSS v3.1 Equations) [81]. Wskaźniki określają wagę podatności jako: żadna (ang. None) – 0.0; niska (ang. Low) – 0.1 – 3.9; średnia (ang. Medium) – 4.0 – 6.9; wysoka (ang. High) – 7.0 – 8.9; krytyczna (ang. Critical) – 9.0 – 10.0.

Rys. 4 pokazuje, że w ostatnich latach waga podatności utrzymywała się na stałym wysokim poziomie (ang. High), a liczba zgłaszanych podatności wzrosła ponad dwukrotnie w ciągu 2 lat.

Z kolei autorzy monografii dotyczącej cyberbezpieczeństwa ICS [82] oraz artykułu opisującego kluczowe podatności dla systemów IACS [83] przedstawiają główne obszary, dla których wymieniono źródła potencjalnych podatności w tabeli 2:

Tabela 2. Obszary i źródła podatności systemów IACS

	Obszary występowania podatności			
	Zarządzanie politykami i procedurami bezpieczeństwa	**Platformy sprzętowo-programowe i oprogramowanie**	**Konfiguracja sieci**	**Protokoły komunikacyjne**
Przyczyny podatności	**Słabe** zarządzanie politykami bezpieczeństwa dla IACS **Nieadekwatna** implementacja zabezpieczeń **Brak** spójności w planach awaryjnych **Zarządzanie** zmianą specyficznych konfiguracji IACS **Błędy** w zarządzaniu, niedokładny audyt, brak planów awaryjnych	**Nieaktualny** sprzęt i oprogramowanie **Używanie** domyślnych ustawień **Błędy** konfiguracji w zdalnym dostępie **Brak** kopii awaryjnych **Słabe** uwierzytelnianie na poziomie sprzętowym i programowym **Słabe** zabezpieczenia przed złośliwym oprogramowaniem **Błędna** konfiguracja systemu operacyjnego **Źle** zaprojektowane oprogramowanie	**Źle** zaprojektowana sieć **Brak** zapisanej konfiguracji sieci lub brak kopii zapasowej **Złe** zarządzanie hasłami sieciowymi **Używanie** niezabezpieczonych portów fizycznych **Brak** lub źle skonfigurowane zapory ogniowe **Ustawienia** sieci sterowania nieodpowiadające wymaganiom IACS **Brak** monitorowania ruchu sieciowego **Używanie** standardowych protokołów takich jak, Telnet, FTP bez mechanizmów szyfrowania **Brak** sprawdzania integralności (np. niedozwolone urządzenia) **Brak** szyfrowania do ochrony danych przesyłanych bezprzewodowo	**Brak** uwierzytelniania pakietów **Brak** szyfrowania pakietów **Ataki** DoS **Przepełnienie** bufora **Ataki** typu Man-in-the-Middle

W celu zapobiegania i minimalizowania występowaniu podatności proponuje się środki zaradcze w postaci zabezpieczeń fizycznych, proceduralnych lub osobowych. Sposoby zapobiegania podatnościom dla ułatwienia pogrupowano w grupy tematyczne, tak jak to pokazuje tabela 3 poniżej.

Tabela 3. Wytyczne bezpieczeństwa minimalizujące podatności dla IACS

1. Polityki i procedury	**2. Bezpieczna komunikacja**
- cele, zakres i czas obowiązywania - odpowiedzialności w zakresie bezpieczeństwa dla każdej roli i użytkownika - urządzenia z zainstalowanym oprogramowaniem i funkcjami - architektura sieci, zapory ogniowe i zasady - użytkownicy, role i kontrola dostępu - plan aktualizacji sprzętu i oprogramowania - plan kopii awaryjnych i odzyskiwania danych - plany szkoleń z bezpieczeństwa	- stosowanie VPN - identyfikacja urządzeń, użytkowników i protokołów - monitorowanie zasad sieciowych - szyfrowanie - bezpieczne protokoły: SFTP, SSL, IPSEC
3. Zapory ogniowe	**4. Kontrola dostępu**
- instalacja i konfiguracja zapory	- role i uprawnienia - użytkownicy i silne hasła

5. Audyt bezpieczeństwa	**6. Monitorowanie**
- przegląd i ocena zabezpieczeń, procedur i środków bezpieczeństwa - raporty z audytu: mocne i słabe strony i rekomendacje	- analiza obszarów podatności - definiowanie podstawowych wzorców ruchu sieciowego - analiza i rejestrowanie ruchu sieciowego - alarmowanie o odstępstwach
7. Konfiguracja sieci	**8. Złośliwe oprogramowanie**
- poprawna implementacja i konfiguracja - stosowanie DMS - segmentacja sieci: IACS, firmowej, publicznej	- stosowanie systemów antywirusowych - procedura aktualizacji sygnatur - procesy analizy oprogramowania - określenie czasu odpowiedzi dla krytycznych urządzeń - alarmowanie o wykryciu złośliwego oprogramowania

Celem niniejszego rozdziału, począwszy od wskazania rosnącej liczby ataków na systemy IACS, poprzez zagrożenia wykorzystujące podatności tych systemów, było nie tylko podkreślenie powagi problemu zapewnienia bezpieczeństwa, ale identyfikacja przykładowych środków ochrony – technicznych, proceduralnych lub osobowych.

W związku z tym, że takich źródeł z wytycznymi bezpieczeństwa jest wiele, to pojawia się problem, w jaki sposób wybierać do stosowania te najbardziej miarodajne i efektywne, które mogą być niejako dokumentami wzorcowymi. Najlepiej, gdyby zalecenia miały sformalizowaną postać, np. były uznanymi międzynarodowymi standardami. Prace w kierunku formalizacji wymagań bezpieczeństwa dla IACS także są prowadzone, a ich rezultatem są dokumentacja standardów, metodyk i narzędzi, które zostaną omówione w kolejnym rozdziale.

3.2. Standardy i metody oceny bezpieczeństwa

Przykłady raportów o podatnościach wskazują na wagę problemu, który został zauważony przez instytucje normalizujące, twórców programów certyfikacji i oceny, a także laboratoria oceniające. Dzięki temu opracowano wiele standardów i poradników bezpieczeństwa dla systemów przemysłowych [9], [10], [84], a wśród nich najczęściej wymienia się następujące:

- IEC 62443 – rodzina standardów dotycząca bezpieczeństwa IACS, składająca się z 4 części: 1) definicje, metryki; 2) wymagania na zarządzanie bezpieczeństwem i procesami w przedsiębiorstwie, 3) wymagania techniczne na bezpieczeństwo systemów, 4) wymagania techniczne na bezpieczeństwo komponentów systemu, która składa się z dwóch oddzielnych dokumentów:
  - IEC 62443-4-1 [11], który specyfikuje wymagania dla tworzenia bezpiecznego produktu w całym jego cyklu życia,
  - IEC 62443-4-2 [12], który określa wymagania techniczne dla komponentów systemów IACS;
- IEEE 1686 [13] – standard dla inteligentnych urządzeń elektronicznych (ang. Intelligent Electronic Devices - IED Cyber Security Capabilities), który określa

wymagania na funkcjonalność urządzeń w celu wspierania programów ochrony infrastruktury krytycznej;

- SP 800-82 – NIST (National Institute of Standards and Technology) Special Publication [19] – dokument niemający statusu normy, który zawiera wytyczne dla bezpieczeństwa IACS (ang. Guide to Industrial Control Systems Security); dokument opisuje, m.in.: główne źródła zagrożeń i podatności dla PLC, RTU, SCADA oraz proponuje stosowanie konkretnych środków zabezpieczających.

W artykule [85], opisującym problemy i wyzwania bezpieczeństwa IACS, zwrócono uwagę na standard IEC 62443 opracowany przez komitet ISA99. Podkreślono w nim, że standard jako wywodzący się ze standardu do zarządzania bezpieczeństwem informacji (ang. Information Security Management System, ISMS), zdefiniowany w rodzinie norm ISO/IEC 27000 [86], nie jest dostosowany do stosowania w sieciach przemysłowych (ang. Operational Technology, OT) ze względu na to, że nie przystaje do potrzeb specyficznych dla sieci przemysłowych.

Kolejne aktualizacje standardu IEC co raz lepiej odpowiadały potrzebom bezpieczeństwa IACS, co widać po wynikach analiz w publikacji [60], która w przeglądzie metodyk i standardów możliwych do zastosowania w systemach przemysłowych, wskazuje na normę IEC 62443 jako już dojrzały standard do stosowania w bezpieczeństwie przemysłowym.

Także grupa robocza ERNCIP, w projekcie badawczym [41], zwróciła uwagę na fakt stosowania standardu IEC 62443 w metodyce oceny bezpieczeństwa dla urządzeń wbudowanych (ang. Embedded Device Secure Assurance, EDSA), która jest stosowana w autorskim programie certyfikacji „ISASecure Certification Programme.

W artykule [58] opisany został m.in. program certyfikacji „Achilles" autorstwa General Electric (ang. Achilles Communication Certification, ACC), który jest stosowany do badania odporności sieci i protokołów komunikacyjnych.

Z kolei niemiecka firma TeleTrust opracowała metodę oceny urządzeń przemysłowych [87] w ramach lekkiego programu certyfikacji, zgodną z normami IEC 62443-4-1 i IEC 62443-4-2, które potraktowała jako główne źródło wymagań technicznych zastosowanych w metodzie. Grupa badawcza ERNCIP oceniła w raporcie [21], że metoda TeleTrust jest zgodna z opracowaną strukturą zadania zabezpieczeń dla sterownika PLC, a analiza podatności wykonywana jest zgodnie z metodyką oceny CEM.

W celu dokonania wyboru standardu, który mógłby stanowić źródło wymagań do rozwinięcia metodyki CC, przyjęto następujące kryteria oceny:

- ISO/IEC – oznacza, że dokument ma status normy międzynarodowej;
- IT security – oznacza, że wymagania dotyczą bezpieczeństwa IT;
- CC – oznacza, że struktura definiowania wymagań jest podobna do tej dla komponentów SFR i SAR w standardzie CC;

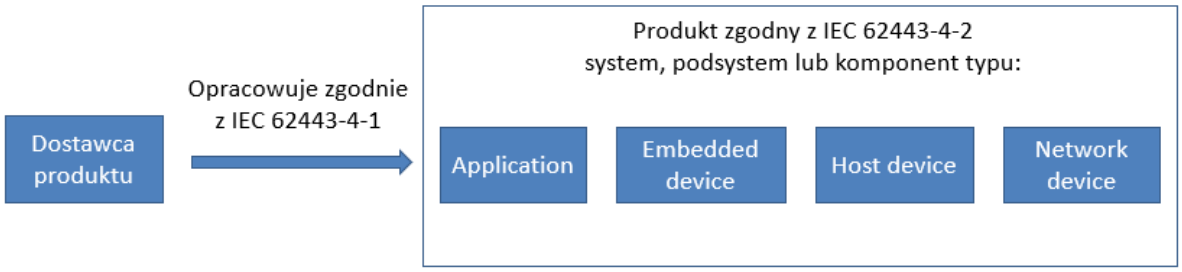
- ERNCIP – oznacza, że grupa badawcza ERNCIP rekomenduje dane rozwiązanie;
- ITSEF – oznacza, że laboratorium ITSEF Łukasiewicz – EMAG posiada już znajomość i doświadczenie w stosowaniu danego rozwiązania.

Tabela 4. Ocena rozwiązań przemysłowych do dalszego stosowania

Kryterium / Dokument	ISO/IEC	IT security	CC	ERNCIP/CSA	ITSEF
IEC 62443	X	X	X	X	X
NIST SP 800-82		X		X	
IEEE 1686	X	X			
EDSA		X		X	
ACC		X		X	
TeleTrust		X	X	X	X

Biorąc pod uwagę argumenty przytaczane w licznych publikacjach oraz na podstawie oceny omawianych rozwiązań, najlepszymi kandydatami do wykorzystania w kolejnych etapach badań okazały się normy IEC 62443-4-1 i IEC 62443-4-2. Wykorzystany zostanie także sposób szacowania potencjału ataku w metodzie TeleTrust stosowany podczas analizy podatności danego urządzenia. Znaczenie ma także fakt, że w ramach realizacji projektu CyberBEAM laboratorium ITSEF zdobyło wiedzę i doświadczenie w zakresie stosowania standardu IEC 62443. Ponadto dodatkowym argumentem świadczącym na korzyść wybranych standardów może być ich podobieństwo strukturalne do metodyki Common Criteria, co zostanie dodatkowo szczegółowo wykazane w rozdziale 4 niniejszej rozprawy.

Podsumowując, norma IEC 62443-4-1 określa wymagania na procesy wytwarzania bezpiecznego produktu w całym jego cyklu życia. Innymi słowy są to wymagania, których zastosowanie w procesie produkcyjnym gwarantuje, że z kolei wymagania techniczne IEC 62443-4-2 zostaną zaimplementowane w produkcie poprawnie, czyli utrzymana zostanie odpowiednia jakość produktu końcowego, co zilustrowano na rys. 5.



Rys. 5. Komplementarność norm IEC 62443-4-1 i IEC 62443-4-2

W kolejnym rozdziale krótko opisano najważniejsze cechy obu norm, które mają istotny wpływ na dalszy tok badań w pracy doktorskiej.

3.3. Wymagania techniczne i cyklu życia

Norma IEC 62443-4-1 zawiera wymagania wytwarzania bezpiecznego produktu w całym jego cyklu życia. Cykl życia definiuje następujące etapy: definiowanie wymagań bezpieczeństwa, projektowanie, implementacja, weryfikacja i walidacja, zarządzanie usterkami bezpieczeństwa, zarządzanie aktualizacjami i poprawkami, koniec cyklu życia produktu.

Wymagania na procesy wytwarzania bezpiecznego produktu zebrano w ośmiu Praktykach (ang. Practices):

- Praktyka 1. Zarządzanie bezpieczeństwem (ang. Security management, SM);
- Praktyka 2. Specyfikacja wymagań bezpieczeństwa (ang. Specification of security requirements, SR);
- Praktyka 3. Bezpieczeństwo na etapie projektowania (ang. Security by design, SD);
- Praktyka 4. Bezpieczna implementacja (ang. Secure implementation, SI);
- Praktyka 5. Weryfikacja bezpieczeństwa i testowanie (ang. Security verification and validation testing, SVV);
- Praktyka 6. Zarządzanie usterkami bezpieczeństwa (ang. Management of security-related issues, DM);
- Praktyka 7. Zarządzanie aktualizacjami bezpieczeństwa (ang. Security update management, SUM)
- Praktyka 8. Wytyczne bezpieczeństwa (ang. Security guidelines, SG).

Szczegółowe wymagania dla każdej z praktyk zawierają tabele 36 i 37 (załącznik 1).

Norma IEC 62443-4-1 mówi jeszcze o poziomach dojrzałości procesów (ang. Maturity level, ML). Poziomy ML są stosowane w celu wsparcia producenta w ocenie gotowości procesów organizacji do wytwarzania bezpiecznego produktu. Dzięki wykonanej ocenie możliwe jest np. wykrycie, że organizacja nie jest przygotowana do implementacji wszystkich procesów na tym samym poziomie dojrzałości. Informacja taka może pomóc producentowi na wdrożenie działań doskonalących w celu poprawy jakości wytwarzanych produktów.

Należy podkreślić, że wymagania praktyk określają podobny zakres wymagań do klasy wymagań ALC (ang. Life-cycle suport) z normy CC, która zawiera wymagania na środowisko rozwojowe produktu IT i zastosowany w nim cykl życia produktu, co zostanie wykorzystane podczas adaptacji wymagań CC.

Norma IEC 62443-4-2 definiuje siedem technicznych wymagań fundamentalnych (ang. Foundational Requirements, FR).

- FR 1. Identyfikacja i uwierzytelnianie (IAC, Identification and Authentication Control),
- FR 2. Kontrola użycia (UC, Use Control),
- FR 3. Integralność systemów (SI, System Integrity),

- FR 4. Poufność danych (DC, Data Confidentiality),
- FR 5. Kontrolowany przepływ danych (RDF, Restricted Data Flow),
- FR 6. Terminowa odpowiedź na zdarzenia (TRE, Timely Response to Events)
- FR 7. Dostępność zasobów (RA, Resource Availability).

Każde wymaganie FR zawiera kilka lub kilkanaście wymagań dla komponentu IACS, oznaczanych w skrócie CR (ang. Component requirement). Wymagania CR mogą zawierać rozszerzenia (ang. Requirement Enhancement, RE), które zawierają dodatkowe wymagania względem podstawowego CR, i które są wymagane na wyższych poziomach bezpieczeństwa SL (ang. Security Level). Kombinacja wymagań CR i rozszerzonych wymagań REs określa możliwy do osiągnięcia poziom SL, jak we fragmencie normy pokazanej w tabeli 5.

Tabela 5. Mapowanie wymagań CR na poziomy SL [12]

Component requirements (CRs) and Requirements Enhancements (REs)	**SL 1**	**SL 2**	**SL 3**	**SL 4**
FR 1 – Identification and authentication control (IAC)				
CR 1.1 – Human user identification and authentication	X	X	X	X
RE (1) Unique identification and authentication		X	X	X
RE (2) Multifactor authentication for all interfaces			X	X
CR 1.2 – Software process and device identification and authentication		X	X	X
RE (1) Unique identification and authentication			X	X

Standard IEC 62443-4-2 określa wymagania bezpieczeństwa dla komponentów IACS na danym poziomie SL. Jeśli komponent spełnia dane wymaganie, to oznacza, że jeżeli zostanie prawidłowo skonfigurowany i zaimplementowany w systemie IACS, to może osiągnąć poziom bezpieczeństwa SL bez stosowania żadnych dodatkowych, wspomagających środków bezpieczeństwa.

Wymagania normy przeznaczone dla ogółu komponentów IACS, w tym także dla sterowników PLC, oznaczane są w skrócie CR. Norma zawiera także zestawy wymagań przeznaczonych dla urządzeń określonego typu i rodzaju zastosowania, takich jak: urządzenia wbudowane (ED, Embedded Device), urządzenia sieciowe (ND, Network Device), urządzenia typu host (HD, Host Device) i oprogramowanie (SA, Software Application). Takie wymagania umieszczono w oddzielnych rozdziałach standardu i oznaczono je skrótami angielskimi od typów tych komponentów, np. NDR 1.6 oznacza wymaganie nr 6 w ramach FR 1 dla urządzenia Network Device.

W wyniku przeprowadzonej analizy określono podstawowe zagrożenia i podatności systemów IACS. Wynikają z tego konkretne potrzeby ochrony systemów w postaci wymagań bezpieczeństwa. Wykonano przegląd dostępnych norm, metod i narzędzi, i wytypowano normy przemysłowe IEC 62443-4-1 i IEC 62443-4-2 oraz metodę TeleTrust jako materiał wejściowy do kolejnego etapu badań, którego celem jest adaptacja standardu CC do przemysłowych wymagań bezpieczeństwa.

4. Adaptacja wymagań bezpieczeństwa CC

Rozdział przedstawia analizę problemu w kontekście możliwości adaptacji wymagań standardu CC do zastosowania dla urządzeń IACS oraz adaptacji metodyki CEM do oceny tych wymagań. W rozdziale zaprezentowano rezultaty adaptacji w postaci docelowych zbiorów wymagań, które będą stosowane w metodzie oceny bezpieczeństwa urządzeń IACS. W wyniku tych prac zrealizowano cel szczegółowy C2.

Do rozwiązania niniejszego zagadnienia wykorzystano metody heurystyczne – metodę porównań i metodę krytycznej analizy i oceny. Metody umożliwiły odkrycie nowych faktów dotyczących związków zachodzących pomiędzy standardami przemysłowym IEC i CC oraz pomiędzy metodyką CEM i normą CC p.4. Metoda porównań wskazała kierunki i warianty adaptacji wymagań normy CC do wymagań przemysłowych.

Z kolei za pomocą metody analizy i konstrukcji logicznej wykonano analizę budowy komponentów dodatkowych w normie CC oraz jednostek oceny w CEM, a także analizę wymagań fundamentalnych FR oraz Praktyk w normach IEC. Następnie wykonano syntezę struktur komponentów z obydwu standardów w nową całość w postaci nowych, zmodyfikowanych wymagań CC i jednostek oceny uwzględniających wymagania norm IEC 62443-4-1 i IEC 62443-4-2.

4.1. Porównanie standardów CC i IEC

Metoda heurystyczna pozwoliła na dojście do nowego rozwiązania poprzez odkrycie nowych faktów dotyczących związków zachodzących pomiędzy standardami IEC i CC oraz pomiędzy metodyką oceny CEM i najnowszą normą CC p.4 [17], która służy do opracowywania metod oceny dla specyficznych urządzeń lub technologii.

W pierwszym kroku zastosowano metodę porównań do standardów IEC 62443-4-1 i IEC 62443-4-2 oraz CC p.2 i CC p.3. Elementami wyjściowymi porównania są normy CC, dla których normy przemysłowe IEC będą stanowić źródło ulepszeń. Płaszczyzna porównawcza została scharakteryzowana za pomocą następujących czynników porównania:

- Charakterystyka urządzenia – określa, czy norma uwzględnia dokument opisujący rodzaj urządzenia i jego podstawową charakterystykę bezpieczeństwa;
- Wymagania bezpieczeństwa – określa, czy norma posiada zbiory sformalizowanych wymagań na funkcjonalność zabezpieczeń i oceny zabezpieczeń;
- Wymagania na testowanie – określa, czy norma posiada zapisy dotyczące warunków i wymagań dotyczących testowania funkcji bezpieczeństwa,
- Wymagania na analizę podatności – określa, czy norma posiada wymagania dotyczące sposobu analizy i szacowania podatności.

Czynniki uwzględnione w porównaniu oraz jego wyniki przedstawia tabela 6.

Tabela 6. Porównanie standardów przemysłowych IEC z Common Criteria

Czynniki porównania	IEC 62443-4-1	IEC 62443-4-2	CC p.2	CC p.3
Charakterystyka urządzenia	Dokument opisujący kontekst użycia; Zasoby krytyczne; Model zagrożeń	Charakterystyka urządzenia za pomocą poziomu bezpieczeństwa Security Level (SL)	Końcowa specyfikacja TOE (TSS) wyrażona za pomocą SFRs	Zadanie zabezpieczeń ST; Definicja problemu bezpieczeństwa (SPD); Deklaracja zgodności TOE z poziomem EAL
Wymagania bezpieczeństwa	Praktyki 1 - 8 i wymagania dla cyklu życia produktu wraz z dokumentacją; Poziom dojrzałości procesów w organizacji ML	Wymagania techniczne fundamentalne FR 1 - 7 na funkcjonalność IACS dla różnych poziomów Security Levels (SL)	Wymagania na funkcjonalność zabezpieczeń SFR	Wymagania na uzasadnienie zaufania SAR na danym poziomie EAL; wymagania do oceny cyklu życia, testowania, dokumentacji użytkownika i projektowej
Wymagania na testowanie	Praktyka 5 – SVV Testowanie i weryfikacja wymagań bezpieczeństwa	NA	NA	Wymagania klasy ATE Testy
Wymagania na analizę podatności	Praktyka 5 - SVV-3 Testowanie podatności wykonywane przez producenta	NA	NA	AVA_VAN - analiza podatności wykonywana przez laboratorium

W wyniku porównania odkryto następujący fakt nr 1 stwierdzający, że obydwa standardy prezentują podobną logikę inżynierii bezpieczeństwa w swoim zakresie. Zostało to zaznaczone w tabeli tymi samymi kolorami dla odpowiednich par norm w ramach danych czynników porównania.

Okazało się, że prawie dla każdego czynnika porównawczego (oprócz wymagań na analizę podatności, co zostanie wyjaśnione dalej), każda para norm: IEC 62443-4-1 razem z CC p.3 oraz IEC 62443-4-2 razem z CC p.2 mają elementy wspólne. Można zatem zakładać, że dalszy kierunek doskonalenia norm CC będzie polegał na tym, że w ramach danego czynnika, norma CC w danej parze będzie doskonalona na podstawie odpowiadającej jej źródłowej normy IEC. W ten sposób otrzymujemy następujące kierunki doskonalenia:

- Norma CC p.3, zawierająca komponenty uzasadnionego zaufania SAR będzie doskonalona na podstawie cech charakterystycznych dla IACS zidentyfikowanych w normie IEC 62443-4-1 w następującym zakresie:

  - Charakterystyka urządzenia zostanie uzupełniona w dokumencie zadania zabezpieczeń ST (rozdz.4.2 Uzupełnienie zadania zabezpieczeń);
  - Wymagania SAR zostaną odpowiednio zmodyfikowane na podstawie analizy wymagań zawartych w Praktykach 1 – 8 (rodz. 4.4 Adaptacja wymagań SAR);
  - Wymagania klasy ATE do oceny testów zostaną uzupełnione na podstawie Praktyki 5 i wymagania SVV-3 (rozdz. rodz. 4.4 Adaptacja wymagań SAR);
  - Wymagania klasy AVA zostaną pozostawione bez zmian, ponieważ wymagania z normy IEC dotyczą badań podatności wykonywanych przez konstruktora, natomiast klasa AVA w CC dotyczy badań wykonywanych wyłącznie przez laboratorium; jedynym ulepszeniem, które zostanie zastosowanie, to możliwość wykorzystania wyników badań podatności wykonanych przez producenta w analizie podatności wykonywanej przez laboratorium; dodatkowe usprawnienie dotyczące analizy podatności zostało zastosowane w metodzie oceny w zakresie wykorzystania poziomów bezpieczeństwa SL (rozdz. 5.3.3 Analiza podatności).
- Norma CC p.2, zawierająca komponenty wymagań na funkcjonalność zabezpieczeń SFR, będzie doskonalona na podstawie cech charakterystycznych dla IACS zidentyfikowanych w normie IEC 62443-4-2 w następującym zakresie:
  - Charakterystyka urządzenia zostanie uzupełniona w zadaniu zabezpieczeń ST w części dotyczącej specyfikacji funkcji zabezpieczających (ang. TOE summary specification, TSS), które będą implementować dostosowane do IACS wymagania SFR (rozdz. 4.2 Uzupełnienie zadania zabezpieczeń);
  - Wymagania SFR zostaną odpowiednio zmodyfikowane na podstawie analizy wymagań fundamentalnych FR oraz z wykorzystaniem informacji o poziomie bezpieczeństwa SL dla wymagań FR (rozdz. 4.3 Adaptacja wymagań SFR).

W kolejnym kroku zastosowano metodę porównań dla metodyki oceny CEM i najnowszego wydania normy CC p.4. Potrzeba wykonania tego porównania wynikała z możliwości użycia wyników dostosowania CC w normie CC p.4. Dostosowanie CC wymusza wykonanie zmian w metodyce CEM, a te zmiany w postaci nowych jednostek oceny mogą być wykorzystane zgodnie z zaleceniami normy CC p.4 do opracowania w przyszłości kolejnych metod oceny dla IACS oraz do tworzenia tzw. Evaluation Activities (EAs), czyli działań oceniających, zawierających sposoby testowania funkcji bezpieczeństwa.

Elementem wyjściowym w tym porównaniu jest norma CC p.4, dla której zmiany w metodyce CEM stanowić będą źródło ewentualnych ulepszeń. Płaszczyzna porównawcza została scharakteryzowana za pomocą następujących czynników porównania:

- Działania oceniające dla urządzeń IACS – określa, czy jednostki oceny CEM (WU) mogą być dostosowane do oceny IACS;

- Metoda oceny dla urządzeń IACS – określa, czy norma dopuszcza tworzenie metod oceny przeznaczonych dla urządzeń IACS.

Powyższe czynniki zostały uwzględnione w porównaniu metodyki CEM i CC p.4, a wyniki porównania zostały przedstawione w tabeli 7.

Tabela 7. Porównanie metodyki oceny CEM z normą do tworzenia metod oceny CC p.4

Czynniki porównania	CEM	CC p.4
Działania oceniające dla urządzeń IACS	Uszczegółowienie jednostek oceny (Work Units, WUs) lub dodanie nowych dodatkowych WU_EXT na podstawie wymagań SAR dostosowanych do IACS	Evaluation activities (EAs), zgodnie z postanowieniami normy, muszą być opracowane na podstawie jednostek oceny wyprowadzonych (ang. derived) z CEM. W celu opracowania EAs dla IACS w pierwszej kolejności muszą zostać utworzone w CEM rozszerzone jednostki oceny WU_EXT dla IACS.
Metoda oceny dla urządzeń IACS	CEM umożliwia wykorzystanie rozszerzonych jednostek oceny WU_EXT dla IACS	Metody oceny grupują działania oceniające (EAs). EAs składają się z rozszerzonych WU_EXT. EAs można włączać do cPP dla IACS. EAs zawierają sposoby oceny SAR_EXT oraz sposoby testowania SFR_EXT.

W wyniku porównania, odkryto następujący fakt nr 2 stwierdzający, że nowa norma CC p.4 w pewnym określonym zakresie, zależnym od CEM, może być zastosowana do wykonywania ocen urządzeń IACS oraz do wspierania stosowania metodyki CEM. Generalnie, obydwie metodyki spełniają obydwa czynniki porównania, jednak z pewnymi różnicami.

Wyniki porównania wykazały, że dalszy kierunek doskonalenia i sposobu wykorzystania normy CC p.4 uwarunkowany jest wykonaniem w pierwszej kolejności dostosowania metodyki CEM. Dopiero w następnym kroku można zastosować normę do utworzenia następujących przyszłych wariantów rozwiązań w postaci metod oceny dla IACS:

- Opracowanie działań oceniających (EAs) dla urządzeń IACS na podstawie jednostek oceny utworzonych wcześniej w CEM;
- Uzupełnienie działań oceniających o sposoby oceny i testowania rozszerzonych wymagań SAR i SFR dla urządzenia IACS.
- Opracowanie metody oceny dla IACS, która grupuje działania oceniające (EAs), i która może stanowić integralną część wspólnego profilu zabezpieczeń cPP (ang. collaborative Protection Profile, cPP) dla IACS.

Podsumowując, fakt 2 dotyczący CC p.4 mówi, że norma umożliwia tworzenie dedykowanych metod dla specyficznych produktów poprzez przygotowanie odpowiednich działań oceniających wyprowadzonych z dostosowanych jednostek oceny CEM.

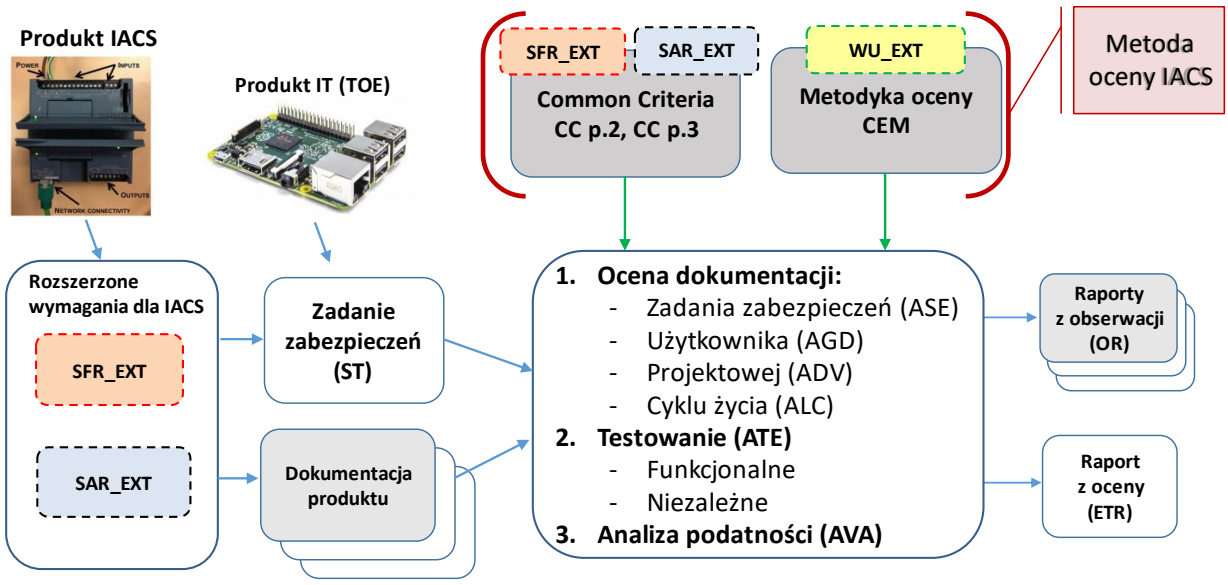
Ostatecznie, porównanie standardów i odkrycie związków pomiędzy nimi pozwoliło na odkrycie następujących faktów:

- Fakt 1 - standardy IEC i CC prezentują podobną logikę inżynierii bezpieczeństwa;
- Fakt 2 - norma CC p.4 może być zastosowana do tworzenia nowych metod oceny urządzeń IACS oraz wspiera stosowanie metodyki CEM.

Odkrycie tych faktów umożliwiło zaproponowanie dojścia do rozwiązania problemu badawczego w kontekście dostosowania normy CC za pomocą następujących kroków:

- uzupełnienie dokumentu zadania zabezpieczeń ST;
- adaptacja wymagań SFR na podstawie normy IEC 62443-4-2;
- adaptacja wymagań SAR na podstawie normy IEC 62443-4-1;
- adaptacja jednostek oceny CEM dla rozszerzonych komponentów SAR;
- opracowanie działań oceniających (EAs) dla rozszerzonych wymagań SFR,
- opracowanie metody oceny IACS implementującej powyższe rozwiązania.

W wyniku realizacji powyższych kroków otrzymamy rozwiązanie w postaci metody oceny IACS jako rozszerzenie standardu Common Criteria oraz metodyki oceny CEM, której umiejscowienie w modelu procesu oceny przedstawiono na rys. 6.



Rys. 6. Model procesu oceny IACS z wykorzystaniem zmodyfikowanej metodyki CC

Kolejny rozdział prezentuje pierwszy krok rozwiązania problemu dostosowania metodyki Common Criteria w postaci adaptacji dokumentu zadania zabezpieczeń.

4.2. Uzupełnienie zadania zabezpieczeń

W rozdziale zostanie przedstawiony kierunek doskonalenia dokumentu zadania zabezpieczeń (ST) na podstawie porównania z proponowanym przez ERNICP [21] wzorcem zadania zabezpieczeń dla sterownika.

Uzupełnienie dokument ST jest niezbędne, aby podczas oceny produktu, ewaluator mógł zapoznać się i przygotować do zakresu oceny wynikającego z wymagań dotyczących urządzeń IACS. Zakres ten wynika z tego, jakie wymagania norm IEC 62443-4-1 i IEC 62443-4-2 zadeklarował producent podczas implementacji produktu oraz jakie jego zasoby krytyczne i zasoby środowiska zdefiniował w modelu zagrożeń.

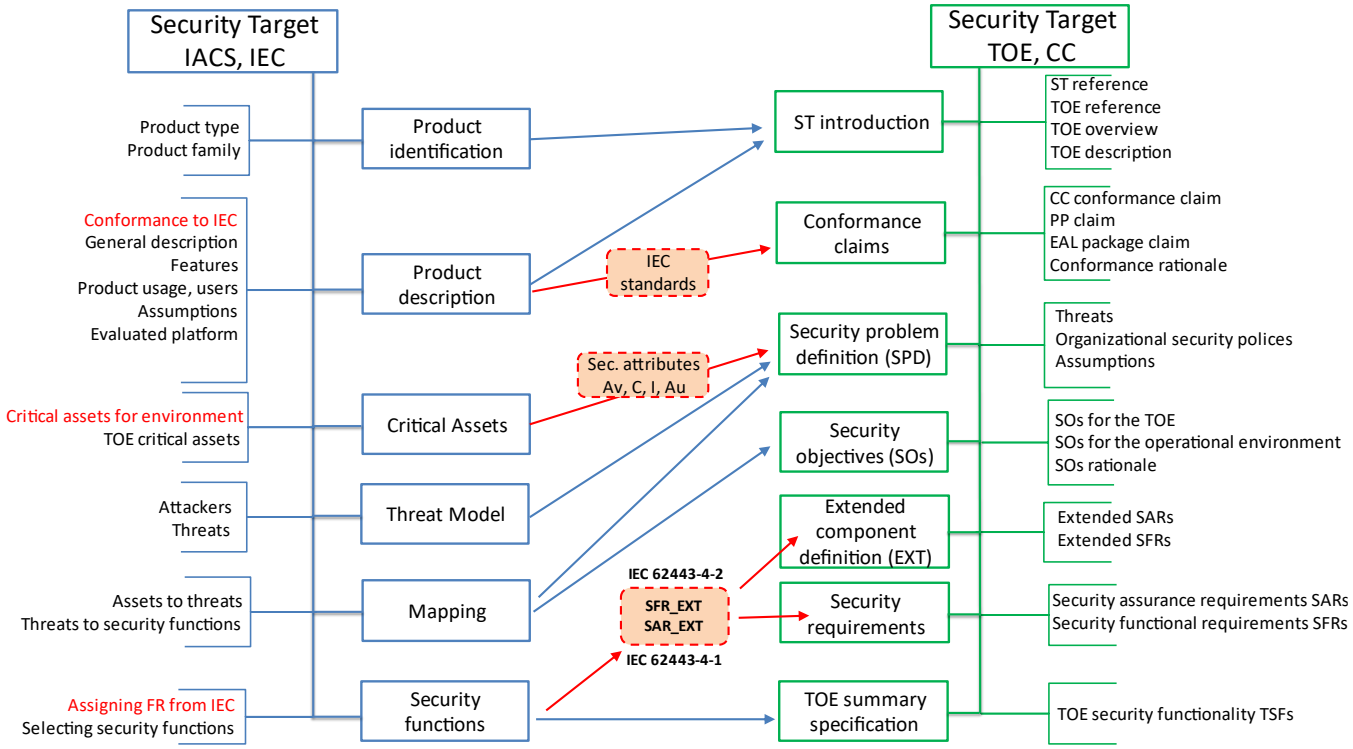
Z punktu widzenia ewaluatora są to informacje ułatwiające wykonanie oceny dokumentu ST i samego urządzenia IACS. Dzięki nim, podczas oceny ST z użyciem opracowanej metody, ewaluator uwzględni deklarację konstruktora o użyciu specyficznych wymagań technicznych z norm IEC. Ewaluator jednocześnie będzie przygotowany na to, że w sekcji dokumentu ST zawierającej wymagania bezpieczeństwa SFR i SAR znajdą się komponenty wymagań CC dostosowane do IACS na bazie wskazanych przez producenta standardów technicznych. Dzięki temu ewaluator przygotuje zestaw wymagań do oceny wraz z tabelami mapującymi, które zawierają jednostki oceny WU dla IACS, stosowane do wydawania werdyktów.

Na początku w zwięzły sposób zostaną opisane struktury obydwu dokumentów, a szczegóły zostaną pokazane w tabeli porównania, w dalszej części rozdziału.

W standardzie CC zadanie zabezpieczeń (ST) jest podstawowym dokumentem charakteryzującym TOE przeznaczone do oceny, który jest opracowywany przez producenta produktu [1]. Dokument ST zawiera opis i analizę bezpieczeństwa produktu w kontekście jego użycia w przewidywanym środowisku operacyjnym. ST może być konstruowany na bazie profilu zabezpieczeń (PP), który definiuje wymagania dla danego typu produktu, np. firewall, a wtedy ST przedstawia konkretną implementację urządzenia danego producenta.

Strukturę zadania zabezpieczeń wraz z opisem zawartości poszczególnych rozdziałów przedstawia rys. 7. Dokument zawiera opis problemu bezpieczeństwa (SPD), czyli m.in. specyfikuje zagrożenia, polityki bezpieczeństwa i założenia dla środowiska operacyjnego. Następnie ST podaje sposób rozwiązania tego problemu za pomocą celów zabezpieczeń dla produktu i jego środowiska operacyjnego. Dalej cele są wyrażane są za pomocą komponentów wymagań na funkcjonalność zabezpieczeń SFR z normy CC p.2, a następnie są one implementowane w postaci funkcji zabezpieczających TOE (ang. TOE Security functionality, TSF). Funkcje TSF są przedstawione w sekcji ST zawierającej podsumowanie specyfikacji TOE (ang. TOE summary specification). Specyfikacja prezentuje, w jaki sposób funkcje TSF zostały zaimplementowane, aby spełniały wymagania SFR, które z kolei zostały dobrane do zaproponowanych celów zabezpieczeń.

Funkcje TSF można opracowywać na różnym poziomie uzasadnionego zaufania (EAL), stąd dla każdego produktu poziom ten jest deklarowany w ST. Poziomy EAL określane są przez pakiety komponentów uzasadnionego zaufania. Szczegółowy opis poziomów EAL oraz ich interpretacja znajdują się w rozdz. 4.4 Adaptacja wymagań SAR.



Rys. 7. Porównanie struktur zadań zabezpieczeń dla IACS i TOE

Rysunek 7 powyżej przedstawia także strukturę zadania zabezpieczeń dla sterownika. Dokument zawiera rozdziały, w których znajdują się, m.in. takie informacje jak: typ produktu (np. konkretny sterownik danej firmy) i rodzina produktu (np. sterowniki, RTU, HMI); opis produktu z kontekstem użycia, czyli przewidywanego środowiska pracy; zasoby krytyczne dla produktu i otoczenia; model zagrożeń, opisujący zagrożenia dla zasobów krytycznych; mapowanie zagrożeń do zasobów oraz mapowanie funkcji zabezpieczających przeciwstawiających się zagrożeniom; funkcje bezpieczeństwa, które implementują wymagania podstawowe (FR) z normy IEC 62443-4-2.

Metoda porównania dwóch wzorców pozwoliła wskazać, jakie informacje dodatkowe powinny uzupełnić docelowy dokument zadania zabezpieczeń.

Elementem wyjściowym porównania jest zatem ST, dokumentem źródłowym jest dokument szablonu zadania zabezpieczeń sterownika, czynniki porównania będą dotyczyć wymaganej zawartości rozdziałów obydwu porównywanych dokumentów. Celem porównania jest identyfikacja specyficznych cech opisu IACS, które powinny zostać włączone do ST. Wyniki porównania przedstawiono w tabeli 8.

Tabela 8. Wyniki porównania zadań zabezpieczeń IACS i CC

Czynniki porównania	**Zadanie zabezpieczeń IACS**		**Zadanie zabezpieczeń CC**	
	Oryginalny tytuł rozdziału	Treść rozdziału	Oryginalny tytuł rozdziału	Treść rozdziału
Deklaracja zgodności z normami	Product identification	Typ produktu, konfiguracja produktu przeznaczona do oceny. Deklaracja norm: IEC 62443-4-1, IEC 62443-4-2 Deklaracja Security Level (SL)	Conformance claim	Deklaracja zgodności z normami CC CC p.1, p.2, p.3, CEM, z profilami zabezpieczeń PP, cPP, EAL
Kontekst użycia TOE	Product description	Ogólny opis urządzenia, funkcje, sposób użycia, użytkownicy, założenia dotyczące środowiska eksploatacji, oceniania platforma	ST introduction	Referencje do dokumentu ST, jednoznaczne oznaczenie wersji i konfiguracji TOE podlegającej ocenie, przegląd TOE i jego środowiska eksploatacji, zakres logiczny i fizyczny
Zasoby TOE	Critical assets	Opis zasobów krytycznych TOE i zasobów krytycznych środowiska z przypisanymi atrybutami Av, C, I, Au	Security problem definition	Definicja problemu bezpieczeństwa (SPD) opisuje zagrożenia, założenia na środowisko, polityki bezpieczeństwa, opisuje zasoby w kontekście zidentyfikowanych zagrożeń, nie identyfikuje zasobów krytycznych środowiska, stosuje atrybuty.
Model zagrożeń	Threat model	Model zagrożeń opisuje atakujących atrybuty bezpieczeństwa zasobów krytycznych w sposób półformalny, tu jeszcze nie są wskazywane cele zabezpieczeń.	Security problem definition	SPD definiuje półformalnie zagrożenia i wskazuje cele zabezpieczeń dla TOE i środowiska, które się im przeciwstawiają
	Mapping	Przedstawia mapowanie zagrożeń do zasobów krytycznych i ich atrybutów.		
Cele zabezpieczeń przeciw zagrożeniom	Mapping	Przedstawia mapowanie zagrożeń do zasobów krytycznych i ich atrybutów. Mapuje funkcje bezpieczeństwa wyrażone za pomocą wymagań fundamentalnych FR (IEC 62443-4-2) na zagrożenia w celu weryfikacji pokrycia zagrożeń.	Security objectives	Rozdział definiuje cele zabezpieczeń dla TOE i środowiska, które przeciwstawiają się zidentyfikowanym zagrożeniom. Zawiera mapowanie celów na zagrożenia, założenia i polityki bezpieczeństwa.
Wymagania norm	Security Functions	Zawiera specyfikację funkcji zabezpieczających wyrażonych za pomocą wymagań fundamentalnych FR z normy IEC 62443-4-2 na danym poziomie SL. Proces implementacji funkcji zabezpieczających ma być zgodny z wybranymi w deklaracji zgodności Praktykami normy IEC 62443-4-1.	Security requirements	Rozdział zawiera specyfikację wymagań SFR z CC p.2, które realizują cele zabezpieczeń. Wskazany jest także pakiet komponentów SAR z danego EAL.
			Extended component definition (EXT)	Rozdział zawiera specyfikację dodatkowych komponentów spoza normy CC, a włączonych do oceny TOE
Funkcje zabezpieczeń	Security Functions	Zawiera specyfikację funkcji zabezpieczających wyrażonych za pomocą wymagań fundamentalnych FR z normy IEC 62443-4-2 na danym poziomie SL.	TOE summary specification	Rozdział zawiera listę funkcji zabezpieczających TSF, które implementują wymagania SFR wynikające ze zdefiniowanych celów zabezpieczeń.

W wyniku porównania wyciągnięto następujące wnioski:

- Wszystkie czynniki porównania dotyczące treści zadania zabezpieczeń są uwzględniane w obydwu dokumentach;
- Rozdziały obydwu dokumentów zawierają zbliżone opisy, co zostało zaznaczone tymi samymi kolorami; istnieją różnice w nazewnictwie rozdziałów, np. ST dla IACS zawiera rozdziały „Critical assets", „Threats" „Mapping", które co do treści opowiadają jednemu rozdziałowi „Security problem definition" ze wzorca ST normy CC;
- Zidentyfikowano treści charakterystyczne dla IACS:
    - Deklaracja zgodności ze standardami przemysłowymi IEC 62443-4-1 i IEC 62443-4-2 oraz poziomem bezpieczeństwa SL – informacja o zgodności powinna uzupełnić rozdział „Conformance claims";
    - Definicja zasobów krytycznych środowiska włącznie z atrybutami bezpieczeństwa – informacja powinna znaleźć się w rozdziale „Security problem definition";
    - Zadeklarowany przez producenta zakres wymagań FR z normy IEC 62443-4-2 oraz zakres stosowanych Praktyk z normy IEC 62443-4-1 powinien być uwzględniony w rozdziałach „Security requirements" i „Extended component definition".

Wykonane porównanie struktur i zawartości zadania zabezpieczeń dla IACS z zadaniem zabezpieczeń CC umożliwiło wprowadzenie dodatkowych informacji charakterystycznych dla IACS, które ułatwią prowadzenie oceny bezpieczeństwa dla IACS.

Wynik porównania został zaznaczony na rys. 7, gdzie czerwoną czcionką zaznaczono informacje, które uzupełnią ST, natomiast czerwone strzałki wskazują ich miejsca docelowe w wynikowym zadaniu zabezpieczeń normy CC.

Dzięki uzupełnionemu ST, podczas oceny urządzenia IACS, ewaluator uwzględni deklarację konstruktora o użyciu specyficznych wymagań technicznych FR i Praktyk z normy IEC za pomocą odpowiednich rozszerzeń rodzin klasy ASE. Ewaluator będzie miał także wiedzę o zasobach krytycznych IACS i funkcjach zabezpieczających zbudowanych z użyciem wymagań FR. Wymagania FR z kolei będą wyrażone w postaci zmodyfikowanych komponentów SFR w sekcji „Security requirements".

Tak uzupełniony dokument zadania zabezpieczeń zobowiązuje konstruktora do wykazania, które wymagania przemysłowe zastosowano w produkcie, natomiast oceniającemu pozwala przygotować odpowiednie zestawy dostosowanych wymagań SAR i SFR do oceny produktu.

Kolejny rozdział omawia sposób, w jaki utworzono zestawy komponentów SFR uwzględniających wymagania normy IEC 62443-4-2.

4.3. Adaptacja wymagań SFR

Niniejszy rozdział przedstawia sposób adaptacji wymagań SFR z normy CC p.2 do specyficznych wymagań bezpieczeństwa IACS. Funkcje bezpieczeństwa określane wymaganiami normy IEC 62443-4-2 będą podlegały ocenie według normy CC, dlatego też konieczne jest wyrażenie tych funkcji za pomocą odpowiednio zmodyfikowanych komponentów SFR.

Do utworzenia zmodyfikowanych komponentów SFR została wykorzystania metoda analizy i konstrukcji logicznej wspomagana metodą porównań. Pierwszy etap analizy polegał na poznaniu budowy i struktury wymagań oraz wykonaniu wstępnego mapowania standardów w celu wyznaczenia par wymagań do porównań. W etapie porównań analizowana była treść wymagań w celu identyfikacji cech charakterystycznych dla IACS. W ostatnim etapie następowała synteza cech w zmodyfikowane, wyjściowe wymaganie SFR.

Proces tworzenia nowych i udoskonalonych wymagań SFR został zrealizowany w następujących krokach:

1. Analiza budowy komponentu CR;
2. Analiza budowy komponentu SFR;
3. Mapowanie wstępne wymagań CR i SFR;
4. Realizacja porównań komponentów CR i SFR:
    a. Selekcja elementu CR;
    b. Ustalenie elementu wyjściowego SFR;
    c. Czynnik porównania – cechy charakterystyczne dla IACS;
    d. Identyfikacja cechy IACS jako źródła uzupełnienia dla SFR.
5. Synteza wymagania SFR i cechy IACS do jednej z poniższych postaci:
    a. SFR oryginalny – niezmieniony komponent SFR zmapowany do wymagania CR w przypadku pełnego pokrywania się obszaru wymagań;
    b. SFR [*refinement*, *assignment*] – dostosowany SFR za pomocą jednej z dozwolonych operacji: uszczegółowienia lub przypisania w przypadku, gdy treści wymagań częściowo się pokrywają, a także w przypadku wymagania CR na wyższych poziomach SL;
    c. SFR_EXT – dodatkowy SFR w przypadku, gdy wymaganie CR nie ma swojego odpowiednika SFR lub SFR nie może być dostosowany za pomocą dozwolonych operacji uszczegółowienia lub przypisania;
6. Utworzenie działań oceniających EA (ang. Evaluation Activities) dla wszystkich zmapowanych i zmodyfikowanych komponentów SFR na podstawie planów testów źródłowego wymagania CR, zastosowanych w ocenie pilotażowej urządzenia IACS.
7. Utworzenie wynikowych tabel mapujących wymagania CR i SFR.

Każdy z tych kroków opisano szczegółowo poniżej.

1. Analiza budowy komponentu CR

Opis podstawowej struktury wymagań normy IEC 62443-4-2 w postaci wymagań FR, CR oraz poziomów bezpieczeństwa zostały już przedstawione w rozdz. 3.3, dlatego w tym miejscu zostanie od razu pokazana szczegółowa struktura komponentu CR na przykładzie komponentu oznaczonego symbolem CR 1.7.

Konwencja zapisów komponentów w normie IEC 62443-4-2 jest następująca:
SL # - poziom bezpieczeństwa # (gdzie # przyjmuje wartość całkowitą od 1 do 4)
FR X – wymaganie fundamentalne nr X (X występuje w zakresie od 1 do 7)
CR X.Y – wymaganie nr Y w ramach wymagania fundamentalnego FR X

Przykłady zapisu dla przykładowego komponentu:
SL 1 – poziom bezpieczeństwa 1
FR 1 – Identification and authentication control (IAC) – nazwa wymagania FR
CR 1.7 Strength of password-based authentication – nazwa wymagania CR
wymaganie nr 7 w ramach FR 1 na poziomie SL 1

Tabela mapowania komponentu i jego uszczegółowień do poziomów SL wygląda następująco (na podstawie tabeli B.1 z normy IEC 62443-4-2).

Tabela 9. Mapowanie wymagania CR 1.7 na poziomy SL

	CRs and REs	SL 1	SL 2	SL 3	SL 4
FR 1 - Identification and authentication control					
CR 1.7 - Strength of password-based authentication		V	V	V	V
	RE (1) Password generation and lifetime restrictions for human users			V	V
	RE (2) Password lifetime restrictions for all users (human, software process, or device)				V

Komponent CR 1.7 wymaga stosowania uwierzytelniania za pomocą silnych haseł i składa się z wymagania bazowego, które obowiązuje od najniższego poziomu SL 1 oraz dwóch możliwych uszczegółowień RE (1) i (2). Uszczegółowienie RE (1) narzuca dodatkowe wymaganie na czas ważności hasła dla użytkownika, aby wymusić okresową zmianę hasła. Uszczegółowienie RE (2) określa okres ważności hasła, ale już nie tylko dla użytkowników, ale także dla procesów lub urządzeń.

Każdy komponent w dokumencie normy zdefiniowany jest za pomocą 4 sekcji:

1. Requirement – opisuje szczegółowo treść wymagania podstawowego;

2. Rationale and supplemental guidance – podaje uzasadnienie i wytyczne uzupełniające zawierające dodatkowe informacje ułatwiające implementację danego wymagania;
3. Requirement enhancements (REs) – zawiera uszczegółowienie wymagania poprzez dodanie kolejnych, bardziej restrykcyjnych sformułowań;
4. Security Levels – podaje kombinacje wymagania podstawowego i jego uszczegółowień wymaganych na danym poziomie SL w następujący sposób:
   a. SL 1: CR 1.7
   b. SL 2: CR 1.7
   c. SL 3: CR 1.7 (1)
   d. SL 4: CR 1.7 (1) (2)

Zapis z punktu c. oznacza, że komponent bazowy CR 1.7 łącznie z jego uszczegółowieniem RE (1) zapewniają poziom ochrony komponentu przemysłowego zgodnie z poziomem SL 3.

Takie same zapisy będą stosowane podczas porównań wymagań, a cechy charakterystyczne dla IACS będą wynikiem analizy sekcji opisujących wymaganie. Zgodnie z normą IEC 62443, poziomy SL oznaczają, że zabezpieczenia zaimplementowane w komponencie IACS zapewniają:

- SL 1 – ochronę przed przypadkowym naruszeniem;
- SL 2 – ochronę przed świadomym naruszeniem prostymi środkami, gdy sprawca dysponuje podstawowymi środkami, ma ogólne umiejętności i niską motywację;
- SL 3 – ochronę przed świadomym naruszeniem za pomocą zaawansowanych środków, gdy sprawca dysponuje średnimi zasobami, umiejętnościami specyficznymi dla IACS i przeciętną motywacją;
- SL 4 – ochronę przed świadomym naruszeniem za pomocą zaawansowanych środków, gdy sprawca dysponuje umiejętnościami specyficznymi dla IACS i wysoką motywacją.

Powyższe poziomy opisano tutaj w sposób jakościowy. Poziomy zostaną także opisane ilościowo, co zostanie pokazane i wykorzystane w rozdziale 5.3.3, dotyczącym analizy podatności w metodzie oceny IACS.

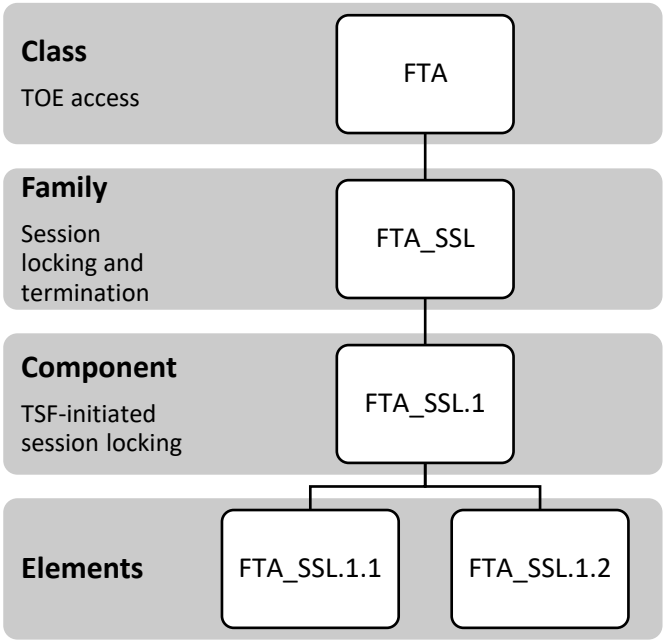
2. Analiza budowy komponentu SFR

Komponenty wymagań na funkcjonalność zabezpieczeń SFR (ang. Security functional requirements) zdefiniowane są w normie CC p.2 i określają wymagania, jakie muszą spełniać funkcje zabezpieczające implementowane w TOE. Norma zawiera 11 klas komponentów podzielonych na rodziny, natomiast rodziny zawierają komponenty wymagań. Tabela 10 przedstawia listę klas komponentów funkcjonalnych [88].

Tabela 10. Klasy komponentów SFR

Klasa	**Nazwa klasy**
FAU	Audyt bezpieczeństwa (ang. Security Audit)
FCO	Transmisja (ang. Communication)
FCS	Ochrona kryptograficzna (ang. Cryptographic Support)
FDP	Ochrona danych użytkownika (ang. User Data Protection)
FIA	Identyfikacja i uwierzytelnianie (ang. Identification and Authentication)
FMT	Zarządzanie bezpieczeństwem (ang. Security Management)
FPR	Prywatność (ang. Privacy)
FPT	Ochrona funkcji zabezpieczających (ang. Protection of the TSF)
FRU	Wykorzystanie zasobów (ang. Resource Utilization)
FTA	Dostęp do TOE (ang. TOE Access)
FTP	Wiarygodne ścieżki/kanały (ang. Trusted path/channels)

Każda z powyższych klas zawiera rodziny wymagań, a te z kolei zawierają komponenty wymagań podzielone na elementy. Poniższy rys. 8 przedstawia strukturę wymagań funkcjonalnych w normie na przykładzie klasy FTA – Dostęp do TOE.



Rys. 8. Przykładowa struktura wymagań funkcjonalnych w CC p.2

Podczas porównań brane będą pod uwagę komponenty wymagań wraz z ich elementami. Każdy komponent opisany jest w normie unikalną krótką nazwą, hierarchią do innych komponentów w ramach tej samej rodziny oraz listą elementów funkcjonalnych. Element

funkcjonalny definiowany jest jako najmniejsze możliwe wymaganie, którego dalszy podział nie przyniósłby znaczących rezultatów w implementacji.

Podany powyżej na rysunku 8 opis komponentu **FTA_SSL.1** „TSF-initiated session locking" i jego elementów w normie CC p.2 wygląda następująco.

Rodzina FTA_SSL jest jedną z sześciu rodzin klasy FTA – regulującej zasady dostępu do TOE, która dotyczy blokowania sesji użytkownika inicjowanej przez funkcję zabezpieczającą TSF po określonym czasie. Komponent posiada dwa elementy: FTA_SSL.1.1 oraz FTA_SSL.1.2 zdefiniowane następująco:

FTA_SSL.1.1 The TSF shall lock an interactive session after [assignment: *time interval of user inactivity*] by:
a) clearing or overwriting display devices, making the current contents unreadable;
b) disabling any activity of the user's data access/display devices other than unlocking the session.
FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [assignment: *events to occur*].

Element FTA_SSL.1.1 wymaga, aby funkcja TSF blokowała interaktywne sesje po określonym czasie braku aktywności ze strony użytkownika, przy czym wartość tego czasu ustalana jest za pomocą operacji przypisania [*assignment*] – jest to przykład adaptacji treści wymagania do określonej implementacji funkcji. Dalej czytamy, że TSF musi blokować sesje poprzez a) wyczyszczenie lub nadpisanie wyświetlanej treści, aby nie była czytelna i b) wyłączyć wszystkie aktywności urządzeń umożliwiających użytkownikowi dostęp do danych z wyjątkiem możliwości odblokowania sesji.

Element FTA_SSL.1.1 stwierdza, że funkcja TSF wymusza przed odblokowaniem sesji, aby wystąpiły określone zdarzenia, które także są ustalane za pomocą operacji [*assignment*].

Niniejszy przykład pokazuje możliwość wykorzystania jednej z możliwych operacji służących do dostosowania wymagania. Pozostałe operacje to: iteracja (ang. Iteration) – pozwala na użycie komponentu więcej niż jeden raz w dokumencie ST z różnymi wartościami parametrów; selekcja (ang. Selection) – pozwala na wybór jednej lub więcej opcji z listy wyboru dla parametru; uszczegółowienie (ang. Refinement) – umożliwia dodanie szczegółów do wymagania, bez zmiany jego oryginalnego brzmienia.

Operacje umożliwiają odpowiednie dopasowanie wymagania do szczególnych potrzeb danej implementacji TSF. W trakcie porównań wymagań CR i SFR może wystąpić sytuacja, w której żadnego z komponentów SFR nie będzie można dostosować za pomocą operacji. W takim przypadku, norma CC dopuszcza tworzenie komponentów dodatkowych oznaczanych przyrostkiem EXT. Norma CC przedstawia sposób tworzenia dodatkowych

komponentów w CC p.1, w rozdz. 8.3 oraz aneksie C.4. Komponenty dodatkowe muszą mieć strukturę zgodą z CC p.2. Na podstawie dokumentu cPP dla urządzeń sieciowych można przedstawić przykładowy komponent dodatkowy [89] następująco:

> **FTA_SSL_EXT.1** TSF-initiated session locking, requires system initiated locking of an interactive session after a specified period of inactivity. It is the only component of this family.
>
> **FTA_SSL_EXT.1.1** The TSF shall, for local interactive sessions, [selection:
> • *lock the session - disable any activity of the Administrator's data access/display devices other than unlocking the session, and requiring that the Administrator re-authenticate to the TSF prior to unlocking the session*;
> • *terminate the session*]
> after a Security Administrator-specified time period of inactivity.

Powyższy przykład pokazuje modyfikację wymagania za pomocą komponentu dodatkowego, który w tym wypadku uszczegóławia blokowanie sesji administratora bezpieczeństwa. Oryginalny komponent nie dawał takiej możliwości, ponieważ nie rozróżniał typów użytkowników. Dodatkowo komponent zawiera operację selekcji [selection]. W ten sposób, w przypadku braku wymagań w normie CC p.2, można utworzyć własne wymaganie, zgodnie ze strukturą wymaganą przez normę.

3. Mapowanie wstępne wymagań CR i SFR

W kolejnym kroku wykonano wstępne mapowanie wymagań fundamentalnych FR do klas funkcjonalnych. Mapowanie takie jest przydatne w celu wstępnego typowania obszarów poszukiwań odpowiadających sobie lub podobnych par wymagań CR – SFR. Typowanie jest wysokopoziomowe, ponieważ powstało na podstawie analizy opisów celów wymagań bez szczegółowej analizy treści poszczególnych komponentów CR i SFR (zob. Tabela 11).

Tabela 11. Wstępne mapowanie wymagań FR na klasy wymagań SFR

FR – Foundational Requirements IEC 62443-4-2	**SFR – Security Functional requirements ISO/IEC 15408-2**
FR 1 - Identification and authentication control (IAC), Identyfikacja i autoryzacja	**FIA**: Identification and authentication, Identyfikacja i uwierzytelnianie
FR 2 - Use control (UC), Kontrola użycia	**FAU**: Security audit - Audyt bezpieczeństwa **FRU**: Resource utilization - Usuwanie zasobów

FR 3 - System integrity (SI), Integralność systemów	**FIA**: Identification and authentication, Identyfikacja i uwierzytelnianie **FCO**: Communication, Komunikacja
FR 4 - Data confidentiality (DC) Poufność danych	**FDP**: User data protection, Ochrona danych użytkownika **FPR**: Privacy, Prywatność **FCS**: Cryptographic suport, Wsparcie kryptografii
FR 5 - Restricted data flow (RDF) Ograniczenie przepływu danych	**FTP**: Trusted paths/channels, Zaufane ścieżki/kanały **FCO**: Communication, Komunikacja
FR 6 – Timely response to events (TRE) Czasowa odpowiedź na zdarzenia	**FAU**: Security audit, Audyt bezpieczeństwa
FR 7 - Resource availability (RA) Dostępność zasobów	**FRU**: Resource utilization, Usuwanie zasobów

4. Realizacja porównań komponentów CR i SFR
5. Synteza wymagania SFR i cech IACS
6. Utworzenie działań oceniających EA

Kroki 4, 5 i 6 były realizowane z wykorzystaniem jednego arkusza Excel, dlatego ich wykonanie przebiegało jednocześnie i będą opisywane łącznie w tej sekcji pracy. Arkusz został wykazany w załączniku 1 w tabeli 39 i zawiera wybrane do porównania pary wymagań CR i SFR na podstawie wstępnej tabeli mapowania (realizacja kroku 4). Komponent SFR w danej parze stanowi element wyjściowy do doskonalenia na podstawie cech IACS zidentyfikowanych podczas analizy treści wymagania CR.

Zidentyfikowana cecha stanowi element doskonalenia wymagania SFR zgodnie z kolejnymi punktami kroku 5. Poniżej zostaną przedstawione rezultaty syntezy dostosowanego wymagania SFR na trzech przykładach ilustrujących każdy możliwy wynik syntezy.

Przykład 1 – mapowanie CR do oryginalnego wymagania SFR

Poniższy przykład ilustruje sytuację, w której po analizie wymagania źródłowego CR 1.1, którego celem jest wymuszenie stosowania zasad identyfikacji i uwierzytelniania użytkowników przez urządzenie IACS, zostały wytypowane 3 możliwe komponenty SFR z klasy FIA – Identyfikacja i uwierzytelnianie. Treść tych komponentów w pełni pokrywa obszar wymagania CR, dlatego też zaznaczono w 4 kolumnie tabeli, że można stosować wszystkie operacje udostępniane przez te komponenty - All applicable operations. Tym samym został osiągnięty jeden z trzech możliwych rezultatów syntezy w kroku 5.

Tabela 12. Przykład 1 - mapowanie CR do oryginalnego SFR

IEC 4-2 Foundational Requirements (FRs)	**IEC Component**	**CC SFR class, family, component**	**CC adapted SFR/ [*refinement*]/ [assignment]/ _EXT**	**CC Evaluation Activities (EAs)**
FR 1 - Identification and authentication control (IAC)	Requirement Enhancements (REs) = (#)	SFRs from CC p.2 or SFR_EXT	Requirement Refinements (RRs) = (#)	EAs for collaborative Protection Profile (cPP)
Human user identification and authentication	CR1.1	**FIA - Identification and authentication** FIA_UAU.5 - User authentication Multiple authentication mechanisms FIA_UID.1 - User identification Timing identification FIA_UID.2 - User identification User identification before any action	All applicable operations	Evaluation activities: CR1.1 test plan in the pilot evaluation report

Ostatnia kolumna CC Evaluation Activities zawiera działania oceniające, które można wykorzystać podczas testowania funkcji zabezpieczającej TSF implementującej wymagania danego SFR. W tym przypadku wskazano, że EAs są zgodne z planem testów dla tego wymagania „CR1.1 test plan in the pilot evaluation report", który opracowano na potrzeby oceny pilotażowej i wykazano w sprawozdaniu z badań w załączniku 2 do niniejszej pracy.

Plan testów dla CR 1.1 może być wykorzystany podczas testów TSF implementujących wymagania SFR, ponieważ pokrywają ten sam obszar zagadnień, co źródłowe wymaganie przemysłowe CR 1.1.

Plan testów i warunki akceptacji, czyli możliwości wydania werdyktu spełnienia wymagania CR 1.1 na podstawie tego testu, przedstawiono poniżej (wyciąg z załącznika 2).

Plan testów:

1. Identyfikacja dostępnych interfejsów dostępnych dla użytkowników.
2. Sprawdzenie dla zidentyfikowanych interfejsów, czy jest:
   a) wymuszana autoryzacja użytkowników przed uzyskaniem przez nich dostępu do funkcjonalności;
   b) zaimplementowana możliwość przydziału użytkownikom ról i uprawnień.
3. Opracowanie listy scenariuszy możliwych awarii urządzenia lub jego otoczenia, które mogą mieć wpływ na przeprowadzenie przez użytkownika procesu identyfikacji i autoryzacji użytkowników.

4. Ocena dla wszystkich opracowanych scenariuszy, czy w przypadku zaistnienia sytuacji awaryjnej nie będzie ona miała wpływu na możliwość podjęcia podstawowych działań na urządzeniu.

Warunki akceptacji

1. Zapewniona i wymuszona możliwość identyfikacji i autoryzacji użytkowników na wszystkich dostępnych dla użytkownika interfejsach (fizycznych i komunikacyjnych) potwierdzona wynikami testów lub uzasadnieniem na podstawie analizy dokumentacji.
2. Potwierdzone wynikami testów lub uzasadnieniem na podstawie analizy dokumentacji, że w żadnym z założonych scenariuszy awarii działanie procesu identyfikacji i autoryzacji urządzenia nie zostanie zakłócone w taki sposób, aby niemożliwe było podjęcie działań przynajmniej w stopniu podstawowym, niezbędnym w przypadku awarii.

Opracowując listę Evaluation Activities, tym samym zrealizowano krok 6 procesu dostosowania wymagania SFR dla pierwszego przykładu możliwego wyniku syntezy.

Poniżej przedstawiono drugi przykład możliwego wyniku syntezy.

Przykład 2 – SFR [*refinement, assignment*]

Poniższy przykład ilustruje sytuację, w której po analizie wymagania źródłowego CR 1.3, które narzuca stosowanie zarządzania kontami użytkowników w systemie IACS, wytypowano komponent SFR z klasy FMT – zarządzanie bezpieczeństwem. Komponent FMT_SMF.1 narzuca wymagania dotyczące specyfikacji funkcji zarządzających. Z kolei element FMT_SMF.1.1 precyzuje za pomocą operacji [*assignment*], jakie funkcje zarządzające mają być zapewnione przez TSF, co przedstawia tabela 13. Kolorem niebieskim oznaczono komponenty po operacji [*assignment*].

Tabela 13. Przykład 2 – dostosowanie SFR za pomocą operacji [*assignment*]

FR 1	CR	SFRs from CC p.2	SFR after assignment	EAs
Account management	CR1.3	**FMT - Security management** FMT_SMF.1 Specification of Management Functions	FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*assignment: list of management functions to be provided by the TSF*] [*assignment: account management*]	Evaluation activities: CR1.3 test plan in the pilot evaluation report

Zastosowanie w tym wypadku wartości operacji [*assignment:* a*ccount management*], czyli wprowadzenie do listy funkcji zarządzania kontami, pozwala na modyfikację komponentu SFR, aby uwzględniał wymaganie CR 1.3. (realizacja kroku 5).

Podobnie do przykładu 1, działania oceniające wskazują na plan testów przygotowany dla wymagania CR 1.3 podczas oceny pilotażowej (zob. załącznik 2, str. 158). Plan testów zawiera m.in. pkt 1, w którym przewiduje się sprawdzenie funkcjonalności związanej z zarządzaniem użytkownikami ze szczególnym uwzględnieniem możliwości odebrania uprawnień. Tak opracowana lista Evaluation Activities prowadzi do zrealizowania kroku 6 procesu dostosowania wymagania SFR, dla drugiego przykładu możliwego wyniku syntezy.

Poniżej przedstawiono trzeci, ostatni przykład możliwego wyniku syntezy.

Przykład 3 - SFR_EXT – dodatkowy SFR

Przykład przedstawia sytuację, gdy nie istnieje wymaganie SFR, które można zmapować lub zmodyfikować do potrzeb wymagania CR. W takim przypadku należy utworzyć komponent dodatkowy SFR_EXT.

Sytuację tę można zilustrować na przykładzie komponentu CR 1.2 (Software process and device identification and authentication), który narzuca urządzeniu IACS konieczność identyfikowania się i uwierzytelniania względem innych urządzeń. Komponent bazowy spełnia wymagania poziomu SL 2. Kombinacja komponentu bazowego i jego uszczegółowienia RE (1) – narzucającego konieczność unikalnej identyfikacji i uwierzytelniania urządzeń, spełnia wymagania poziomów SL 3 i SL 4.

Po analizie wymagań normy CC p.2 okazało się, że nie istnieje żaden komponent, rodzina ani klasa wymagań, która pokrywa ten obszar. Tabela 14 przedstawia przykład definicji komponentu dodatkowego FFR_IAC_EXT.1 Kolorem zielonym oznaczono komponenty rozszerzone EXT.

Tabela 14. Przykład 3 – utworzenie komponentu dodatkowego SFR_EXT

FR 1	CR	SFR_EXT class, family	SFR_EXT element	EAs
Software process and device identification and authentication	CR1.2 REs: (1) Security Level: CR1.2 - SL2 CR1.2(1) - SL3, SL4	**FFR - Function Foundational Requirement** **FFR_IAC_EXT.1** Software process and device identification and authentication	FFR_IAC_EXT.1.1 = CR1.2 RRs: (1) EAL level: FFR_IAC_EXT.1.1 - EAL1-3 (SL2) FFR_IAC_EXT.1.1(1) -EAL4 (SL3, SL4)	Evaluation activities: 1) All entities shall be identified and authenticated for all access to the control system 2) Tests shall verify methods such as passwords, tokens, or location (physical or logical)

Dla komponentu utworzono także rodzinę wymagań FFR_IAC_EXT (Software process and device identification and authentication). Nowa rodzina z kolei została przypisana do nowej klasy FFR – Function Foundational Requirement, która w swojej nazwie nawiązuje do wymagania fundamentalnego FR.

Treść elementu wymagania została sformułowana na bazie wymagania źródłowego CR 1.2, co oznaczono skrótowo FFR_IAC_EXT.1.1 = CR 1.2

FFR_IAC_EXT.1.1 – The TSF shall provide a capability of IACS component to identify itself and authenticate to any other component [selection: *software application, embedded devices, host devices, network devices*]

W elemencie zastosowano dodatkowo operację selekcji [*selection*], która umożliwia wybór jednej lub wszystkich dostępnych opcji wskazujących typy komponentów IACS, z którymi powinna zachodzić wzajemna identyfikacja i uwierzytelnianie.

Ponadto zgodnie z tym, że komponent CR 1.2 posiada uszczegółowienie RE (1), to zostało także zdefiniowane uszczegółowienie dla komponentu SFR oraz wskazano, że jest tożsame z RE (1) za pomocą skróconego zapisu RRs: (1).

Dzięki temu, w przypadku, gdy komponent przemysłowy będzie musiał spełnić wymagania wyższego poziomu, np. SL 3 i zastosować uszczegółowienie RE (1), co zapisuje się jako CR 1.2 (1), to w ten sam sposób będzie można uszczegółowić element FFR_IAC_EXT.1.1

Oryginalne uszczegółowienie komponentu CR 1.2 brzmi:

(1) – Unique identification and authentication

Użyte w tabeli oznaczenie FFR_IAC_EXT.1.1 (1) oznacza, że należy zastosować RE (1) komponentu CR 1.2 w definicji elementu SFR, poniżej fragment uszczegółowienia, które został wyróżniony pogrubioną czcionką z podkreśleniem:

FFR_IAC_EXT.1.1 – The TSF shall provide a capability of IACS component to **uniquely** identify itself and authenticate to any other component [selection: *software application, embedded devices, host devices, network devices*]

W tabeli także przypisano poziom EAL do uszczegółowionego elementu, co zapisano FFR_IAC_EXT.1.1(1) = EAL4 (SL 3, SL 4). Zapis ten należy rozumieć, że element po operacji [*refinement*] spełnia wymagania poziomu uzasadnionego zaufania EAL 4 zgodnie z normą CC. Poziom EAL został przypisany na podstawie tabeli 33 zawierającej mapowanie poziomów SL i EAL według wartości potencjału ataku stosowanego w analizie podatności (rozdz. 5.3.3).

W powyższy sposób opracowano komponent rozszerzony wraz z propozycją zastosowania operacji selekcji i uszczegółowienia (realizacja kroku 5).

Działania oceniające Evaluation Activities obejmują dwie możliwości testowania polegające na: 1) sprawdzeniu, czy wszystkie urządzenia identyfikują się i uwierzytelniają na wszystkich możliwych poziomach dostępu do systemu; 2) testowaniu metod identyfikacji i uwierzytelniania za pomocą takich środków, jak hasła, tokeny lub lokalizacja.

Zdefiniowanie Evaluation Activities dla elementu kończy realizację kroku 6.

Powyższe 3 przykłady zilustrowały możliwe rodzaje wyników syntezy wymagań CR i SFR. Analiza dla pozostałych par wymagań przebiega dokładnie według przedstawionych kroków. Ze względu na dużą liczbę wymagań CR oraz SFR, wyniki procesu adaptacji wymagań, które przedstawiono w załączniku 2, w tabeli 39, obejmują tylko kilka wymagań dla wymagań CR na poziomie SL 1 dla wymagania fundamentalnego FR 1, a które zostały także zweryfikowane podczas pilotażowej oceny bezpieczeństwa.

Ostatnim krokiem procesu kończącym proces adaptacji wymagań SFR jest utworzenie wynikowych tabel zawierających wszystkie zmodyfikowane wymagania włącznie z wymaganiami źródłowymi CR, tak jak to przedstawia tabela 39. W wyniku przeprowadzonych analiz powstała nowa tabela mapująca wymagania FR na klasy SFR pokazana poniżej.

7. Utworzenie wynikowych tabel mapujących wymagania CR i SFR

W wyniku szczegółowych analiz porównań powstała tabela mapowania (zob. Tabela 15), dokładniej wskazująca obszary występowania podobnych wymagań dla obydwu standardów.

Tabela 15. Mapowanie FRs IEC 62443-4-2 na klasy wymagań SFR CC p.2

FRs – Foundational Requirements from IEC 62443-4-2	**SFRs – Security Functional Requirements classes from ISO/IEC 15408-2**
FR 1 – Identification and authentication control (IAC)	**FIA** – Identification and authentication **FMT** – Security management
FR 2 – Use control (UC)	**FIA** –Identification and authentication **FTA** – TOE access **FAU** – Security audit **FRU** – Resource utilization
FR 3 – System integrity (SI)	**FPT** – Protection of the TSF **FTP** – Trusted path/channels **FPT** – Protection of the TSF
FR 4 – Data confidentiality (DC)	**FDP** – User data protection **FPT** – Protection of the TSF **FCS** – Cryptographic support
FR 5 – Restricted data flow (RDF)	**FTP** – Trusted paths/channels
FR 6 – Timely response to events (TRE)	**FAU** – Security audit review and analysis
FR 7 – Resource availability (RA)	**FRU** – Resource utilization **FMT** – Security management

Kolejnym krokiem jest adaptacja wymagań uzasadniających zaufanie SAR na podstawie Praktyk z normy IEC 62443-4-1.

4.4. Adaptacja wymagań SAR

Niniejszy rozdział przedstawia sposób adaptacji wymagań na zapewnienie zaufania do oceny zabezpieczeń (ang. Security Assurance Requirements, SAR) zawartych w normie CC p.3 Nazwa tej klasy wymagań wskazuje, że dotyczą one zapewnienia pewności, inaczej zaufania do funkcji zabezpieczających TOE. Zaufanie to osiągane jest w toku oceny zadania zabezpieczeń, dokumentacji użytkownika, dokumentacji projektowej, środowiska powstawania produktu, testowania i analizy podatności produktu.

Komponenty SAR określają postać i treść materiału dowodowego, który razem z produktem podlega ocenie w laboratorium oceny bezpieczeństwa. Dlatego też stanowią podstawę dla jednostek oceny w metodyce CEM, które określają czynności ewaluatora, które musi on zrealizować, aby wydać werdykt, czy dana zawartość materiału dowodowego odpowiada wymaganiom stawianym w komponencie SAR. Stąd wymagania CC p.3 w metodyce CC służą do projektowania i do oceny zabezpieczeń oraz stanowią podstawę uzasadnionego zaufania do produktu i jego zabezpieczeń.

Komponenty SAR mają podobną strukturę do komponentów SFR, dlatego też sposób ich adaptacji do cech IACA określonych w wymaganiach normy IEC 62443-4-1 będzie przebiegał w analogiczny sposób.

Do utworzenia udoskonalonych wymagań SAR została wykorzystania metoda analizy i konstrukcji logicznej oraz metoda porównań. Pierwszy etap analizy polegał na poznaniu budowy i struktury wymagań SAR oraz wstępnym mapowaniu standardów w celu wyznaczenia par wymagań do porównań. W etapie porównań analizowana była treść wymagań w celu identyfikacji cech charakterystycznych dla IACS. W ostatnim etapie następowała synteza cech charakterystycznych IACS w zmodyfikowane, wyjściowe wymaganie SAR.

Proces tworzenia nowych i udoskonalonych wymagań SAR zawiera następujące kroki:

1. Analiza struktury wymagań w normie IEC 62443-4-1
2. Analiza budowy komponentu SAR
3. Mapowanie wstępne Praktyk i klas SAR
4. Realizacja porównań Praktyk i SAR
    a. Selekcja elementu wymagania z danej Praktyki;
    b. Ustalenie elementu wyjściowego SAR;
    c. Czynnik porównania – cechy charakterystyczne dla IACS;
    d. Identyfikacja cechy IACS jako źródła uzupełnienia dla SAR.
5. Synteza wymagania SAR do jednej z poniższych postaci:
    a. SAR oryginalny – niezmieniony komponent SAR zmapowany do wymagania z Praktyki w przypadku pełnego pokrywania się obszarów wymagań,
    b. SAR [*refinement*] – dostosowany SAR za pomocą operacji: uszczegółowienia w przypadku, gdy treści wymagań częściowo się pokrywają;

c. SAR_EXT – dodatkowy komponent SAR w przypadku, gdy wymaganie z Praktyki nie ma swojego odpowiednika SAR lub SAR nie może być dostosowany za pomocą operacji uszczegółowienia;

6. Utworzenie jednostek oceny WU dla wszystkich zmapowanych i zmodyfikowanych komponentów SAR (w rozdz. 4.5).
7. Utworzenie wynikowych tabel mapujących wymagania Praktyk oraz SAR.

Każdy z tych kroków opisano szczegółowo poniżej.

1. Analiza struktury wymagań w normie IEC 62443-4-1

Wymagania normy dotyczą procesów wytwarzania bezpiecznego produktu IACS. Wymagania procesów zebrano w ośmiu Praktykach (zob. rozdz. 3.3), które zawierają szczegółowe wymagania na procesy (ang. Process requirements, PRs). Tabela 16 zawiera przykład wymagań PRs dla Praktyki 1 – Zarządzanie bezpieczeństwem i Praktyki 2 – Specyfikacja wymagań bezpieczeństwa.

Tabela 16. Wymagania procesowe w Praktykach 1 i 2

IEC 4-1 Practices	Process requirements
Practice 1 - Security management	SM-1: Development process
	SM-2: Identification of responsibilities
	SM-3: Identification of applicability
	SM-4: Security expertise
	SM-5: Process scoping
	SM-6: File integrity
	SM-7: Development environment security
	SM-8: Controls for private keys
	SM-9: Security requirements for externally provided components
	SM-10: Custom developed components from third-party suppliers
	SM-11: Assessing and addressing security related issues
	SM-12: Process verification
	SM-13: Continuous improvement
Practice 2 - Specification of security requirements	SR-1: Product security context
	SR-2: Threat model
	SR-3: Product security requirements
	SR-4: Product security requirements content
	SR-5: Security requirements review

Norma IEC 62443-4-1 opisuje cykl życia wytwarzania systemu IACS i jego komponentów przeznaczonych do pracy w środowisku przemysłowym i zawiera wytyczne, w jaki sposób spełnić wymagania dotyczące budowy i implementacji każdego elementu systemu IACS.

Norma specyfikuje wymagania procesowe PRs niezbędne do bezpiecznego wytwarzania produktów IACS. Dokument definiuje bezpieczny cykl rozwoju produktu (ang. Secure development life-cycle, SDL) na potrzeby wytwarzania i utrzymania bezpiecznych produktów.

Cykl SDL zawiera takie elementy, jak: definicja wymagań bezpieczeństwa, bezpieczny projekt, bezpieczna implementacja, weryfikacja i walidacja, zarządzanie usterkami, zarządzanie poprawkami, wycofanie z użycia. Wymagania te dotyczą producenta i konstruktora urządzenia i z tego względu obejmują podobny obszar wymagań, jaki obejmuje klasa ALC (ang. Life-cycle support) z normy CC p.3, która zostanie omówiona szczegółowo w kroku 2.

Konwencja zapisu wymagań w normie IEC 62443-4-1 jest następująca:

Practice # - grupa wymagań procesowych (gdzie # przyjmuje wartości od 1 do 8)

PR-X – wymaganie procesowe w ramach danej praktyki, gdzie PR jest zastępowane akronimem nazwy danej praktyki, a X oznacza kolejny numer wymagania, np.:

SM-Y – oznacza jedno z trzynastu wymagań procesowych dla Praktyki 1 – Security Management (SM), gdzie Y przyjmuje wartości od 1 do 13

SR-D – oznacza jedno z czterech wymagań PR dla Praktyki 2 - Specification of security requirements (SR), gdzie D przyjmuje wartości od 1 do 4

Każdy komponent PR zdefiniowany jest w normie IEC 62443-4-1 za pomocą 2 sekcji:

1. Requirement – opisuje szczegółowo treść wymagania procesowego;
2. Rationale and supplemental guidance – podaje uzasadnienie i wytyczne zawierające dodatkowe informacje ułatwiające implementację danego wymagania;

Powyższy sposób oznaczania komponentów PR będzie stosowany podczas etapu porównywania wymagań.

2. Analiza budowy komponentu SAR

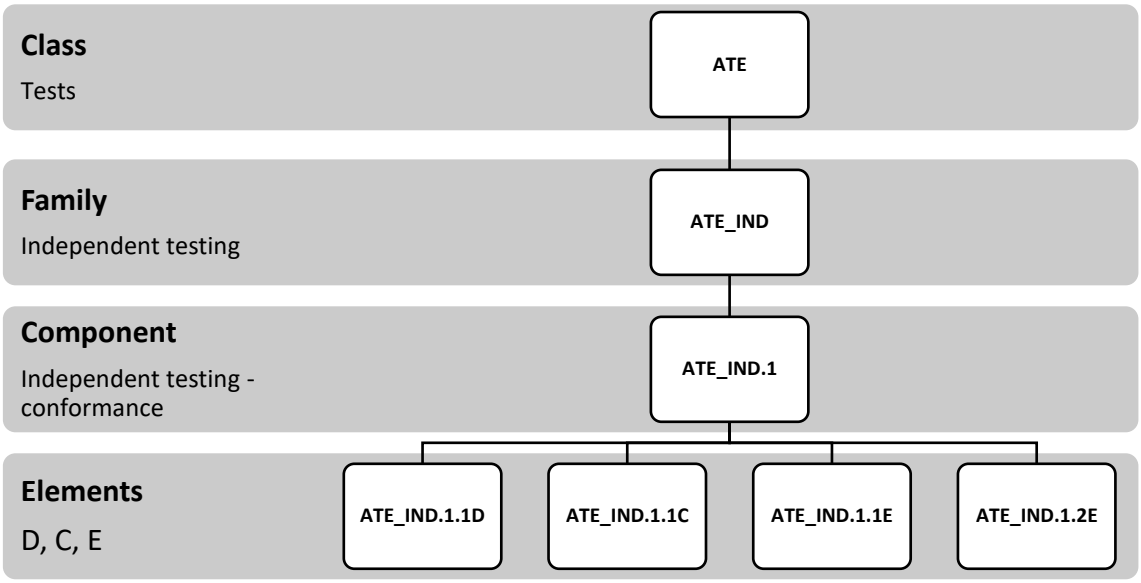
Komponenty SAR zdefiniowane są w normie CC p.3 i podobnie do komponentów SFR pogrupowane są w klasy, rodziny, komponenty i elementy. W danej rodzinie komponenty uszeregowane są hierarchicznie, gdzie każdy komponent o wyższym numerze oznacza bardziej rygorystyczne wymaganie w stosunku do poprzedniego. Norma CC p.3 zawiera, m.in. następujące klasy uzasadniające zaufanie [88]:

- APE, Ocena dokumentu PP (ang. Protection Profile Evaluation);
- ASE, Ocena dokumentu ST (ang. Security Target Evaluation);
- AGD, Dokumentacja użytkownika (ang. Guidance Documents);
- ADV, Projektowanie (ang. Development);
- ALC, Wsparcie cyklu życia (ang. Life-Cycle Support);
- ATE, Testowanie (ang. Tests);
- AVA, Szacowanie podatności (ang. Vulnerability Assessment).

Klasy APE i ASE określają odpowiednio wymagania na strukturę i zawartość dokumentów profilu zabezpieczeń (PP) i zadania zabezpieczeń (ST), które specyfikują wymagania

bezpieczeństwa TOE. Istotne dla kreowania uzasadnionego zaufania wobec produktu są klasy ADV, AGD i ATE ukierunkowane na produkt wytwarzany w środowisku rozwojowym. Natomiast środowisko rozwojowe oceniane jest według wymagań klasy ALC. Klasa AVA służy do analizy podatności produktu.

Każda z powyższych klas zawiera rodziny wymagań, a te z kolei zawierają komponenty wymagań podzielone na elementy. Poniższy rys. 9 przedstawia strukturę wymagań SAR w klasie ATE – Testowanie:



Rys. 9. Przykładowa struktura wymagania SAR w CC p.

Podczas porównań brane będą pod uwagę komponenty wymagań wraz z ich elementami. Każdy komponent opisany jest w normie za pomocą nazwy, zależności od innych komponentów, celów komponentu, wytycznych aplikacyjnych. Każdy z komponentów posiada elementy C, D i E, które zdefiniowano poniżej:

- element D (ang. Developer Action Element) określa, jaki materiał dowodowy powinien dostarczyć konstruktor, aby spełnić dane wymaganie,
- element C (ang. Content & Presentation of Evidence Element) określa, jaką postać i zawartość powinien mieć dostarczony materiał dowodowy,
- element E (ang. Evaluator Action Element) określa, w jaki sposób dostarczony materiał dowodowy sprawdzany przez oceniającego.

Podany wyżej komponent **ATE_IND.1** Independent testing – conformance jest zdefiniowany w normie CC p.3 i należy do rodziny ATE_IND, która nakłada wymagania na testy niezależne TOE wykonywane w laboratorium. Definicja komponentu w normie została przedstawiona w tabeli 17 poniżej.

Tabela 17. Przykład definicji komponentu SAR - ATE_IND.1

Elementy definicji	Wyjaśnienie
Dependencies: ADV_FSP.1 Basic functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures	**Zależności** z innymi komponentami, oznaczają, że spełnienie wymagania bieżącego komponentu wiąże się także ze spełnieniem odpowiednio wymagań dotyczących podstawowej specyfikacji funkcjonalnej, dokumentacji użytkowania i procedur przygotowania TOE do pracy
Objectives In this component, the objective is to demonstrate that the TOE operates in accordance with its design representations and guidance documents.	**Celem** komponentu jest wykazanie, że TOE działa zgodnie z dokumentacją projektową i dokumentacją użytkownika
Application notes This component does not address the use of developer test results.	**Notka stosowania** Komponent nie dotyczy możliwości użycia wyników testów wykonanych przez producenta.
Developer action elements: **ATE_IND.1.1D** The developer shall provide the TOE for testing	**Element D**, mówiący, że konstruktor powinien dostarczyć TOE do testów
Content and presentation elements: **ATE_IND.1.1C** The TOE shall be suitable for testing.	**Element C**, mówiący, że TOE powinno być przygotowane do testowania, czyli w konfiguracji przeznaczonej do oceny i z odpowiednią platformą testową.
ATE_IND.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.	**Element E**, mówiący, że ewaluator musi potwierdzić, że dostarczona informacja na temat TOE spełnia wszystkie wymagania dotyczące prezentacji i zawartości materiału dowodowego
ATE_IND.1.2E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.	**Element E**, mówiący, że ewaluator musi wykonać test wybranego zbioru funkcji TSF, aby potwierdzić, że funkcje TSF działają zgodnie z ich specyfikacją przedstawioną przed konstruktora.

Komponenty SAR można dostosować za pomocą operacji uszczegółowienia i iteracji, co zostanie przedstawione na konkretnych przykładach wyników metody porównań. Uszczegółowienie (refinement) umożliwia odpowiednie dopasowanie komponentu SAR do specyficznych wymagań, co zostanie wykorzystane w przypadku adaptacji wymagań SAR do potrzeb wynikających z wymagań normy IEC 62443-4-1.

Należy w tym miejscu wskazać na charakterystyczną cechę metodyki Common Criteria, czyli miary uzasadnionego zaufania. Miary tworzone są przez odpowiednio dobrane grupy komponentów SAR, zwane pakietami uzasadnionego zaufania. Pakiety te symbolizowane są przez poziomy EAL.

W tabeli 18 pokazano budowę poszczególnych pakietów EAL. Wiersze tabeli reprezentują komponenty z poszczególnych rodzin wchodzące w skład danych pakietów EAL. Pakietom EAL odpowiadają kolumny.

Tabela 18. Komponenty SAR wchodzące w skład poszczególnych pakietów EAL

Klasa	Rodzina	Poziom uzasadnionego zaufania						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ADV	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	3
	ADV_SPM						**1**	1
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**
AGD	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
ALC	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR	opcjonalne dla dowolnego EAL						
	ALC_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	**3**	3
ASE	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
ATE	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	**2**	**3**	3	**4**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
AVA	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

W ramach danej rodziny komponenty uszeregowano według rosnących wymagań, czy też rygoru, to znaczy, że komponent o wyższym numerze, np. ADV_TDS.4 zawiera wymagania swojego poprzednika ADV_TDS.3 oraz pewne dodatkowe wymagania. Wyższy rygor oznacza większą szczegółowość opisu, analiz, działań oceniających. Komponenty danej rodziny mogą pojawiać się od pewnego poziomu EAL. W tabeli wytłuszczono numery komponentów pojawiające się po raz pierwszy lub zastępujące komponenty o mniejszym poziomie rygoru [49].

Poziomy EAL mają następującą interpretację:

- EAL 1 – TOE testowany funkcjonalnie (ang. functionally tested),
- EAL 2 – TOE był testowany strukturalnie (ang. structurally tested),

- EAL 3 – TOE był metodycznie sprawdzany i testowany (ang. methodically tested and checked),
- EAL 4 – TOE był metodycznie projektowany, testowany i przeglądany (ang. methodically designed, tested, and reviewed),
- EAL 5 – TOE był półformalnie projektowany i testowany (ang. semiformally designed and tested),
- EAL 6 – projekt TOE został półformalnie zweryfikowany i przetestowany (ang. semiformally verified design and tested),
- EAL 7 – projekt TOE został formalnie zweryfikowany i przetestowany (ang. formally verified design and tested).

Z danego pakietu EAL nie można usuwać żadnego komponentu, można natomiast dodać komponent (ang. augmentation) lub zastąpić komponent z pakietu komponentem o wyższym rygorze (ang. substitution).

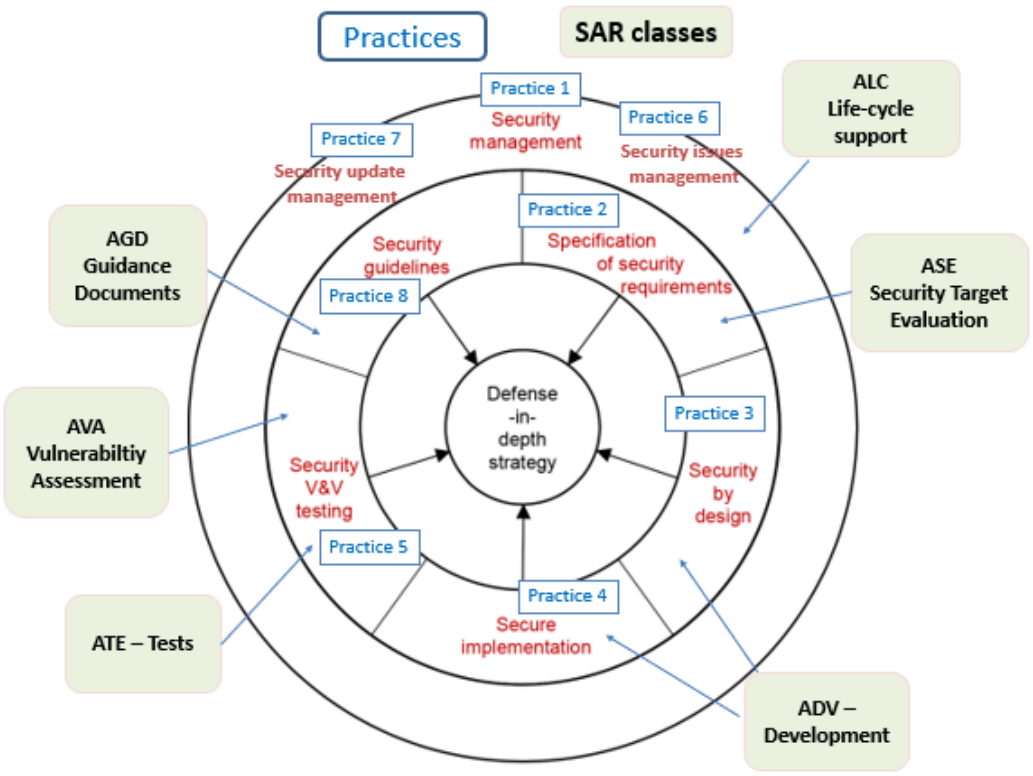
Należy zauważyć, że im wyższy poziom EAL, tym więcej zawiera on komponentów i tym bardziej są one rygorystyczne.

Po przedstawieniu podstawowych struktur wymagań norm CC p.3 i IEC 62443-4-1 można przystąpić do kolejnego kroku procesu analizy i tworzenia dostosowanych wymagań SAR.

3. Mapowanie wstępne Praktyk i klas wymagań SAR

W kolejnym kroku wykonano wstępne mapowanie Praktyk normy IEC 62443-4-1 do klas wymagań SAR normy CC p.3. Mapowanie to pozwoliło na wytypowanie podobnych obszarów wymagań obu norm. Mapowanie jest wysokopoziomowe, ponieważ zostało wykonane na podstawie analizy opisów celów Praktyk i klas SAR bez szczegółowej analizy treści poszczególnych komponentów PR i SAR. Mapowanie przedstawia rysunek 10.

Wstępne mapowanie powstało w kontekście promowanej w normie IEC 62443-4-1 tzw. strategii ochrony w głąb (ang. Defense-in-depth strategy). Standard zawiera wymagania na procesy tworzenia bezpiecznego produktu, czyli wspiera zasadę, że bezpieczeństwo produktu może być zapewnione za pomocą bezpiecznego projektu tego produktu (ang. Security by design). Rysunek pokazuje na najbardziej zewnętrznej warstwie praktykę zarządzania bezpieczeństwem, ponieważ jest stosowana do wszystkich pozostałych praktyk. Praktyki na drugim okręgu stosowane są w całym cyklu życia rozwoju produktu. Każda z praktyk ma swój wkład do zapewnienia strategii w głąb, która jest pokazana jako centralny okrąg, ponieważ reprezentuje kluczowy rezultat stosowania cyklu życia do projektowania bezpiecznego produktu IACS.



Rys. 10. Wstępne mapowanie Praktyk na klasy wymagań SAR

Po określeniu wstępnego mapowania, można realizować kolejne kroki procesu adaptacji SAR.

4. Realizacja porównań Praktyk i SAR
5. Synteza wymagania SAR
6. Utworzenie jednostek oceny WU

Kroki 4, 5 i 6 były realizowane z wykorzystaniem jednego arkusza Excel, dlatego ich wykonanie przebiegało jednocześnie i będą opisywane łącznie w tej sekcji pracy z wyjątkiem kroku 6 dotyczącego adaptacji jednostek oceny WU. Wyniki kroku 6 zostaną zaprezentowane w rozdz. 4.5 ze względu na ich dodatkowe możliwe wykorzystanie w normie CC p.4 do tworzenia Evaluation Activities dla nowych metod oceny stosowanych w profilach cPP.

Arkusz wynikowy porównań przedstawia tabela 36 w załączniku 1. Znajdują się tam wyniki porównań dla wszystkich wymagań procesowych PRs w ramach ośmiu Praktyk normy IEC 62443-4-1, także tych, które zostały wytypowane na podstawie wstępnej tabeli mapowania (realizacja kroku 4). Komponent SAR w danej parze stanowi element wyjściowy do doskonalenia na podstawie cech IACS zidentyfikowanych podczas analizy treści wymagań PRs w ramach danej praktyki.

Zidentyfikowana cecha stanowi element doskonalenia wymagania SAR zgodnie z kolejnymi punktami kroku 5. Poniżej przedstawiono rezultaty syntezy dostosowanego wymagania SAR na trzech przykładach ilustrujących każdy możliwy wynik syntezy.

Przykład 1 – mapowanie PR do oryginalnego wymagania SAR

Poniższy przykład ilustruje sytuację, w której po analizie wymagań źródłowych SM-6, SM-7 i SM-8 w Praktyce 1, dobrano 2 komponenty ALC_DEL.1 oraz ALC_DVS.1, które pokrywają ten sam obszar wymagań.

Tabela 19. Przykład 1 – mapowanie PRs do oryginalnych SARs

Practice	Process requirement	SAR component	SAR element	Work Unit
Practice 1	SM-6: File integrity	**ALC_DEL.1**	NA	NA
	SM-7: Development environment security	**ALC_DVS.1**	NA	NA
	SM-8: Controls for private keys			

Analiza treści wymagań PRs:
SM-6 – wymaga zapewnienia mechanizmu weryfikowania integralności dla wszystkich plików produktu,
SM-7 – wymaga zapewnienia proceduralnych i technicznych zabezpieczeń do ochrony produktu podczas rozwoju, wytwarzania i dostawy,
SM-8 – wymaga zapewnienia proceduralnych i technicznych zabezpieczeń do ochrony kluczy prywatnych do podpisywania kodów źródłowych.

Analiza treści wymagań SAR:
ALC_DEL.1 – wymaga bezpiecznej dostawy ukończonego produktu ze środowiska rozwojowego do użytkownika.
ALC_DVS – wymaga stosowania fizycznych, proceduralnych, osobowych i innych środków bezpieczeństwa w środowisku rozwojowym w celu ochrony TOE i jego części.

Porównując treści wymagań widać, że pary SM-6 – ALC_DEL.1 oraz SM-7, SM-8 – ALC_DVS. 1 pokrywają te same obszary, więc nie jest wymagana modyfikacja komponentów SAR. Podczas oceny urządzenia IACS wybrane komponenty SAR zostaną wskazane do oceny odpowiednich wymagań przemysłowych.

Przykład 2 – SAR [*refinement*]

Poniższy przykład ilustruje sytuację, w której analizowano wymaganie SM-5 Process scoping, które narzuca konstruktorowi wskazanie zakresów norm IEC 62443-4-1 oraz IEC 62443-4-2, które zostały zastosowane w procesie wytwarzania produktu. Taka informacja uzupełnia deklarację zgodności w zadaniu zabezpieczeń, co wykazano w rozdz. 4.2.

W związku z tym, że rodzina ALC_LCD dotyczy definicji cyklu życia, w którym określone powinny być także etapy wytwarzania produktu, to ona stanowiła źródło doboru komponentu pasującego do wymagania SM-5.

Do analizy wybrano komponent ALC_LCD.1 i jego element ALC_LCD.1.1C, który wymaga, aby dokumentacja cyklu życia produktu opisywała model używany do rozwoju i utrzymania TOE. W dokumentacji modelu może się zatem znaleźć dodatkowa informacja o standardach wymagań, które stosowane są dla danych typów produktów. Stąd uszczegółowienie elementu C i skojarzonej z nim jednostki oceny WU, które pokazano w tabeli 20. Kolorem niebieskim oznaczono komponenty po operacji [*refinement*].

Tabela 20. Przykład 2 - dostosowanie SAR za pomocą operacji [*refinement*]

Process requirement	SAR component	SAR element	Work Unit
SM-5: Process scoping	**ALC_LCD.1 [*refinement 2*] Developer defined life-cycle model**	**ALC_LCD.1.1C** [*The life-cycle definition documentation shall include justification by documented security analysis to identify the parts of IEC 62443-4-1 and IEC 62443-4-2 documents that are applicable to a selected product development project*]	ALC_LCD.1-1(2) Evaluation activities [*The evaluator shall examine the documented description of the life-cycle model used to determine that it covers parts of standards IEC 62443-4-1 and IEC 62443-4-2 the product claims conformance*]

Ponieważ większość wymagań Praktyk dotyczy procesów wytwarzania produktów, to naturalne jest, że z kolei najwięcej wspólnych obszarów wymagań będą miały z klasą ALC, co zostało wykazane po przeanalizowaniu wszystkich par. Ze wszystkich 33 zmapowanych wymagań SAR, aż 25 z nich pochodzi z klasy ALC. Dlatego też, w opisie zmodyfikowanego wymagania przy operacji [*refinement*] znajduje się numer kolejnej modyfikacji komponentu (iteracja) w celu jej jednoznacznej identyfikacji.

Przykład 3 - SAR_EXT – dodatkowy SAR

Przykład przedstawia sytuację, gdy żadnego komponentu SAR nie można zmapować lub zmodyfikować do potrzeb wymagania PR. W takim przypadku należało utworzyć komponent dodatkowy SAR_EXT.

Sytuację tę można zilustrować na przykładzie wymagania Praktyki 7, SUM-1 (Security update qualification), które dotyczy kwalifikacji aktualizacji bezpieczeństwa jako gotowego do dystrybucji do klienta. Kwalifikacja weryfikuje, czy poprawki niwelują wskazane w produkcie podatności.

W normie CC p.3 istnieje rodzina opcjonalna ALC_FLR, która dotyczy zarządzania procesem usuwania usterek, jednakże jej przeznaczenie różni się od wymagania SUM-1, gdyż dotyczy procesu zarządzania usterkami bezpieczeństwa zgłaszanymi przez użytkowników i w tym wypadku nie mogła być użyta. Dlatego też utworzono nową rodzinę ALC_SUM_EXE (Security update management) i włączono do niej komponent dodatkowy ALC_SUM_EXT.1

(Security update qualification) oraz skojarzoną z nim jednostkę oceny ALC_SUM_EXT.1-1, co przedstawia tabela 21.

Tabela 21. Przykład 3 – utworzenie komponentu dodatkowego SAR_EXT

Process requirement	SAR component	SAR element	Work Unit
SUM-1: Security update qualification (*SAR_EXT component name*)	**ALC Life-cycle support**	**ALC_SUM_EXT.1 - Security update qualification** ATE_SUM_EXT.1.1D [The developer shall provide documentation for security update qualification including confirmation that update is not contradicting to operational or legal constraints] ALC_SUM_EXT.1.1C [The documentation of security update qualification shall include 1) security updates created by the product developer addressing the intended security vulnerabilities; 2) the results of updates verification that they do not introduce regressions including patches created by: a) the product developer; b) suppliers of dependent components] ALC_SUM_EXT.1.1E [The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence]	**ALC_SUM_EXT.1-1** Evaluation activities [The evaluator shall check that the qualification documentation includes confirmation that updates do not contradict operational, safety or legal constraints] [The evaluator checks the qualification documentation whether there are evidence that security updates do not introduce regressions] [The evaluator checks the documentation if it includes a confirmation that patches applicable to the product are evaluated to ensure that they do not adversely affect operation of the product]

Powyższe 3 przykłady zilustrowały możliwe rodzaje wyników syntezy wymagań PR i SAR. Analiza dla pozostałych par wymagań przebiegała dokładnie według przedstawionych kroków.

Krok 6, którego celem jest omówienie utworzonych jednostek oceny WU kontekście normy CC p.4, przedstawiono w kolejnym rozdziale.

Ostatnim krokiem procesu kończącym proces adaptacji wymagań SAR jest utworzenie wynikowych tabel zawierających wszystkie zmodyfikowane wymagania włącznie z wymaganiami źródłowymi PR, tak jak to przedstawiają tabele 36, 37, 38 w załączniku 1.

7. Utworzenie wynikowych tabel mapujących wymagania Praktyk i SAR

Pierwsze przybliżenie mapowania na podstawie rys. 10 zakresu głównych klas CC i praktyk IEC było wysokopoziomowe, dlatego służyło tylko do orientacyjnego kojarzenia par

wymagań w celu porównań. W wyniku analizy wszystkich Praktyk otrzymano tabelę końcową mapowania klas SAR na Praktyki, co pokazuje tabela 22.

Tabela 22. Wynikowe mapowanie klas CC na Praktyki IEC

CC Class	Family	IEC Practices	IEC requirements
AGD Guidance documents	**AGD_PRE** Preparative procedures	**Practice 8** Security guidelines	Product defense in depth Defense in depth measures expected in the environment Security hardening guidelines
ADV Development	**ADV_ARC** Security architecture	**Practice 3** Secure by design	Security by design
ALC Life-cycle support	**ALC_FLR** Flaw remediation	**Practice 6** Security issues management	Periodic review of security defect management practice
	ALC_TAT Tools and techniques	**Practice 4** Secure implementation	Secure coding standard
	ALC_CMS Configuration management scope	**Practice 1** Security management	Security requirements for externally provided components Custom developed components from third-party suppliers
	ALC_LCD Life-cycle definition		Security expertise
			Process scoping
			Process verification Continuous improvement
		Practice 2 Specification of security requirements	Product security context
			Threat model
			Product security requirements Product security requirements content Security requirements review
		Practice 3 Security by design	Security design review
			Secure design best practices
		Practice 4 Secure implementation	Security implementation review
		Practice 8 Security guidelines	Secure disposal guidelines
			Security update qualification
			Security update documentation

	ALC_SUM_EXT Security update management	**Practice 7** Security update management	Dependent component or operating system security update documentation
			Security update delivery
			Timely delivery of security patches
ATE Tests	**ATE_FUN** Functional testing	**Practice 5** Security verification and validation testing	Independence of testers
			Security requirements testing
	ATE_IND Independent testing - conformance		Security requirements testing
	ATE_SVV_EXT Security verification and validation testing		Threat mitigation testing
			Vulnerability testing
			Penetration testing

Porównanie mapowań wstępnego i wynikowego pokazuje tabela 23.

Tabela 23. Porównanie mapowania wstępnego i wynikowego dla Praktyk i klas SAR

Praktyki	Mapowanie wstępne	Mapowanie po analizie
Praktyka 1	ALC	ALC
Praktyka 2	ASE	ALC
Praktyka 3	ADV	ADV, ALC
Praktyka 4	ADV	ALC
Praktyka 5	ATE, AVA	ATE, ATE_EXT
Praktyka 6	ALC	ALC
Praktyka 7	ALC	ALC_EXT
Praktyka 8	AGD	AGD, ALC

Z powyższego porównania wynika, że wymagania klasy ASE nie są uwzględnione w normie IEC 62443-4-1, ponieważ norma nie wymaga takiego dokumentu, jak zadanie zabezpieczeń. Dlatego też nie występuje tu mapowanie na odpowiednie wymaganie Praktyki.

Jednakże z wyników porównania zadania zabezpieczeń w rozdz. 4.2 wynika konieczność uzupełnia dokumentu ST, co wiąże się z modyfikacją komponentów następujących rodzin klasy ASE:

- ASE_CCL (Conformance claims) – w celu uwzględnienia i oceny informacji na temat zadeklarowanych standardów przemysłowych, ich zakresie oraz poziomie SL;
- ASE_SPD (Security problem definitione) – w celu uzupełnienia i oceny informacji na temat krytycznych zasobów TOE i środowiska wraz z ich atrybutami bezpieczeństwa w ujęciu standardu przemysłowego;

- ASE_ECD (Extended component definition) – w celu uwzględnienia i oceny informacji na temat zaadaptowanych wymagań przemysłowych SAR_EXT, SFR_EXT;
- ASE_REQ (Security requirements) – w celu uwzględnienia i oceny informacji na temat zadeklarowanych wymagań rozszerzonych SAR_EXT – dla EAL i SFR_EXT – dla SL.

W wyniku uszczegółowienia komponentów rodzin ASE otrzymano następujące dostosowane komponenty i odpowiadające im jednostki oceny WU (tabela 24).

Tabela 24. Klasa ASE adaptowana do oceny ST dla IACS

ASE Class	**ASE component**	**Adapted ASE elements [*refinement*]**	**WU_EXT - Adapted Work Units (WUs)**
ASE **Security Target evaluation**	**ASE_CCL.1 [*refinement*]**	**ASE_CCL.1.1C** [*The conformance claim shall contain a conformance to security industrial standards IEC 62443-4-1, IEC 62443-4-2 including security level SL*]	**ASE_CCL.1-1** [*The evaluator shall check that the conformance claim contains a conformance claim that whether it includes IEC 62443-4-1 and IEC 62443-4-2 standards and SL claimed for an IACS component*]
	ASE_SPD.1 [*refinement*]	**ASE_SPD.1.2C** [*All threats shall be described in terms of a threat agent, an asset, and an adverse action. Definitions of threats shall also include assets for IACS component: critical assets for TOE and critical assets of environment with their security attributes assigned*]	**ASE_SPD.1-2** [*The evaluator shall examine the security problem definition to determine that assets for an IACS component are described as critical assets for TOE and critical assets for environment with their security attributes assigned: AV, I, C, Au*]
	ASE_ECD.1 [*refinement*]	**ASE_ECD.1.1C** [*The statement of security requirements shall identify all extended security requirements for an IACS component*]	**ASE_ECD.1-1** Original Work unit applies [*The evaluator shall check that all security requirements in the statement of security requirements that are not identified as extended requirements are present in CC Part 2 or in CC Part 3*]
	ASE_REQ.1 [*refinement*]	**ASE_REQ.1.1C** [*The statement of security requirements shall describe the SFRs and the SARs including tailored security requirements IACS components*]	**ASE_REQ.1-1** [*The evaluator shall check that the statement of security requirements describes the SFRs derived from IEC 62443-4-2 for the given SL*] **ASE_REQ.1-2** [*The evaluator shall check that the statement of security requirements describes the SARs derived from IEC 62443-4-1*]

Natomiast wymagania dotyczące analizy podatności w Praktyce 5 normy IEC 62443-4-1, wymagają, aby to konstruktor wykonał analizę, podczas gdy w normie CC p.3 jest ona wykonywana wyłącznie przez laboratorium.

Załącznik 1 zawiera tabele, które ilustrują wyniki mapowań z różnych perspektyw. Tabela 36 jest główną tabelą, która zawiera pełny wynik adaptacji wymagań i szczegółowe treści dostosowanych komponentów SAR i jednostek oceny WU. Tabela 37 jest uproszczoną wersją prezentacji wyników (w następującej kolejności kolumn: Praktyka, PR, SAR, WU, EAL) bez szczegółowych definicji komponentów. Z kolei tabela 38 jest odpowiednikiem tabeli 37, czyli tabelą z uproszczoną prezentacją wyników, ale w innej kolejności kolumn: Klasa SAR, komponent SAR, jednostka WU, EAL, Praktyka, bez szczegółowych definicji komponentów. Różne sposoby prezentacji wyników ułatwiają korzystanie z wyników mapowania.

Kolejny rozdział podsumowuje wykonane syntezy wymagań w kontekście jednostek oceny, które będą wykorzystywane w metodzie oceny IACS.

4.5. Adaptacja jednostek oceny dla CC p.4

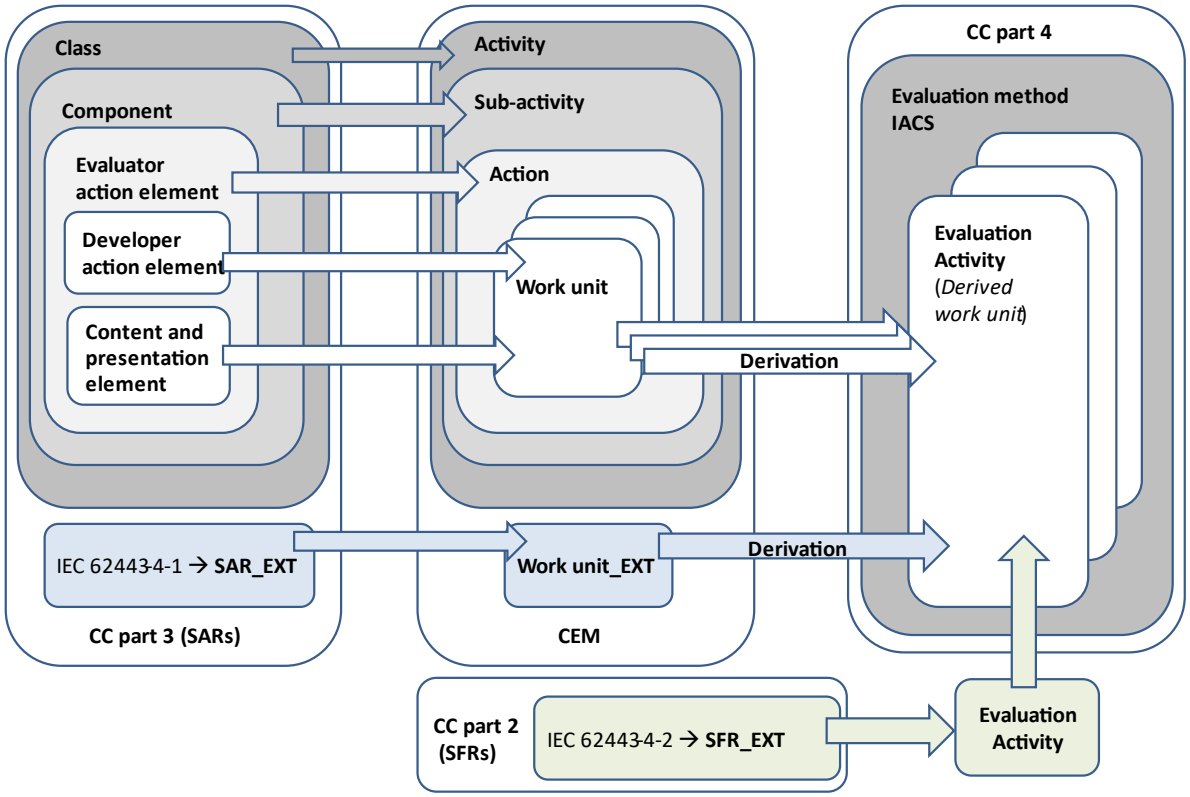
Celem niniejszego rozdziału jest zebranie wyników adaptacji wymagań SFR i SAR w zakresie utworzonych jednostek oceny WU i działań oceniających (EAs) oraz wskazanie sposobu ich wykorzystania w świetle normy CC p.4.

W pierwszej części rozdziału odkryto fakt nr 2, dotyczący zastosowania normy CC p.4, mówiący, że umożliwia ona przygotowanie odpowiednich działań oceniających wyprowadzonych z dostosowanych jednostek oceny CEM w celu tworzenia metod oceny dla specyficznych produktów lub technologii. Zatem, aby móc w przyszłości zastosować normę CC p.4 do rozwijania metod oceny dla IACS, to należało opracować odpowiednio zaadaptowane jednostki oceny WU przeznaczone dla IACS. Jednostki oceny po adaptacji oznaczono przyrostkiem EXT, czyli WU_EXT, w celu odróżnienia ich od oryginalnych jednostek WU w CEM, sprzed adaptacji.

Jednostki oceny WU opracowano już w trakcie adaptacji wymagań SFR i SAR (zob. rozdz. 4.3 i 4.4), otrzymując:

- jednostki oceny WU_EXT dla rozszerzonych komponentów SAR;
- działania oceniające EAs dla rozszerzonych wymagań SFR.

Szczegółowa zawartość działań oceniających i jednostek oceny znajduje się w tabelach mapujących dla SFR i SAR. Rysunek 11 przedstawia w sposób całościowy możliwość wykorzystania wszystkich rezultatów badań otrzymanych w rozdz. 4 niniejszej pracy do opracowywania metod oceny z wykorzystaniem normy CC p.4.



Rys. 11. Mapowanie CC p.3 i CEM oraz wymagań rozszerzonych na normę CC p.4

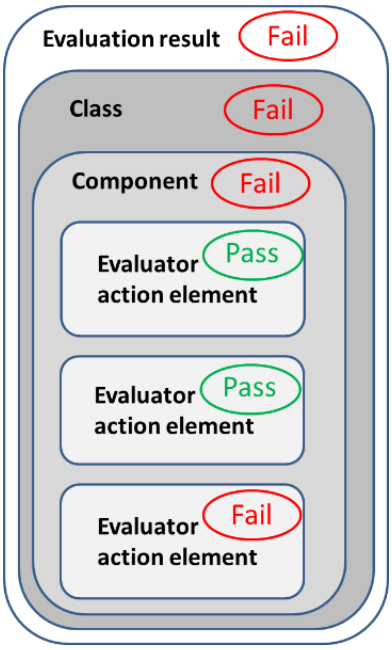
Komponenty SAR po adaptacji (SAR_EXT) są źródłem jednostek oceny (WU_EXT), z których można dalej wyprowadzić jednostki oceniające (ang. Derived work unit) dla CC p.4. Natomiast komponenty SFR po adaptacji są źródłem działań oceniających (ang. Evaluation Activity), które zostaną wykorzystane do dwóch celów:

- pierwszy dotyczy walidacji metody oceny dla IACS w zakresie możliwości wydawania werdyktów dla oceny uszczegółowionego [*refinement*] komponentu ATE_IND.1 (zob. rozdz. 5.3.2 Testy funkcjonalne i niezależne);
- drugi dotyczy możliwości włączenia utworzonych działań oceniających do profili zabezpieczeń cPP dla sterowników, które zostaną użyte do testowania rozszerzonych komponentów SFR_EXT.

Wszystkie komponenty rozszerzone (SFR_EXT, SAR_EXT) łącznie z jednostkami oceny (WU_EXT) oraz działaniami oceniającymi (EA) będą mogły być włączone do tworzonych w przyszłości cPP dla urządzeń IACS.

Należy tu przytoczyć podstawowe zasady wydawania werdyktów z oceny wymagań, które obowiązują w Common Criteria i będą stosowane w opracowanej metodzie oceny dla IACS. Werdykty przypisuje się do każdego elementu E (Evaluator action element) danego komponentu SAR. Elementowi E odpowiada działanie z CEM (Action), które składa się z jednostek oceny WU (jak to pokazano na rys. 11 powyżej). Po wykonaniu wszystkich działań

określonych w jednostkach WU przypisuje się werdykt do odpowiadającego elementu E. Końcowy werdykt dla komponentu jest pozytywny (Pass) wtedy i tylko wtedy, gdy wszystkie składające się na niego werdykty są także pozytywne. Rys. 12 ilustruje zasadę, że jeśli co najmniej jeden werdykt dla elementu E jest negatywny (Fail), to wtedy werdykty dla komponentu i całej klasy SAR oraz końcowy wynik oceny także są negatywne.



Rys. 12. Zasada przyznawania werdyktów

Rozdział 4 miał na celu rozwiązanie problemu w kontekście możliwości adaptacji metodyki Common Criteria do stosowania dla urządzeń IACS. Do rozwiązania tego problemu wykorzystano metody heurystyczne, metodę porównań, metodę analizy i konstrukcji logicznej.

W trakcie badań wykonano analizy:

- struktury i zawartości dokumentu zadania zabezpieczeń,
- wymagań bezpieczeństwa standardów IEC 62443-4-1 i IEC 62443-4-2,
- wymagań bezpieczeństwa standardów CC p.2 i CC p.3,
- jednostek oceny CEM,
- działań oceniających zgodnych z CC p.4.

W rezultacie zidentyfikowano dane, które stanowią uzupełnienie zadania zabezpieczeń dostosowanego do IACS. Otrzymano także szczegółowe tabele zawierające:

- listę zaadaptowanych wymagań SAR i jednostek oceny – tabele 24 i 36,
- listę zaadaptowanych wymagań SFR i działań oceniających – tabela 39.

W rezultacie analizy możliwości zastosowania standardu CC p.4 przedstawiono relacje i związki pomiędzy standardami IEC 62443-4-1, IEC 62443-4-2 oraz CC p.2, CC p.3 CC p.4, CEM, które wskazują na możliwość wykorzystania wyników badań w przyszłości, stosując

podejście najnowszej wersji standardu, a ponadto stanowią przygotowanie laboratorium ITSEF do implementacji najnowszego wydania rodziny norm Common Criteria.

Podsumowując, wykonane badania potwierdziły możliwość adaptacji metodyki Common Criteria i jej elementów do stosowania dla urządzeń IACS, co stanowi realizację celu szczegółowego C2. Dzięki temu, otrzymane wyniki zostaną zastosowane w metodzie oceny IACS, która zostanie zaprezentowana w kolejnym rozdziale.

5. Opracowanie metody oceny dla IACS

Rozdział przedstawia rozwiązanie problemu badawczego w kontekście opracowania metody oceny bezpieczeństwa dla urządzeń IACS (realizacja celu szczegółowego C3), która implementuje wyniki adaptacji metodyki Common Criteria do zastosowań przemysłowych (cel szczegółowy C2).

Zaproponowane rozwiązanie powstało dzięki zastosowaniu metody krytycznej oceny i analizy oraz metody analizy i konstrukcji logicznej. Metoda krytycznej oceny i analizy umożliwiła wybór najlepszego wariantu rozwiązania problemu badawczego. Natomiast metoda analizy i konstrukcji logicznej została wykorzystana do określenia etapów metody oceny, umożliwiających wydawanie werdyktów z oceny wymagań bezpieczeństwa dla IACS.

Rozwiązanie problemu uzyskano w wyniku realizacji następujących etapów:

1) Krytyczna ocena i analiza w celu wyboru wariantu rozwiązania
2) Opracowanie metody oceny bezpieczeństwa IACS
3) Przykład teoretyczny zastosowania metody

W kolejnych podrozdziałach przedstawiono sposób realizacji powyższych etapów.

5.1. Wybór optymalnego wariantu

W rozdziale za pomocą krytycznej oceny i analizy wariantów zostanie zaproponowane najbardziej odpowiednie rozwiązanie służące opracowaniu metody oceny, ze względu na dostępne możliwości realizacji w ramach doktoratu.

Rodzina norm Common Criteria wspomagana jest przez dokumenty dodatkowe, m.in. przez metodykę oceny CEM, którą opisano w międzynarodowym standardzie ISO/IEC 18045 [8]. Znormalizowana metodyka oceny, jaką jest CEM, nie musi być dodatkowo walidowana, np. w celu uzyskania przez laboratorium oceniające akredytacji do jej stosowania w badaniach. Laboratorium musi wykazać wystarczające kompetencje techniczne i wiedzę do stosowania metodyki, natomiast sama metoda już nie podlega walidacji, tak jak to ma miejsce w przypadku nowych metod, nieujętych jeszcze w dokumentach normatywnych.

Biorąc pod uwagę ten fakt oraz to, że metodyka CEM wspiera stosowanie standardu Common Criteria, to wydaje się najlepszym wyborem jako podstawa dla metody oceny dla IACS. Należy jednak ustalić, w jakim kierunku poprowadzić proces adaptowania metodyki.

Do wyboru kierunku doskonalenia zastosowano metodę krytycznej oceny i analizy zaproponowanego wariantu. Metoda zawiera trzy główne fazy:

1. Faza przygotowania, która obejmuje:
    a. Określenie przedmiotu badań;
    b. Określnie czynników przedmiotu badań, które zostaną poddane analizie.
2. Faza diagnozy, która obejmuje:

   a. Krytyczną analizę stanu faktycznego przedmiotu badań;
   b. Uzasadnienie stosowania rozwiązań w obecnym stanie.
3. Faza prognozowania, która obejmuje:
   a. Opracowanie propozycji wariantów usprawnień;
   b. Wybór i uzasadnienie wariantu optymalnego.

W fazie przygotowania ustalono, że przedmiotem badań będzie metodyka oceny CEM, a analizowanymi czynnikami są:

- Cel – cel i motywacja stosowania metody;
- Miejsce – lokalizacja stosowania metody;
- Wykonawcy – personel używający metodę;
- Narzędzia – sprzęt niezbędny do realizacji metody;
- Normy i dokumentacja – źródła wymagań niezbędnych do stosowania metody;
- Sposób wykonywania – określone działania i kroki występujące w metodzie.

W fazie diagnozy wykonano krytyczną analizę stanu aktualnego stosowania metodyki CEM w laboratorium, zgodnie z ustalonymi czynnikami, której wyniki przedstawia tabela 25.

Tabela 25. Analiza stanu faktycznego stosowania metodyki CEM w ITSEF

Czynnik	**Charakterystyka metody**	**Uzasadnienie**
Cel	Ocena wymagań bezpieczeństwa IT zgodnie z Common Criteria	Celem głównym metody jest zapewnienie sformalizowanej, unormowanej i wspólnej metodyki do stosowania we wszystkich laboratoriach oceny bezpieczeństwa. W ten sposób zapewnia się obiektywność i porównywalność wyników ocen z różnych laboratoriów. Podnosi to jakość i zaufanie do certyfikatów bezpieczeństwa CC wydawanych na podstawie ocen z użyciem metody.
Miejsce	Laboratorium oceny bezpieczeństwa	Norma wymaga wykonywania badań w odpowiednio zabezpieczonym, wyposażonym i akredytowanym laboratorium ITSEF zgodnie z ISO/IEC 17025.
Wykonawcy	Pracownicy laboratorium	Badania powinien wykonywać personel posiadający odpowiednią wiedzę, doświadczenie i kwalifikacje.
Narzędzia	Wyposażenie laboratorium	Sprzęt i oprogramowanie muszą być odpowiednio dobrane, przygotowane, np. wzorcowane do realizacji badań i testowania produktów.
Normy i dokumentacja	Standard Common Criteria i dokumenty wspierające	Certyfikacja i ocena muszą być wykonywana zgodnie z wymaganiami norm i porozumień SOG-IS, CCRA, aby certyfikat był uznawany międzynarodowo.
Sposób wykonywania	Ocena wykonywana jest zgodnie z metodyką CEM, która określa czynności ewaluatora konieczne do wydania werdyktu oceny dla: 1. Dokumentacji 2. Testowania 3. Analizy podatności	W celu uzyskania certyfikatu bezpieczeństwa Common Criteria na danym poziomie EAL należy stosować metodykę oceny CEM wg klas uzasadnionego zaufania dla danego EAL: ASE, AGD, ADV, ALC, ATE, AVA – wszystkie klasy obejmują ocenę dokumentacji, testowanie i analizę podatności oraz określone działania ewaluatora niezbędne do oceny danego wymagania.

W fazie prognozy, dla wszystkich czynników, zaproponowano warianty usprawnień do obecnego sposobu stosowania metodyki CEM wraz z uzasadnieniami (tabela 26).

Tabela 26. Analiza wariantów usprawnień stosowania metodyki CEM w ITSEF

Czynnik	**Propozycje wariantów usprawnień**	**Wybór najlepszego wariantu**	**Uzasadnienie wyboru wariantu**
Cel	Dodanie możliwości oceny bezpieczeństwa dla IACS	Dodanie możliwości oceny urządzeń IACS.	Możliwość wydawania certyfikatów CC dla urządzeń IACS poszerzy ofertę usług oceny bezpieczeństwa laboratorium ITSEF. Producenci urządzeń IACS wyrażają zainteresowanie i chcą uzyskać certyfikat CC. Doświadczenie ze stosowania oceny dla IACS może stanowić punkt wyjścia do oceny kolejnych specyficznych typów urządzeń.
Miejsce	Bez zmian	Bez zmian	Laboratorium ITSEF jest odpowiednio przygotowane technicznie, proceduralnie i osobowo do wykonywania badań oceny bezpieczeństwa.
Wykonawcy	Zatrudnienie dodatkowego personelu; szkolenia obecnego zespołu laboratorium	Szkolenia personelu	Szkolenie personelu jest kosztowo bardziej dostępne niż pozyskanie nowych pracowników. Szkolenia stanowią inwestycję w kompetencje techniczne zespołu badawczego, które podlegają audytom prowadzonym przez PCA. Szkolenia pozwalają na poprawę jakości oferowanych usług oceny bezpieczeństwa.
Narzędzia	Zakup sprzętu i oprogramowania do testowania IACS, wykorzystanie możliwości obecnie posiadanego sprzętu	Wykorzystanie możliwości obecnego sprzętu	Tańsze rozwiązanie i w kontekście badania bezpieczeństwa IT może być wystarczające. Po ocenie pilotażowej i szkoleniach kompetencyjnych wykonana zostanie ponowna ocena identyfikacja potencjalnych inwestycji w sprzęt i oprogramowanie. Ewentualny zakup dodatkowych narzędzi nastąpi po ocenie i uzasadnieniu potrzeb.
Normy, dokumentacja	Zastosowanie norm: IEC 62443-4-1, IEC 62443-4-2, NIST SP-800-82 lub innych standardów przemysłowych	Wprowadzenie do stosowania norm IEC 62443-4-1 IEC 62443-4-2	Seria rodziny norm IEC 62433 przedstawia kryteria oceny bezpieczeństwa dla IACS w sposób znormalizowany i najbardziej zbliżony do metodyki CC, co ułatwia jej implementację w laboratorium ITSEF.
Sposób wykonywania	1) Opracować nową metodę dedykowaną do oceny bezpieczeństwa IACS w oparciu o standard przemysłowy; 2) zastosować obecnie wykorzystywaną do badań metodykę CEM na bazie dostosowanych wymagań CC p.2, p.3	**Zastosowanie obecnej metodyki CEM z wykorzystaniem dostosowanych wymagań CC**	Proponowane rozwiązanie jest najbardziej odpowiednie pod względem kosztów i czasu realizacji. Stosowana w ITSEF metodyka CEM nie musi być walidowana – jest określona normą ISO/IEC 18045. ITSEF posiada akredytację na stosowanie CC i CEM; CEM wspiera ocenę wymagań zdefiniowanych w CC p.3; standard CC można adaptować do specyficznych wymagań IACS; w dalszej kolejności można opracowywać metody oceny IACS na potrzeby profilu cPP dla IACS zgodnie z najnowszą normą CC p.4.

W wyniku krytycznej oceny stanu faktycznego i analizy zaproponowanych wariantów ulepszenia metodyki, zdecydowano o zastosowaniu obecnie stosowanej w ITSEF metodyki oceny CEM uzupełnionej o wymagania SAR i SFR, które zostały zaadaptowane do wymagań przemysłowych.

Argumenty świadczące za wybraną opcją doskonalenia można podsumować następująco:

- Metodyka CEM jest dedykowana dla standardu CC, który umożliwia adaptację wymagań do specyficznych zastosowań;
- Metodyka CEM jest znormalizowana i nie wymaga dodatkowej walidacji;
- Metodyka CEM stanowi źródło jednostek oceny, które można wykorzystać do tworzenia metod oceny dla IACS zgodnie z CC p.4;
- Metody oceny IACS utworzone zgodnie z CC p.4 mogą być stosowane w profilach zabezpieczeń cPP przeznaczonych dla IACS.

Argumenty przeciw wariantowi opracowania dedykowanej metody w oparciu o standard przemysłowy uzupełniony o wymagania dla systemów informatycznych są następujące:

- Standard przemysłowy IEC nie umożliwia adaptacji wymagań FR i Praktyk, czyli tworzenia wymagań rozszerzonych EXT jak w normie CC;
- Obecnie nie jest dostępna żadna znormalizowana metodyka oceny bezpieczeństwa dla IACS zgodnie z wymaganiami FR (IEC 62443-4-2) i Praktykami (IEC 62443-4-1);
- Opracowana w ten sposób metoda oceny podlega walidacji.

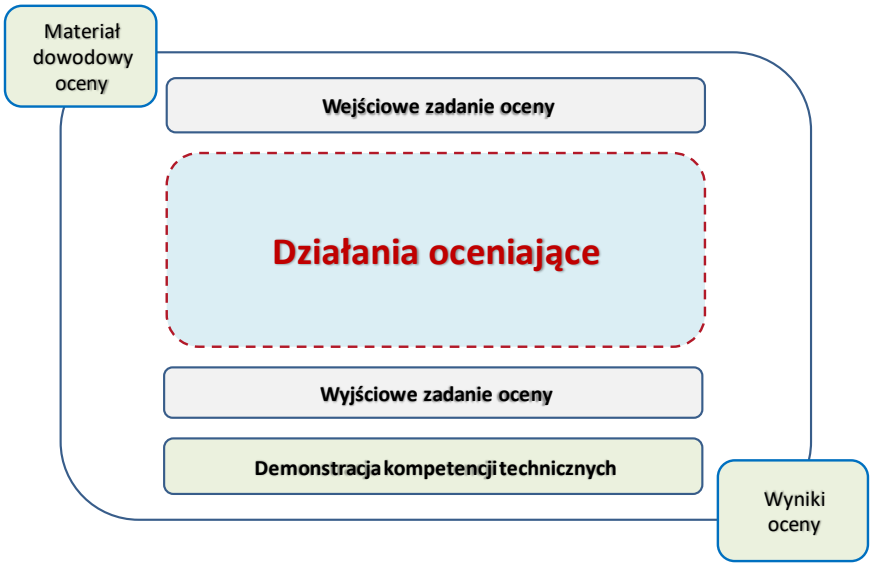
Podsumowując, do opracowania metody oceny bezpieczeństwa IACS wybrano wariant oparty o metodykę oceny CEM, która implementuje dostosowane wymagania CC. Ponadto standard CC i CEM jest już ugruntowany i mocno upowszechniony na rynku, w którym certyfikowane produkty mają przewagę konkurencyjną.

W kolejnym rozdziale przedstawiono ogólny model procesu oceny wg CEM, do którego zostanie włączona metoda oceny.

5.2. Ogólny model procesu oceny

Metoda oceny dla IACS, przeznaczona dla poziomów EAL 4 / SL 1, pozwala na ocenę wszystkich wymagań uzasadniających zaufanie SAR z danego pakietu EAL (zob. Tabela 18) łącznie z rozszerzonymi wymaganiami SAR_EXT, SFR_EXT (dla poziomu SL 1) z wykorzystaniem oryginalnych jednostek oceny WU metodyki CEM i dodatkowych jednostek rozszerzonych WU_EXT.

Model procesu oceny przedstawiony na rys. 6 na str. 40 jest zgodny z ogólnym modelem procesu oceny metodyki CEM [7], który wygląda następująco (rys. 13).



Rys. 13. Ogólny model procesu oceny CEM

Model składa się z zadania wejściowego i wyjściowego oceny, działań oceniających oraz demonstracji kompetencji technicznych. W modelu, materiał dowodowy oceny to z jednej strony dokumentacja produktu, która przekazywana jest do zadania wejściowego, a z drugiej strony, jest to dokumentacja zawierająca wyniki oceny, będąca produktem zadania wyjściowego oceny. Poszczególne elementy modelu scharakteryzowano poniżej.

1. **Wejściowe zadanie oceny –** celem tego zadania jest zapewnienie, że ewaluator otrzymał poprawną wersję produktu oraz jego dokumentacji niezbędną do wykonania oceny. W przeciwnym razie nie można zagwarantować technicznej dokładności oceny oraz tego, że ocena będzie dawała powtarzalne i odtwarzalne wyniki. W tym zadaniu ewaluator weryfikuje następujący materiał dowodowy dostarczony do oceny:
    a. TOE w konfiguracji przeznaczonej do oceny;
    b. Zadanie zabezpieczeń ST z deklaracją EAL;
    c. Dokumentacja użytkownika i projektowa włącznie z kodami źródłowymi;
    d. Dokumentacja z wykonanych testów TOE;
    e. Dokumentacja środowiska rozwojowego TOE.
2. **Działania oceniające –** celem tego zadania jest wykonanie przez ewaluatora czynności oceniających przewidzianych w jednostkach WU metodyki CEM, aby wydać werdykty dla wymagań SAR z pakietu EAL zadeklarowanego w ST. Dlatego też, zakres działań ewaluatora i ich rygoryzm różnią się w zależności od EAL. Działania oceniające obejmują następujące klasy wymagań SAR:
    a. ASE – ocena zadania zabezpieczeń ST;
    b. AGD – ocena dokumentacji użytkownika;
    c. ADV – ocena dokumentacji projektowej TOE;

d. ALC – ocena środowiska rozwojowego TOE;
e. ATE – ocena testów funkcjonalnych i wykonanie testów niezależnych;
f. AVA – analiza podatności i testy penetracyjne TOE.

3. **Demonstracja kompetencji technicznych –** wszelkie działania wykonane przez ewaluatorów w procesie oceny stanowią dowód i są informacjami wejściowymi dla jednostki certyfikującej (JC) do oceny kompetencji technicznych laboratorium. Proces jest realizowany przez JC, która analizuje i weryfikuje rezultaty oceny oraz wydaje swoją ocenę na temat kompetencji technicznych. JC może dodatkowo żądać od ewaluatorów prezentacji wyników lub powtórzenia czynności oceniających w celu zapewnienia, że wszystkie laboratoria w ramach schematu certyfikacji cyberbezpieczeństwa zapewniają porównywalny i adekwatny poziom kompetencji technicznych. Proces ten należy do odpowiedzialności JC i nie będzie tu szczegółowo opisywany.
4. **Wyjściowe zadanie oceny –** celem tego zadania jest opracowanie przez ewaluatora dwóch rodzajów dokumentów zawierających obserwacje i wyniki oceny: raportów uwag OR (ang. Observation Report), zwanymi także raportami uwag, oraz raportu technicznego oceny ETR (ang. Evaluation Technical Report). W celu utrzymania spójności raportowania, metodyka CEM określa strukturę i minimalną zawartość obydwu raportów.
    a. Raport uwag (OR) dla klienta – opracowywany w przypadku werdyktu negatywnego „Fail", spowodowanego brakami lub błędami w materiale dowodowym i wyrażający potrzebę wyjaśnienia i korekcji błędów przez producenta. Każdy raport OR powinien zawierać co najmniej następujące informacje:
        i. Identyfikator TOE, wersja, konfiguracja;
        ii. Jednostka WU, dla której sporządzono obserwację;
        iii. Treść obserwacji;
        iv. Ocena krytyczności obserwacji (np. skutkuje werdyktem negatywnym, wstrzymuje proces oceny, wymaga naprawy przed ukończeniem oceny);
        v. Organizacja odpowiedzialna za rozwiązanie problemu;
        vi. Sugerowany czas na rozwiązanie problemu;
        vii. Ocena wpływu na ocenę w przypadku braku rozwiązania obserwacji.
    b. Raport uwag (OR) dla JC – zawiera prośbę do JC o wyjaśnienie lub interpretację kwestii dotyczących stosowania danego wymagania z normy CC lub CEM;
    c. Raport techniczny oceny (ETR) – zawiera techniczne uzasadnienie wydanych werdyktów. CEM definiuje minimalną zawartość dokumentu, która pozwala

jednostce certyfikującej potwierdzić, że ocena została wykonana zgodnie z wymaganiami standardu. Strukturę dokumentu ETR przedstawia rys. 14.

Rys. 14. Struktura raportu ETR

Poszczególne sekcje zawierają następującą treść:

1. Wprowadzenie:
    a. Identyfikator i logo schematu certyfikacji;
    b. Identyfikator ETR, nazwa, data i numer wersji;
    c. Identyfikator zadania zabezpieczeń ST, data i numer wersji;
    d. Konfiguracja ST i TOE określająca zakres oceny;
    e. Deklaracja zgodności z profilami zabezpieczeń PP;
    f. Nazwa producenta i dane kontaktowe;
    g. Nazwa sponsora oceny i dane kontaktowe;
    h. Nazwa laboratorium oceniającego i dane kontaktowe;
2. Opis architektury TOE:
    a. Wysokopoziomowy opis głównych części TOE oparty o opis komponentów zgodnie z klasą ADV;
3. Ocena:
    a. Metody oceny, techniki, użyte narzędzia i standardy;
    b. Odniesienie do kryteriów oceny, metodyki i interpretacji lub urządzeń użytych do testowania TOE;

   c. Identyfikacja wszelkich ograniczeń oceny, ograniczeń w dostarczaniu wyników oceny i założenia, które miały wpływ na rezultaty oceny;
   d. Inne informacje dotyczące spraw prawnych, organizacyjnych lub poufności;
4. Wyniki oceny:
   a. Dla każdej czynności oceny ewaluator dostarcza informację o nazwie działania oceniającego wg CEM oraz werdykt dla każdego komponentu SAR wraz z uzasadnieniem;
   b. Informacje dotyczące wyników testowania (ATE) oraz analizy podatności (AVA) zgodnie z opisem WU dla tych klas.
5. Wnioski i rekomendacje:
   a. Wnioski z oceny odnoszące się do tego, czy TOE spełnia specyfikację wykazaną w zadaniu zabezpieczeń ST;
   b. Ewaluator podaje rekomendacje, które mogą być użyteczne dla JC i mogą np. zawierać wady produktu odkryte podczas oceny lub wskazywać na szczególnie użyteczne właściwości produktu.
6. Lista materiału dowodowego: dla każdego dokumentu należy wskazać wydawcę, tytuł i unikalny odnośnik (data, wersja).
7. Słownik terminów: należy podać definicje terminów, skrótów i akronimów użytych w ETR.
8. Raporty OR: należy wykazać kompletną listę unikalnie zidentyfikowanych raportów z obserwacji i ich status. Każdy OR powinien zawierać jego identyfikator, tytuł oraz krótkie podsumowanie jego zawartości.

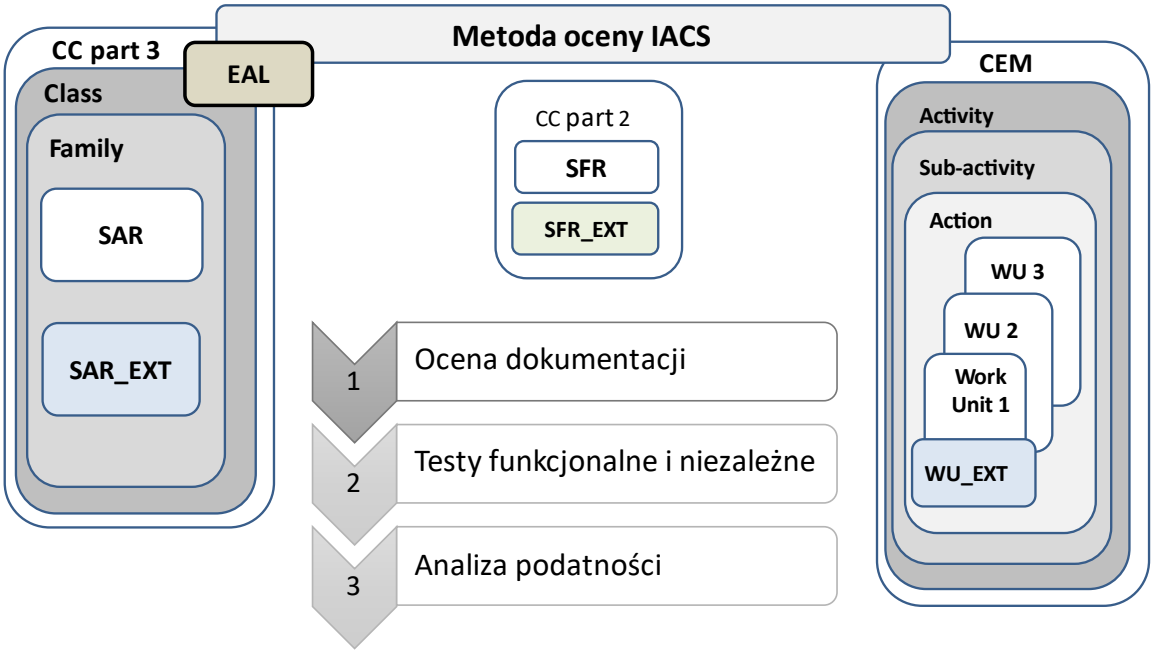
W kolejnym rozdziale przedstawiono metodę oceny dla IACS, za pomocą, której realizowane są działania oceniające kroku 2 w modelu procesu oceny.

5.3. Metoda oceny IACS

Metoda oceny IACS służy do realizacji działań oceniających w modelu procesu oceny.

W metodzie stosuje się zarówno oryginalne, niezmienione komponenty SFR, SAR z norm CC p.2 i CC p.3 oraz WU z CEM, jak i rozszerzone komponenty SAR_EXT i SFR_EXT oraz jednostki WU_EXT, a także działania EAs (Evaluation Activities) dla SFR_EXT.

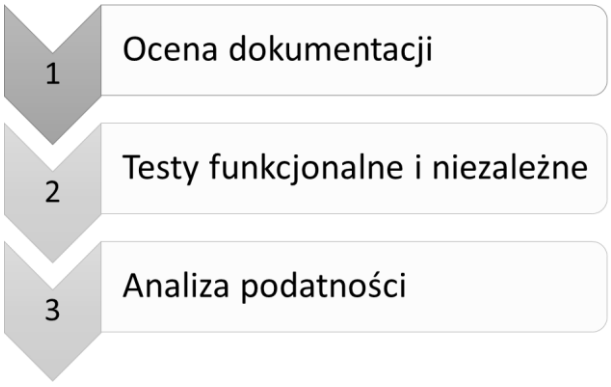
Uwzględniając wszystkie składowe zaadaptowanej metodyki Common Criteria i CEM, otrzymamy model metody dostosowanej do oceny IACS, jak pokazano na rys. 15.



Rys. 15. Model metody oceny IACS

Metodyka oceny CEM definiuje działania oceniające w postaci jednostek WU, które musi wykonać oceniający do oceny dokumentacji, testów wykonywanych przez producenta oraz nakazuje realizację testów niezależnych przez laboratorium. Ponadto metodyka określa czynności analizy podatności i testów penetracyjnych na danym poziomie EAL.

W związku z powyższym określono 3 główne kroki w metodzie oceny IACS (rys. 16), które w kolejnych rozdziałach będą szczegółowo przedstawione wraz z ich komponentami SAR i jednostkami oceny WU włącznie z ich uszczegółowionymi/rozszerzonymi wersjami oznaczanymi przyrostkiem EXT.



Rys. 16. Główne kroki metody oceny IACS

Kroki metody zawierają następujące działania oceniające:

1. Ocena dokumentacji – zawiera jednostki oceny dla klas ASE, AGD, ADV, ALC;
2. Testy funkcjonalne i niezależne – zawiera jednostki oceny dla klasy ATE;
3. Analiza podatności – zawiera jednostki oceny dla klasy AVA.

Poszczególne klasy wymagań dotyczą następujących elementów produktu:

- ASE – dokument zadania zabezpieczeń dla produktu;
- AGD – dokumentacja użytkownika, instalacji i uruchamiania;
- ADV – dokumentacja projektowa obejmująca: architekturę zabezpieczeń, specyfikację funkcjonalną, reprezentację implementacji, projekt podstawowy;
- ALC – dokumentacja cyklu życia produktu, dokumentacja systemowa środowiska wytwarzania i utrzymania produktu, dokumentacja systemu zarządzania konfiguracją i usuwaniem usterek;
- ATE – dokumentacja testów funkcjonalnych wykonanych przez producenta, wykonanie testów niezależnych wraz z dokumentacją przez laboratorium;
- AVA – wykonanie analizy podatności, testów penetracyjnych i opracowanie dokumentacji z wynikami wykonanych analiz wraz z wnioskami.

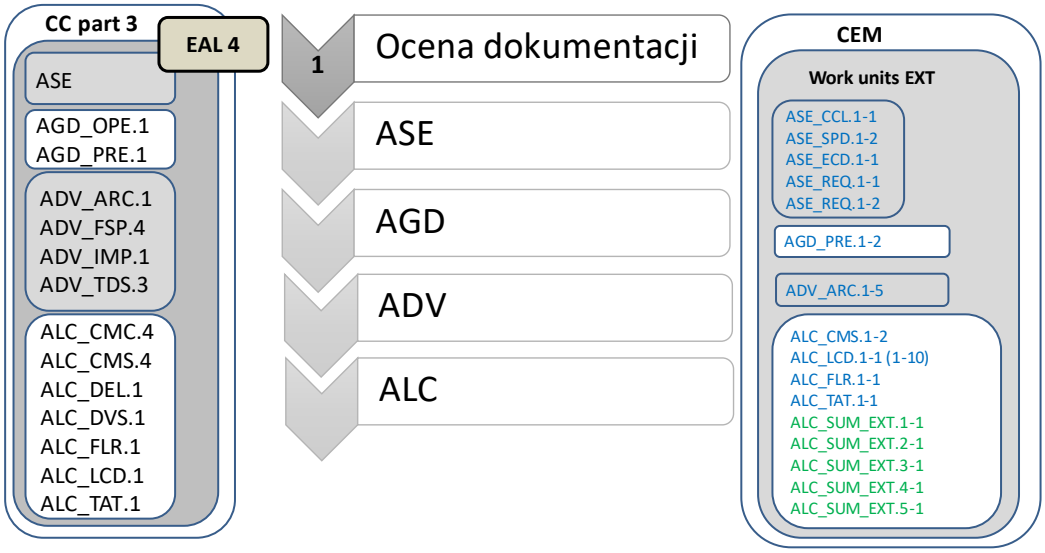
Ocena urządzenia na danym poziomie EAL będzie przebiegała zgodnie z przedstawionymi krokami i będzie dotyczyć oceny elementów w danym kroku.

W poniższych podrozdziałach przedstawiono kolejne kroki wraz z przykładami zastosowania. Przykłady będą dotyczyć poziomu EAL 4, w których zostaną zaprezentowane odpowiednie komponenty SAR, zgodnie z tabelą 18 zawierającą pakiety wymagań EAL.

Kroki metody będą opisywane w podrozdziałach 5.3.1 (krok 1 – ocena dokumentacji), 5.3.2 (krok 2 – testy funkcjonalne i niezależne), 5.3.3 (krok 3 – analiza podatności).

5.3.1. Ocena dokumentacji

Zgodnie z krokiem 1 modelu metody, dla poziomu EAL 4 będą obowiązywać następujące komponenty wymagań SAR z CC p.3 oraz jednostki oceny WU_EXT pokazane na rys. 17.



Rys. 17. Krok 1 - ocena dokumentacji

Po lewej stronie znajduje się lista wymagań SAR dla pakietu EAL 4 wybranych zgodnie z tabelą 18, natomiast po prawej stronie, znajduje się lista WU_EXT (uszczegółowionych/rozszerzonych) dla IACS, które należy uwzględnić podczas oceny.

W tym wypadku najważniejsze jest pokazanie zasady, że dla danego poziomu EAL dobiera się oprócz standardowych WU, także te, dostosowane do urządzeń IACS. Kolorem niebieskim oznaczone są WU powstałe w wyniku operacji uszczegółowienia komponentu SAR [*refinement*], natomiast zielonym oznaczono WU powstałe w wyniku utworzenia komponentu dodatkowego SAR_EXT, zgodnie z oznaczeniami zastosowanymi w tabelach mapowań.

W przypadku klasy ASE stosuje się standardowe WUs z CEM (tabela 27) oraz dostosowane WU_EXT (tabela 28) dla komponentów do oceny uzupełnionego ST dla IACS.

Tabela 27. Komponenty klasy ASE do oceny zadania zabezpieczeń

Assurance class	ASE component	Component description
ASE Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.1	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.2	Security problem definition
	ASE_TSS.1	TOE summary specification

Podczas oceny zadania zabezpieczeń należy zwrócić uwagę, czy w ST znajdują się informacje uzupełniające dla IACS, które zidentyfikowano w rozdz. 4.2 Uzupełnienie zadania zabezpieczeń. W celu oceny ST utworzono uszczegółowione [*refinement*] komponenty klasy ASE w rozdz. 4.4, których listę przedstawia poniższa tabela.

Tabela 28. Klasa ASE – lista uszczegółowionych SAR i WU dla oceny ST dla IACS

Class	Component	Element [*refinement*]	WU_EXT	EAL
ASE Security Target evaluation	**ASE_CCL.1** Conformance claims	ASE_CCL.1.1C [*refinement*]	ASE_CCL.1-1	1 - 7
	ASE_SPD.1 Security problem definition	ASE_SPD.1.2C [refinement]	ASE_SPD.1-2	1 - 7
	ASE_ECD.1 Extended component definition	ASE_ECD.1.1C [refinement]	ASE_ECD.1-1 (here: original WU)	1 - 7
	ASE_REQ.1 Security requirements	ASE_REQ.1.1C [refinement]	ASE_REQ.1-1 ASE_REQ.1-2	1 - 7

Dla komponentów AGD, ADV i ALC dobiera się komponenty rozszerzone oraz jednostki oceny z tabeli 29. W tabeli, kolumna EAL oznacza poziom, na którym należy stosować dane rozszerzenie, natomiast kolumna IEC 62443-4-1 przedstawia pomocniczo wymaganie, które było źródłem rozszerzenia.

Tabela 29. Ocena dokumentacji za pomocą klas rozszerzonych AGD, ADV, ALC

CC Class	CC SAR [*refinement*]/ EXT	CC WU_EXT	EAL	IEC 62443-4-1
AGD	AGD_PRE.1.1D [*refinement*] AGD_PRE.1.1C [*refinement*]	AGD_PRE.1-2	1 - 4	P8 SG-1, 2, 3
ADV	ADV_ARC.1.1D [*refinement*] ADV_ARC.1.5C [*refinement*]	ADV_ARC.1-5	2 - 4	P3 SD-2
ALC	ALC_FLR.1.1D [*refinement*] ALC_FLR.1.1C [*refinement*]	ALC_FLR.1-1	1 - 4	P6 DM-6
	ALC_TAT.1.1C [*refinement*]	ALC_TAT.1-1	4	P4 SI-2
	ALC_CMS.1.2C [*refinement*]	ALC_CMS.1-2	1 - 4	P1 SM-9, 10
	ALC_LCD.1.1C [*refinement 1*]	ALC_LCD.1-1(1)	3, 4	P1 SM-4
	ALC_LCD.1.1C [*refinement 2*]	ALC_LCD.1-1(2)	3, 4	P1 SM-5
	ALC_LCD.1.1C [*refinement 3*]	ALC_LCD.1-1(3)	3, 4	P1 SM-12, 13
	ALC_LCD.1.1C [*refinement 4*]	ALC_LCD.1-1(4)	3, 4	P2 SR-1
	ALC_LCD.1.1C [*refinement 5*]	ALC_LCD.1-1(5)	3, 4	P2 SR-2
	ALC_LCD.1.1C [*refinement 6*]	ALC_LCD.1-1(6)	3, 4	P2 SR-3, 4, 5
	ALC_LCD.1.1C [*refinement 7*]	ALC_LCD.1-1(7)	3, 4	P3 SD-3
	ALC_LCD.1.1C [*refinement 8*]	ALC_LCD.1-1(8)	3, 4	P3 SD-4
	ALC_LCD.1.1C [*refinement 9*]	ALC_LCD.1-1(9)	3, 4	P4 SI-1
	ALC_LCD.1.1C [*refinement 10*]	ALC_LCD.1-1(10)	3, 4	P8 SG-4
	ALC_SUM_EXT.1	ALC_SUM_EXT.1-1	1 - 4	P7 SUM-1
	ALC_SUM_EXT.2	ALC_SUM_EXT.2-1	1 - 4	P7 SUM-2
	ALC_SUM_EXT.3	ALC_SUM_EXT.3-1	1 - 4	P7 SUM-3
	ALC_SUM_EXT.4	ALC_SUM_EXT.4-1	1 - 4	P7 SUM-4
	ALC_SUM_EXT.5	ALC_SUM_EXT.5-1	1 - 4	P7 SUM-5

W kolejnym kroku ewaluator musi zapoznać się z treścią wymagania danego komponentu SAR i jego elementami D, C i E, a następnie zrealizować działania (jednostki oceny), które umożliwią mu wydanie werdyktu dla danego elementu E wymagania SAR.

Na przykład, aby ocenić wymaganie komponentu ALC_LCD.1 (2) [*refinement*] należy odnieść się do tabeli 36 i odnaleźć opis wymagania i jednostki oceny, tak jak na poniższym rys.18 pokazującym fragment tabeli mapowania.

Adapted SAR	Adapted C element	Adapted Work unit
ALC_LCD.1 [*refinement 2*] Developer defined life-cycle model	**ALC_LCD.1.1C** [*The life-cycle definition documentation shall include justification by documented security analysis to identify the parts of IEC 62443-4-1 and IEC 62443-4-2 documents that are applicable to a selected product development project*]	ALC_LCD.1-1 (2) Evaluation activities [*The evaluator shall examine the documented description of the life-cycle model used to determine that it covers parts of standards IEC 62443-4-1 and IEC 62443-4-2 the product claims conformance*]

Rys. 18. Fragment tabeli 30 z przykładem ALC_LCD.1

Powyższe wymaganie SAR w elemencie C, który określa postać i zawartość materiału dowodowego, nakazuje, aby dokumentacja cyklu życia produktu posiadała zapis o zakresie stosowanych wymagań przemysłowych podczas rozwoju produktu. Jednostka oceny nakazuje ewaluatorowi sprawdzenie wskazanej dokumentacji, czy takie zapisy się w niej znajdują. Jeśli weryfikacja będzie pozytywna, to ewaluator przyznaje werdykt „Pass" dla danej WU i uzasadnia werdykt.

Należy tu podkreślić, że wszystkie werdykty, dla wszystkich komponentów, rodzin i klas muszą być pozytywne, żeby ocena końcowa była pozytywna (zob. Rys. 12).

Dla pełnego obrazu przedstawiono przykład oceny komponentu rozszerzonego **ALC_SUM.EXT.1** – Security update qualification, który wymaga kwalifikowania aktualizacji zabezpieczeń urządzenia do rozpowszechniania, rys.19.

W tym przykładzie mamy do czynienia z komponentem, w którym mamy także nowe elementy D, C i E. Element D mówi, co producent lub konstruktor muszą dostarczyć jako materiał do oceny. W tym wypadku jest to udokumentowany proces kwalifikacji aktualizacji. Element C określa, co powinno się znaleźć w tej dokumentacji, np. 1) aktualizacje dotyczące przewidywanych podatności, 2) wyniki weryfikacji aktualizacji, czy nie cofają poprzednich aktualizacji.

Class	SAR_EXT	WU_EXT
ALC Life-cycle support	**ALC_SUM_EXT.1 - Security update qualification** ATE_SUM_EXT.1.1D [The developer shall provide documentation for security update qualification including confirmation that update is not contradicting to operational or legal constraints] ALC_SUM_EXT.1.1C [The documentation of security update qualification shall include 1) security updates created by the product developer addressing the intended security vulnerabilities; 2) the results of updates verification that they do not introduce regressions including patches created by: a) the product developer; b) suppliers of dependent components] ALC_SUM_EXT.1.1E [The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence]	**ALC_SUM_EXT.1-1** Evaluation activities [The evaluator shall check that the qualification documentation includes confirmation that updates do not contradict operational, safety or legal constraints] [The evaluator checks the qualification documentation whether there are evidence that security updates do not introduce regressions] [The evaluator checks the documentation if it includes a confirmation that patches applicable to the product are evaluated to ensure that they do not adversely affect operation of the product]

Rys. 19. Fragment tabeli 30 z przykładem ALC_SUM_EXT.1

Jednostka oceny **ALC_SUM_EXT.1-1** określa w jaki sposób ewaluator ma sprawdzić, czy określone informacje zostały zawarte w dokumentacji.

W celu ukończenia oceny dokumentacji należy w ten sam sposób wykonać ocenę i wydać werdykty dla wszystkich komponentów SAR i SAR_EXT na danym poziomie EAL.

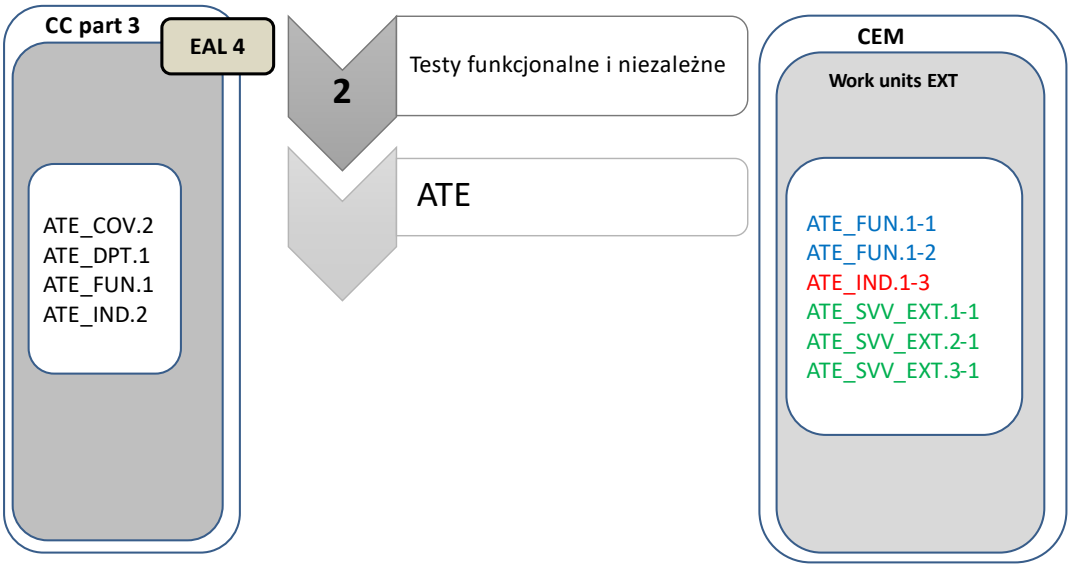
W kolejnym kroku metody wykonuje się ocenę wymagań dotyczących testowania.

5.3.2. Testy funkcjonalne i niezależne

Według modelu metody, dla testów funkcjonalnych i niezależnych realizowanych zgodnie z poziomem EAL 4, będą obowiązywać następujące komponenty wymagań SAR z CC p.3 oraz jednostki oceny WU_EXT (uszczegółowione/rozszerzone) pokazane na rys. 20.

W przypadku klasy ATE, oceniane są następujące komponenty wymagań SAR:

- ATE_COV.2 (Analysis of coverage) – określa zakres pokrycia testami interfejsów podanych w specyfikacji funkcjonalnej (interfejsów podsystemów i modułów wymuszających funkcje zabezpieczające TSF);
- ATE_DPT.2 (Testing: basic design) – określa szczegółowość, tzn. głębokość, testowania zgodnie ze specyfikacją projektu (uwzględnia testy dla wszystkich podsystemów i modułów wymuszających funkcje zabezpieczające TSF).



Rys. 20. Krok 2 - testy funkcjonalne i niezależne

- ATE_FUN.2 (Functional testing) – specyfikuje testy funkcjonalne (procedury, scenariusze, oczekiwane rezultaty).
- ATE_IND.2 (Independent testing – sample) – określa wymagania dla testowania niezależnego – testy funkcjonalne producenta powtarzane kontrolnie i testy niezależne opracowywane przez personel laboratorium.

Oprócz związanych z powyższymi komponentami standardowymi WU z CEM należy uwzględnić dodatkowo komponenty uszczegółowione/rozszerzone zgodnie z tabelą poniżej.

Tabela 30. Testowanie TOE za pomocą rozszerzonej klasy ATE

CC Class	CC SAR [*refinement*]/ EXT	CC WU_EXT	EAL	IEC 62443-4-1
ATE	ATE_FUN.1.1C [*refinement*]	ATE_FUN.1-1	2 - 4	P5 SVV-5
	ATE_FUN.1.2C [*refinement*]	ATE_FUN.1-2	2 - 4	P5 SVV-1
	ATE_IND.1.2E [*refinement*]	ATE_IND.1-3	1 - 4	P5 SVV-1
	ATE_SVV_EXT.1	ATE_SVV_EXT.1-1	1 - 4	P5 SVV-2
	ATE_SVV_EXT.2	ATE_SVV_EXT.2-1	1 - 4	P5 SVV-3
	ATE_SVV_EXT.3	ATE_SVV_EXT.3-1	1 - 4	P5 SVV-4

W celu oceny testów funkcjonalnych, wykonanych przez producenta, należy uwzględnić komponent ATE_FUN.1 oraz ATE_IND.1 [*refinement*] wraz z jednostkami oceny, jak pokazano na rys. 21 obrazującym fragment tabeli 36.

Adapted SAR	Adapted C element	Adapted Work unit
ATE_FUN.1 [*refinement*] Functional testing	**ATE_FUN.1.2C** [*The test plan shall identify tests for verifying that the product handles error scenarios and invalid input correctly. Types of testing shall include a) functional testing of security requirements defined by Foundational Requirements (FRs) for IACS, b) performance and scalability testing, and c) boundary/edge condition, stress and malformed or unexpected input tests*]	**ATE_FUN.1-2** Evaluation activity [*The evaluator shall examine the test plan to determine that it describes the scenarios for performing each type of tests according to Foundational Requirements (FRs) for IACS components*]
ATE_IND.1 [*refinement*] Independent testing - conformance	**ATE_IND.1.2E** [*The evaluator shall test the TSFs to confirm they operate as specified by SFRs derived from Foundational Requirements (FRs) for IACS components*]	**ATE_IND.1-3** Evaluation activity [*The evaluator shall devise a test subset for TSFs defined by SFRs derived from Foundational Requirements (FRs) for IACS components. The evaluator shall produce a test subset documentation which includes expected results, actual results and acceptance criteria*]

Rys. 21. Fragment tabeli 32 z przykładem ATE_FUN.1 oraz ATE_IND.1

ATE_FUN.1.2C po operacji uszczegółowienia wymaga, aby plan testów zawierał testy weryfikujące, czy urządzenie poprawnie realizuje obsługę błędów i błędnych wejść. Testy powinny zawierać, np. testowanie funkcjonalne zgodnie z wymaganiami fundamentalnymi FR i CR z normy IEC 62443-4-2.

Jednostka oceny **ATE_FUN.1-2** nakazuje ewaluatorowi zweryfikować plany testów, czy stosują wymagania FR i CR z normy IEC 62443-4-2. Po wykonaniu tej czynności, ewaluator wydaje werdykt dla elementu E wymagania ATE_FUN.1.1E.

Przykład komponentu ATE_IND.1 (Independent testing – conformance) dotyczy testów niezależnych wykonywanych w laboratorium. Celem tego komponentu jest wykazanie, że TOE działa zgodnie ze swoim projektem i dokumentacją użytkownika. Komponent i jego elementy wyróżniono kolorem czerwonym, ponieważ ocena tego wymagania została zrealizowana w etapie walidacji metody i wyników oceny pilotażowej.

Element działania ewaluatora ATE_IND.1.2E mówi, że ewaluator musi wykonać testy funkcji zabezpieczających TSF, aby potwierdzić, że działają one zgodnie z wymaganiami SFR_EXT dostosowanymi do wymagań FR i CR z normy IEC 62443-4-2. Funkcje TSF implementujące SFR_EXT są wykazywane w zadaniu zabezpieczeń w sekcjach ECD (Extended Component Definition), REQ (Security requirements) oraz TSS (TOE summary specification), zob. rozdz. 4.2 Uzupełnienie zadania zabezpieczeń.

Jednostka oceny ATE_IND.1-3 zawiera działanie, które nakazuje ewaluatorowi wykonanie testów funkcji TSF zgodnie z przygotowanym planem testów, zawierającym kryteria akceptacji, oczekiwane i rzeczywiste wyniki testów.

Wydanie werdyktu dla tej jednostki oceny było możliwe na podstawie wyników testów wykonanych podczas oceny pilotażowej. Załączone do pracy sprawozdanie z pilotażu zawiera

przykładowe plany testów, warunki akceptacji i otrzymane rzeczywiste wyniki testów wymagań CR z normy IEC 62443-4-2.

Ewaluator, wykonując wszystkie czynności zdefiniowane w ATE_IND.1-3 ma podstawy do wydania werdyktu dla elementu ATE_IND.1.1E. Należy pamiętać, że aby wydać ocenę końcową dla komponentu ATE_IND.1, należy wykonać jeszcze ocenę zgodnie ze wszystkimi jednostkami WU przypisanymi do elementu ATE_IND.1.2E. Natomiast, aby wydać werdykt dla całej klasy ATE na poziomie EAL 4, należy ocenić wszystkie wymienione na rys. 20 komponenty z wykorzystaniem ich jednostek oceny, m.in. dla rodziny dodatkowej ATE_SVV_EXT (Testowanie w celu weryfikacji i walidacji bezpieczeństwa).

Standard Common Criteria nie narzuca konstruktorowi obowiązku wykonywania analizy podatności i testów penetracyjnych, aczkolwiek jest to zawsze zalecane. Zgodnie z CC takie działania musi wykonać laboratorium w zakresie wymagań klasy AVA.

Natomiast norma IEC 62443-4-2 w Praktyce 5 narzuca na konstruktora obowiązek wykonywania analizy podatności i testów penetracyjnych. W celu zapewnienia w metodzie oceny możliwości weryfikacji tego wymagania utworzono trzy rozszerzone komponenty ATE_SVV_EXT.1, 2, 3 wraz z jednostkami oceny. Rozszerzona rodzina ATE_SVV_EXT powstała w klasie ATE, a nie w klasie AVA, ponieważ dotyczy oceny testów wykonywanych przez producenta, podczas gdy klasa AVA przeznaczona jest tylko dla laboratorium.

Następnym krokiem w metodzie oceny jest analiza podatności, którą omówiono w kolejnym rozdziale.

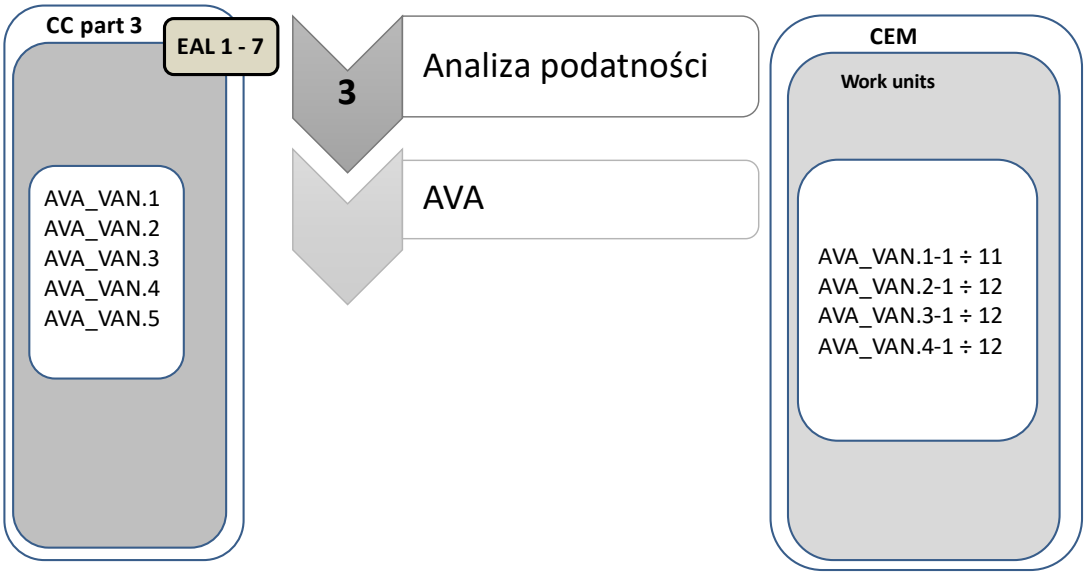
5.3.3. Analiza podatności

Trzecim krokiem metody oceny jest analiza podatności zgodnie z klasą wymagań AVA (Vulnerability assessment). W tym etapie ocena przebiega dokładnie według metodyki CEM bez żadnych modyfikacji, z jednym uzupełnieniem w postaci tabeli 32 mapującej poziomy bezpieczeństwa SL na potencjał ataku. Tabela powstała w początkowej fazie pracy doktorskiej, na podstawie metody opracowanej przez TeleTrust [87].

W pracy utworzono także dodatkową tabelę 33, ilustrującą poziomy bezpieczeństwa aktu CSA [37], EAL i SL w relacji do wartości potencjału ataku obliczanego według CEM.

Na poziomach od EAL 1 do EAL 5 stosuje się 4 komponenty: AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, a każdy z nich posiada od 11 do 12 jednostek oceny WU (zob. Rys. 22).

Na poziomach EAL 6 i EAL 7 obowiązuje jeden komponent AVA_VAN.5, dla którego metodyka CEM nie podaje jednostek WU, jak w przypadku pozostałych. CEM podaje konieczność odbycia konsultacji w tym zakresie z jednostką zarządzającą schematem certyfikacji obowiązującym w danym kraju, który ustala zasady wykonywania testów penetracyjnych o wysokim potencjale. Dla wysokiego potencjału ataku trudno opracować jest uniwersalny sposób postępowania przy opracowywaniu i realizowaniu scenariuszy testowych.



Rys. 22. Krok 3 – analiza podatności

Celem klasy AVA jest ocena, czy potencjalne podatności zidentyfikowane w trakcie oceny procesu projektowania lub oceny przewidywanego środowiska operacyjnego TOE, mogą umożliwić atakującym naruszenie wymagań SFR. Szczegółowy opis wymagań rodziny AVA_VAN i jej wszystkich komponentów można znaleźć w CC p.3 [3] oraz w CEM [7], poniżej przedstawiono najważniejsze cele komponentów:

- AVA_VAN.1 (Vulnerability survey) – wymaganie obowiązuje dla EAL 1 i nakazuje ewaluatorowi wykonanie przeglądu publicznie dostępnych źródeł informacji o podatnościach w celu ustalenia, jakie potencjalne podatności mogą zostać odkryte i wykorzystane przez agenta zagrożenia; ponadto, oceniający musi wykonać testy penetracyjne zakładając podstawowy potencjał ataku (Basic) – zob. Równanie 1. Obliczanie potencjału ataku.
- AVA_VAN.2 (Vulnerability analysis) – wymaganie obowiązuje dla EAL 2 i EAL 3 oraz nakazuje ewaluatorowi wykonanie analizy na bazie dokumentacji użytkownika, specyfikacji funkcjonalnej i projektu TOE w celu ustalenia, czy występują potencjalne podatności w produkcie. Ewaluator wykonuje także testy penetracyjne, aby potwierdzić, że potencjalne podatności nie mogą być wykorzystane w środowisku operacyjnym TOE. Testy penetracyjne w wypadku tego komponentu wykonywane są przy założeniu podstawowego potencjału ataku (Basic).
- AVA_VAN.3 (Focused vulnerability analysis) – wymaganie obowiązuje dla EAL 4 i nakazuje ewaluatorowi, m.in. wykonanie testów penetracyjnych przy założeniu rozszerzonego-podstawowego potencjału ataku (Enhanced-Basic).

- AVA_VAN.4 (Methodical vulnerability analysis) – wymaganie obowiązuje dla EAL 5 i nakazuje ewaluatorowi, m.in. wykonanie testów penetracyjnych przy założeniu średniego potencjału ataku (Moderate).
- AVA_VAN.5 (Advanced methodical vulnerability analysis) – wymaganie obowiązuje dla EAL 6 i EAL 7 i nakazuje ewaluatorowi, m.in. wykonanie testów penetracyjnych przy założeniu wysokiego potencjału ataku (High), komponent nie ma zdefiniowanych jednostek oceny WU w CEM.

Z powyższych wymagań wynika, że ewaluator po identyfikacji potencjalnych podatności musi wykonać testy penetracyjne o zadanym potencjale ataku, w celu sprawdzenia czy podatności mogą być wykorzystane (ang. Exploitable) przez agenta zagrożenia.

Aneks B metodyki CEM zawiera ogólne wskazówki dla oceniających, jak obliczyć potencjał ataku na TOE dla przygotowywanych scenariuszy testów penetracyjnych.

Testy penetracyjne mają na celu ocenę praktyczną czy potencjalne podatności umożliwią atakującemu o określonym potencjale ataku, dokonać naruszenia wymagań bezpieczeństwa SFR. Inaczej mówiąc, czy podatności są możliwe do wykorzystania w środowisku operacyjnym TOE.

Dla każdego scenariusza ataku wykonuje się analizę w celu obliczenia odpowiedniego potencjału ataku. Wartość potencjału ataku rośnie wraz ze wzrastającą motywacją, zasobami i wiedzą atakującego. Potencjał ataku AP (ang. Attack potential) wystarczający do naruszenia TOE można wyrazić jako sumę następujących czynników, jak w równaniu 1:

$$AP = ET + SE + KT + WO + EQ$$

Równanie 1. Obliczanie potencjału ataku

- ET (ang. Elapsed Time) – upływ czasu, który określa czas potrzebny to identyfikacji i wykorzystania podatności w TOE;
- SE (ang. Specialist Expertise) – specjalistyczna wiedza i poziom technicznych kompetencji atakującego;
- KT (ang. Knowledge of the TOE) – wiedza o budowie i działaniu TOE;
- WO (ang. Window of opportunity) – okno dostępu, które określa zakres dostępu atakującego do TOE lub do określonej liczby jego egzemplarzy podczas prowadzenia ataku;
- EQ (ang. Equipment) – wyposażenie atakującego w narzędzia i sprzęt komputerowy, oprogramowanie lub inne urządzenia potrzebne do identyfikacji lub wykorzystania podatności.

W metodyce CEM wartości powyższych składników dobiera się na podstawie specjalnej tabeli z Aneksu B do metodyki CEM (zob. Tabela 31), którą przedstawiono poniżej.

Tabela 31. Obliczanie potencjału ataku wg CEM [7]

Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3[2]
Expert	6
Multiple Experts	8

Factor	Value
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	*[1]
Equipment	
Standard	0
Specialized	4[3]
Bespoke	7
Multiple bespoke	9

Na przykład, jeżeli dla danego scenariusza ataku, ustalimy wartości czynników na: ET = 4, SE = 3, KT = 3, WO = 4, EQ = 4, to otrzymamy wartość potencjału ataku AP = 18

Dalej, jeśli porównamy otrzymaną wartość z wartościami w tabeli 33 w kolumnie „***Attack potential value***”, to zauważymy, że AP=18 znajduje się w przedziale 14 – 19. Przedział ten według kolumny „***Attack potential required to exploit vulnerability***” oznacza średni potencjał ataku (Moderate), który wykorzystuje podatność TOE i przełamuje zabezpieczenia.

Wartości w kolumnach „***Attack potential value***”, „***Attack potential required to exploit vulnerability***” oraz “***TOE resistant to attackers with attack potential of***” zostały przeniesione z metodyki CEM (Table 4 Rating of vulnerabilities and TOE resistance) i są one wykorzystywane podczas oceny komponentów rodziny AVA_VAN.

Tabela 33 została opracowana także po to, aby w jednym miejscu zilustrować wszystkie poziomy bezpieczeństwa w relacji do wartości potencjału ataku z CEM. Tabela 33 zawiera poziomy bezpieczeństwa określone w akcie CSA, poziomy EAL z Common Criteria i poziomy SL z IEC 62443-4-2.

[1] When several proficient persons are required to complete the attack path, the resulting level of expertise still remains “proficient” (which leads to a 3 rating).

[2] Indicates that the attack path is not exploitable due to other measures in the intended operational environment of the TOE.

[3] If clearly different test benches consisting of specialized equipment are required for distinct steps of an attack, this should be rated as bespoke.

Tabela 33 zawiera także wyniki przedstawione w tabeli 32, która zawiera poziomy SL i oszacowane dla nich wartości potencjału ataku zgodnie z CEM przez autorów metody TeleTrust.

W akcie CSA określono poziomy bezpieczeństwa jako: podstawowy (ang. Basic), istotny (ang. Substantial) i wysoki (ang. High) i zostały one powiązane z wartościami potencjału ataku określonymi w komponentach AVA_VAN zgodnie z CEM.

Ustalono, że poziomowi wysokiemu (High) będą odpowiadać wymagania dotyczące analizy podatności zdefiniowane w komponentach AVA_VAN.3 i AVA_VAN.4, co oznacza, że TOE jest odporne na ataki o potencjale co najmniej Enhanced-Basic i wyższym. Natomiast dla poziomu istotnego (Substantial) są to wymagania AVA_VAN.1 i AVA_VAN.2, co oznacza, że TOE jest odporne na ataki o potencjale co najmniej podstawowym (Basic).

Poziomowi „Basic" w CSA nie przypisano żadnego komponentu AVA, więc nie odpowiada on żadnej wartości potencjału ataku i tym samym nie przypisano go do żadnego z poziomów EAL, co oznaczono w tabeli 33 jako „No rating" w kolumnie „**CC EALs**".

Sytuacja ta wynika z tego, że na poziomie Basic, akt CSA dopuszcza deklarację własną producenta o zgodności z wymaganiami bezpieczeństwa i w związku z tym nie wymaga się od producentów stosowania metodycznego podejścia do analizy podatności na tym poziomie.

Tabela 32 zawiera poziomy SL zdefiniowane w normie IEC 62443-4-2. Zostały one przypisane do wartości obliczonych zgodnie z CEM w wyniku analizy wykonanej przez firmę TeleTrust [87]. Wyniki zawarte w tabeli 32 oraz ich uzasadnienia należy czytać łącznie z definicjami opisowymi poziomów SL, które zostały przedstawione w rozdz. 4.3 niniejszej pracy. Wartość dla poziomu SL 4 została obliczona przez doktoranta na bazie przyjętych przez niego wartości czynników, ponieważ autorzy nie uwzględnili w metodzie poziomu SL 4.

Tabela 32. Obliczenie potencjału ataku dla poziomów SL

Poziom bezpieczeństwa SL	**Potencjał ataku**	**Obliczenia i uzasadnienie**
SL 1	> 0	Założony potencjał ataku stosowany jest tylko do niekierowanych, przypadkowych ataków; oznacza to, że jakakolwiek podatność naruszająca już podstawowe wymaganie CR (które znajduje się na poziomie SL 1) zostaje przypisana do poziomu SL 1.
SL 2	>4	Niski potencjał ataku oznacza, że czas jest decydującym czynnikiem, założono zatem, że mniej niż 1 miesiąc na zaprojektowanie i wykonanie ataku jest tu uzasadnione. W tabeli CEM (zob. Tabela 31 wyżej) czas 1 jednego miesiąca został określony na 4 punkty.
SL 3	>14	Założony średni potencjał ataku ma wartość 14 punktów, która wynika z czasu na atak ustalonego na 2 miesiące (7 pkt), wiedza specjalistyczna (3 pkt) lub dostęp do zastrzeżonych danych (także 3 pkt), plus dodatkowo specjalistyczny sprzęt (4 pkt). Łącznie zatem otrzymano 14 pkt.

SL 4	>20	Na tym poziomie zakłada się wysoki potencjał ataku realizowanego za pomocą zaawansowanych środków (zamawiane wyposażenie - 7 pkt), a sprawca dysponuje umiejętnościami specyficznymi dla IACS (wiedza specjalistyczna - 6 pkt) i wysoką motywacją (dwa miesiące - 7 pkt), co łącznie daje wynik 20 pkt.

Wartości potencjału ataku z tabeli 32 wraz z poziomami SL zostały włączone do tabeli 33, bez zmiany oryginalnych wartości z CEM, do kolumny „***Attack potential value***" dla poziomów od EAL 1 do EAL 7.

Tabela 33 może być wykorzystana podczas oceny czy urządzenie IACS spełnia warunek odporności na dany potencjał ataku określony poziomem SL lub poziomem EAL, dokładnie według podejścia CEM. Wniosek ten stanowi wartość dodaną niniejszej pracy, ponieważ metoda oceny dla IACS może być zastosowana do oceny podatności także z punktu widzenia przemysłowego poziomu bezpieczeństwa SL.

Ostatecznie, to wynik analizy podatności i testów penetracyjnych będzie decydował, czy komponent IACS jest w stanie zapewnić ochronę przed atakiem o wskazanym potencjale za pomocą funkcji zabezpieczających TSF implementujących wymagania CR na zadeklarowanym poziomie SL.

Tabela 33. Analiza podatności z użyciem skali potencjału ataku

CSA security levels	**CC AVA assurance component satisfied**	**CC EALs**	**IEC SLs**	**Attack potential value**	**Attack potential required to exploit vulnerability**	**TOE resistant to attackers with attack potential of**
Basic	No component satisfied	No rating	SL 1	0 - 4	Basic	No rating
			SL 2	5 - 9		
Substantial	AVA_VAN.1 Vulnerability survey	EAL 1	SL 2	10 - 13	Enhanced-Basic	Basic
	AVA_VAN.2 Vulnerability analysis	EAL 2				
		EAL 3				
High	AVA_VAN.3 Focused vulnerability analysis	EAL 4	SL 3	14 - 19	Moderate	Enhanced-Basic
	AVA_VAN.4 Methodical vulnerability analysis	EAL 5	SL 4	20 - 24	High	Moderate
	AVA_VAN.5 Advanced methodical vulnerability analysis	EAL 6		> 25	Beyond High	High
		EAL 7				

Poniżej przedstawiono przykład oceny komponentu AVA_VAN zgodnie z CEM. Przedstawione podejście można także zastosować do oceny urządzenia IACS.

Wartości w kolumnie „***Attack potential value***" zawierają wartość potencjału ataku dla danego scenariusza ataku, który jest konieczny, aby przełamać zabezpieczenia, inaczej podważyć wymagania funkcjonalne na zabezpieczenia (SFR).

Przykładowo, aby komponent AVA_VAN.3 na poziomie EAL 4 otrzymał werdykt pozytywny „Pass", to TOE musi być odporne na ataki Enhanced-Basic (zob. kolumna „***TOE resistant to attackers with attack potential of***"), czyli z potencjałem ataku o wartości od 10 do 13 punktów (zob. kolumna „***Attack potential required to exploit vulnerability***"). W takim przypadku, jeśli ewaluator przygotuje scenariusz ataku o wartości potencjału z tego zakresu (od 10 do 13), który w rezultacie wykorzysta podatność i przełamie zabezpieczenia, to werdykt dla komponentu AVA_VAN.3 będzie negatywny „Fail".

Będzie to oznaczało, że jeśli producent zadeklarował w zadaniu zabezpieczeń, że jego produkt jest odporny na ataki o potencjale Enhanced-Basic, czyli zadeklarował poziom EAL 4 dla produktu, a testy penetracyjne z tym potencjałem przełamią zabezpieczenia, to producent będzie musiał albo wprowadzić poprawki do funkcji zabezpieczających, albo obniżyć poziom EAL dla produktu. W ten sam sposób można przeprowadzić powyższą analizę dla produktu IACS w oparciu o poziomy SL, które zmapowano na wartości potencjału ataku zgodne z CEM.

Analiza podatności jest ostatnim krokiem metody oceny i zamyka cały proces, jednakże jest najbardziej kluczowym elementem, który realnie ocenia możliwości zabezpieczeń zaimplementowanych w urządzeniu do ochrony jego krytycznych zasobów.

W niniejszym rozdziale przedstawiono metodę oceny bezpieczeństwa dla IACS. Metoda rozwiązuje problem wynikający z braku ustandaryzowanej metodyki oceny przeznaczonej dla urządzeń z branży automatyki przemysłowej. Poprzez zastosowanie wymagań CC, dostosowanych do potrzeb przemysłowych, w metodyce CEM, która jest metodyką znormalizowaną, otrzymano metodę, która nie musi przechodzić dodatkowej walidacji w myśl ustaleń normy ISO/IEC 17025, która narzuca wymagania dotyczące kompetencji laboratoriów badawczych i wzorcujących.

Jednakże krok 2 metody, w którym wykonuje się testy funkcjonalne i niezależne, powinien być sprawdzony w praktyce. Służy on do weryfikacji czy funkcjonalności zabezpieczeń TSF urządzenia działają zgodnie z wymaganiami przemysłowymi. W kroku 2 wykonano testy wybranego urządzenia podczas oceny pilotażowej w laboratorium ITSEF.

Testy polegały na weryfikacji, czy urządzenie działa w sposób określony przez wymagania bezpieczeństwa FR i CR z normy IEC 62443-4-2. W tym celu opracowano plany testów wraz z warunkami akceptacji. Wyniki tych testów pozwalają wydać werdykt dla wymagania komponentu ATE_IND.1 dotyczącego niezależnych testów. W ten sposób krok 2 metody oceny został zweryfikowany w zakresie testów niezależnych.

Wszystkie rezultaty oceny muszą być udokumentowane w raporcie technicznym oceny ETR (ang. Evaluation Technical Report). Raport ETR przedstawia całościowy wynik oceny TOE wraz z uzasadnieniami werdyktów i jest przekazywany do jednostki certyfikującej. Jednostka certyfikująca, w procesie certyfikacji, dokonuje oceny otrzymanych z laboratorium wyników i podejmuje decyzję o wydaniu certyfikatu dla ocenianego produktu.

Dzięki rezultatom badań przedstawionym w niniejszym rozdziale, można stwierdzić, że cel szczegółowy C3 w postaci opracowania metody oceny bezpieczeństwa dla IACS został osiągnięty.

W kolejnym rozdziale zostanie przeprowadzona walidacja metody w kontekście modelowego procesu oceny zgodnego z CEM.

6. Walidacja metody oceny dla IACS

Rozdział przedstawia walidację metody oceny dla IACS zgodnie z poziomem uzasadnionego zaufania EAL 4 oraz poziomem bezpieczeństwa SL 1. Celem walidacji było potwierdzenie, że metoda jest odpowiednia do zastosowania w ocenie bezpieczeństwa urządzeń IACS. Zweryfikowano użyte w metodzie rozszerzone komponenty wymagań wraz z ich jednostkami oceny z punktu widzenia ich gotowości i dojrzałości do oceny materiału dowodowego zgodnego z Common Criteria. Innymi słowy, zweryfikowano, czy możliwe jest za ich pomocą wydanie werdyktu dotyczącego danego wymagania bezpieczeństwa.

Pozostałe wymagania bezpieczeństwa, dotyczące rozwiązań informatycznych, oceniane są standardowo z użyciem oryginalnych jednostek oceny CEM i nie będą tutaj prezentowane.

Walidację kolejnych kroków metody oceny wykonano zgodnie z modelem procesu oceny zaprezentowanym szczegółowo w rozdz. 5.2, który zawiera następujące etapy:

1. **Wejściowe zadanie oceny**
    a. Weryfikacja urządzenia IACS
    b. Weryfikacja zadania zabezpieczeń ST
    c. Weryfikacja dokumentacji użytkownika – AGD;
    d. Weryfikacja dokumentacji projektowa – ADV
    e. Weryfikacja dokumentacji cyklu życia i środowiska rozwojowego – ALC
    f. Weryfikacja dokumentacji testów funkcjonalnych – ATE_FUN
2. **Działania oceniające**
    a. Ocena ST
    b. Ocena AGD
    c. Ocena ADV
    d. Ocena ALC
    e. Ocena testów funkcjonalnych ATE_FUN
    f. Wykonanie testów niezależnych ATE_IND
    g. Analiza podatności AVA dodatkowo z uwzględnieniem SL

Krok 1 metody

Krok 2 metody

Krok 3 metody

3. **Demonstracja kompetencji technicznych**[4]
4. **Wyjściowe zadanie oceny**
    a. Opracowanie raportu uwag (OR);
    b. Opracowanie raport technicznego oceny (ETR).

W kolejnych podrozdziałach zostaną zaprezentowane czynności walidacyjne wykonane w kolejnych etapach procesu oceny.

[4] Etap nie będzie prezentowany – ocena kompetencji technicznych realizowana jest przez jednostkę certyfikującą.

6.1. Wejściowe zadanie oceny

Ewaluator w tym zadaniu musi zweryfikować przekazane do oceny TOE oraz dołączoną dokumentację. Na czynności ewaluatora składają się:

1. Weryfikacja wersji i konfiguracji TOE wraz z dokumentacją:
   a) TOE, na przykład – programowalny sterownik zabezpieczenia odległościowego dla stacji elektroenergetycznych z numerem seryjnym na tabliczce znamionowej;
   b) Wynik weryfikacji: w tym przypadku pozytywny, gdyż przekazano prawidłowe urządzenie zgodnie z umową.
2. Weryfikacja zadania zabezpieczeń ST;
   a) ST odnosi się do TOE przekazanego do oceny – sprawdza się nr wersji TOE, czy jest zgodny z ST;
   b) Sprawdzenie sekcji „Conformance claims", czy są odpowiednie deklaracje, np.:
      i) producent zadeklarował w ST poziom EAL 4 i SL 1;
      ii) producent zadeklarował zgodność z normami przemysłowymi IEC 62443-4-1, IEC 62443-4-2,
      iii) producent zadeklarował zgodność z CC p.2, CC p.3;
      iv) brak deklaracji zgodności z profilami zabezpieczeń PP
   c) Wynik weryfikacji: pozytywny; ST dotyczy przekazanego TOE.
3. Dokumentacja użytkownika
   a) Załączona dokumentacja: np. instrukcja sterownika, opis modułu komunikacyjnego, opis komunikacji ze sterownikiem za pomocą modułu komunikacyjnego;
   b) Dokumentacja jest aktualna, zawiera daty wydania i nr wersji, dokumentacja dotyczy typu urządzenia przekazanego do ewaluacji;
   c) Wynik weryfikacji: pozytywny, dokumentacja dotyczy przekazanego TOE.
4. Dokumentacja projektowa
   a) Producent załączył dokumentację projektową urządzenia;
   b) Wersja dokumentacji dotyczy przekazanego urządzenia i jest aktualna;
   c) Producent przekazał kody źródłowe oprogramowania;
   d) Wynik weryfikacji: pozytywny; dokumentacja projektowa przekazanego TOE
5. Dokumentacja cyklu życia i środowiska rozwojowego
   a) Dokumentacja zawiera: opis cyklu życia produktu; procedury bezpiecznej dostawy; procedury zarządzania konfiguracją; opis zabezpieczeń środowiska rozwojowego;
   b) Wersja dokumentacji dotyczy środowiska wytwarzania TOE i jest aktualna;
   c) Wynik weryfikacji: pozytywny;
6. Dokumentacja testów funkcjonalnych:

a) Producent przekazał plany testów zawierające przypadki testowe dla wymagań CR z normy IEC 62443-4-2 na poziome SL 1;
b) Plany testów zawierają wartości oczekiwanie i uzyskane rzeczywiste wyniki testów;
c) Producent przekazał właściwe TOE do testów wraz z platformą testową;
d) Wynik weryfikacji: pozytywny.

Biorąc pod uwagę wyniki wszystkich czynności weryfikacyjnych ewaluator potwierdza, że producent przekazał TOE i dokumentację zgodnie z wymaganiami. Wynik realizacji zadania wejściowego oceny jest pozytywny i ewaluator może przejść do realizacji działań oceniających.

6.2. Działania oceniające

W tym etapie walidowane są działania oceniające realizowane zgodnie z metodą oceny dla IACS. Zostanie wykonana walidacja kolejnych 3 kroków metody: 1) ocena dokumentacji; 2) testy funkcjonalne i niezależne; 3) analiza podatności.

Sprawdzeniu będą podlegać czynności ewaluatora opisane w jednostkach oceny WU_EXT, na podstawie których wydawany jest werdykt oceny dla danego SAR_EXT opisującego wymaganie przemysłowe.

6.2.1. Walidacja kroku 1 – ocena dokumentacji

W tym kroku zaprezentowano sposób oceny ocena klas wymagań ASE, AGD, ADV, ALC dla poziomu uzasadnionego zaufania EAL 4 i zweryfikowano, czy jednostki oceny są opracowane w sposób umożliwiający wydanie werdyktu dla danego wymagania.

Ocena klasy ASE

Do oceny zadania zabezpieczeń należy wybrać komponenty wymagań z klasy ASE na poziomie EAL 4 (zob. tabela 18) oraz komponenty dodatkowe (zob. tabela 24), które dotyczą wymagań przemysłowych.

Walidacja przebiega zgodnie z metodyką oceny CEM, w której werdykty wydaje się w zgodnie z opisem w rozdz. 4.5 i rys. 12.

Do oceny wymagań przemysłowych w klasie **ASE** użyto następujących jednostek WU_EXT.

Tabela 34. ASE - jednostki WU_EXT

Component	Element C [refinement]	WU_EXT
ASE_CCL.1	ASE_CCL.1.1C [*refinement*]	ASE_CCL.1-1
ASE_SPD.1	ASE_SPD.1.2C [refinement]	ASE_SPD.1-2

ASE_ECD.1	ASE_ECD.1.1C [refinement]	ASE_ECD.1-1 (here: original WU)
ASE_REQ.1	ASE_REQ.1.1C [refinement]	ASE_REQ.1-1 ASE_REQ.1-2

Zgodnie z tabelą 24, która zawiera pełny opis elementów C i WU_EXT dla klasy ASE, ewaluator wykonuje następujące działania oceniające:

- ASE_CCL.1-1
  - Sprawdza deklarację zgodności ST, czy zawiera odniesienia do standardów IEC 62443-4-1, IEC 62443-4-2;
- ASE_SPD.1-2
  - weryfikuje, czy definicja problemu bezpieczeństwa opisuje zasoby IACS w postaci zasobów krytycznych urządzenia i zasobów krytycznych środowiska łącznie z przypisanymi im atrybutami bezpieczeństwa Av, I, C, Au;
- ASE_ECD.1-1
  - sprawdza, czy zastosowano w ST komponenty rozszerzone SAR_EXT, SFR_EXT przeznaczone dla IACS;
- ASE_REQ.1-1
  - weryfikuje, czy deklaracja wymagań funkcjonalnych opisuje SFR_EXT zmodyfikowane na bazie IEC 62443-4-2 na danym poziomie SL;
- ASE_REQ.1-2
  - weryfikuje, czy deklaracja wymagań uzasadniających zaufanie opisuje SAR_EXT zmodyfikowane na bazie IEC 62443-4-1.

Zastosowanie powyższych jednostek oceny pozwala na ocenę zadania zabezpieczeń, czy zawiera informacje uzupełniające dotyczące IACS zgodnie z wynikami badań w rozdz. 4.2.

Ocena klasy AGD

Do oceny dokumentacji użytkownika należy zastosować następujące jednostki WU_EXT zgodnie z tabelą 38 (Załącznik 1).

Zgodnie z tabelą 36 (Załącznik 1), która zawiera pełny opis elementów C i WU_EXT dla klasy AGD, ewaluator wykonuje następujące działania oceniające:

- AGD_PRE.1-2
  - Weryfikuje dokumentację, czy zawiera kroki utwardzania produktu podczas instalacji i utrzymania poziomu utwardzenia podczas pracy w środowisku klienta;
  - Weryfikuje dokumentację, czy zawiera: zagrożenia rezydualne, środki ochrony przed tymi zagrożeniami, uzupełniające środki ochrony.

- Sprawdza, czy środowisko pracy dostarcza środki bezpieczeństwa wspomagające strategię ochrony w głąb.

Zastosowanie WU pozwala na ocenę dokumentacji użytkownika, czy zawiera wymaganą dla systemów IACS metodę utwardzania i środki ochrony w głąb zgodnie z Praktyką 8.

Ocena klasy ADV

Tabela 36 zawiera pełny opis WU_EXT dla klasy ADV. Tabela 38 zawiera mapowanie komponentu rozszerzonego ADV na wymagania przemysłowe, dla którego ewaluator wykonuje działania oceniające zdefiniowane w następujących jednostkach WU:

- ADV_ARC.1-5
  - Sprawdza opis architektury zabezpieczeń, czy zawiera analizę, w jaki sposób mechanizmy wymuszające SFR nie mogą zostać ominięte (ang. Bypassed) przy zastosowaniu mechanizmu kolejnych warstw ochrony;
  - Bada, czy dodatkowe mechanizmy bezpieczeństwa zapewniają redukcję powierzchni ataku dla następnej warstwy ochrony.

Zastosowanie WU pozwala na weryfikację dokumentacji projektowej, czy zawiera wymaganą dla systemów IACS strategię ochrony warstwowej zgodnie z Praktyką 3.

Ocena klasy ALC

Tabela 36 zawiera pełny opis WU_EXT dla klasy ALC. Tabela 37 zawiera mapowanie komponentu rozszerzonego ALC na wymagania przemysłowe. W przypadku klasy ALC zostały opracowane uszczegółowienia komponentów dla rodzin: ALC_FLR, ALC_TAT, ALC_CMS, ALC_LCD oraz powstał nowy komponent dodatkowy dla rodziny dodatkowej ALC_SUM.EXT (Security update management).

W ramach poszczególnych rodzin, ewaluator wykonuje następujące działania oceniające:

- ALC_FLR.1-1
  - Sprawdza dokumentację procedur usuwania błędów, czy zawiera procedurę okresowych przeglądów błędów bezpieczeństwa i proces zarządzania błędami;
  - Sprawdza, czy ostatni proces przeglądu był efektywny, kompletny i doprowadził do rozwiązania problemu;
  - Weryfikuje, czy przeglądy wykonywane są co najmniej rokrocznie.
- ALC_TAT.1-1
  - Sprawdza, czy w dokumentacji narzędzi rozwojowych, każde narzędzie jest dostatecznie opisane i zawiera co najmniej następujące informacje wymienione w elemencie ALC_TAT.1.1C [*refinement*]: a) unikanie możliwych do wykorzystania konstrukcji kodu; b) unikanie niedozwolonych funkcji, szablonów kodowania; c) użycie zautomatyzowanych narzędzi i ustawień; d) praktyki bezpiecznego kodowania; e) walidacja wejść; f) obsługa błędów.

- ALC_CMS.1-2
    - Sprawdza, czy lista konfiguracyjna unikalnie identyfikuje każdy element konfiguracji pochodzący od zewnętrznych dostawców;
    - Weryfikuje, czy komponenty od zewnętrznych dostawców deklarują zgodność ze standardami IEC 62443-4-1, IEC 62443-4-2;
- ALC_LCD.1-1 (1)
    - Weryfikuje dokumentację cyklu życia w celu określenia wystarczających kompetencji technicznych personelu zaangażowanego do wykonywania zadań w procesach związanych z bezpieczeństwem; kompetencje mogą być nabywane poprzez szkolenia, seminaria, konferencje naukowe, itp.
- ALC_LCD.1-1 (2)
    - Sprawdza, czy dokumentacja cyklu życia obejmuje standardy IEC 62443-4-1 i IEC 62443-4-2, zgodnie z deklaracją zgodności TOE;
- ALC_LCD.1-1 (3)
    - Weryfikuje dokumentację bezpiecznego cyklu życia (SDL), aby określić, czy obejmuje fazy sprawdzania i ulepszania cyklu SDL w celu poprawy jakości produktu;
- ALC_LCD.1-1 (4)
    - Sprawdza dokumentację cyklu życia w celu określenia, czy opisuje kontekst bezpieczeństwa urządzenia IACS, aby zapewnić minimalne wymagania i założenia na środowisko operacyjne, które umożliwiają osiągnięcie zadeklarowanego poziomu bezpieczeństwa SL, na który komponent IACS został zaprojektowany;
    - Weryfikuje, czy dokumentacja cyklu życia opisuje zgodnie z ALC_LCD.1.1C (4): a) lokalizację urządzenia w sieci; b) fizyczne i informatyczne zabezpieczenia środowiska operacyjnego; c) separację do innych sieci; e) potencjalne skutki zagrożeń na środowisko (np. utrata życia, zatrzymanie produkcji, itp.);
- ALC_LCD.1-1 (5)
    - Sprawdza dokumentację cyklu życia w celu określenia, czy opisuje model zagrożeń dla obecnego zakresu rozwoju i projektowania urządzenia;
    - Weryfikuje, czy model zagrożeń obejmuje zgodnie z ALC_LCD.1.1C(5): poprawny przepływ informacji, strefy zaufania, procesy, magazyny danych, zewnętrzne obiekty komunikacji, wewnętrzne i zewnętrzne protokoły komunikacyjne, dostępne na zewnątrz fizyczne porty, połączenia na płytkach drukowanych, np. JTAG, potencjalne wektory ataków włączając ataki na hardware, potencjalne zagrożenia zdefiniowane w CVSS, środki i sugestie do

zapobiegania zagrożeniom, zidentyfikowane problemy bezpieczeństwa i zależności od zewnętrznych elementów takich, jak sterowniki lub aplikacje od zewnętrznych producentów;

- Sprawdza, czy model zagrożeń jest weryfikowany nie rzadziej niż co rok przez zespół projektowy dla wyprodukowanych produktów i aktualizowany w przypadku pojawienia się nowych zagrożeń;

- ALC_LCD.1-1 (6)
  - Sprawdza dokumentację cyklu życia w celu określenia, czy pokrywa wszystkie wymagania bezpieczeństwa związane z cyklem życia produktu zawierają zgodnie z ALC_LCD.1.1C (6), m.in.: a) uprawnienia do instalacji, uruchomienia i utrzymania produktu; b) opcje bezpieczeństwa włączając usuwanie domyślnych haseł używanych do instalacji, konfiguracji, uruchamiania; c) opcji bezpieczeństwa związanych z wycofaniem produktu z użycia;
  - Weryfikuje, czy wymagania bezpieczeństwa zawierają informacje: a) o zakresie i granicach urządzenia; b) wymaganego osiągalnego poziomu bezpieczeństwa produktu SL-C (Capability Security Level);
- ALC_LCD.1-1 (7)
  - Weryfikuje dokumentację cyklu życia w celu określenia, czy zawiera etap przeglądu projektu bezpieczeństwa, na który składają się następujące działania określone w ALC_LCD.1.1C (7): a) identyfikacja wymagań bezpieczeństwa, które nie zostały uwzględnione w projekcie; b) identyfikacja zagrożeń i ich możliwości do wykorzystania interfejsów, stref bezpieczeństwa i zasobów produktu; c) identyfikacja praktyk bezpiecznego projektu, które nie były realizowane, np. pominięcie zasady nadawania najmniejszych uprawnień;
- ALC_LCD.1-1(8)
  - Sprawdza dokumentację cyklu życia w celu określenia, czy zawiera etap projektowania zabezpieczeń i jakie praktyki zostały zastosowane w fazie projektowania w celu zapewnienia bezpieczeństwa produktu;
  - weryfikuje, czy praktyki bezpiecznego projektowania zawierają zgodnie z ALC_LCD.1.1C (8): a) najmniejsze uprawnienia; b) gwarantowane bezpieczne komponenty; c) mechanizmy efektywnościowe (prosty projekt); d) bezpieczne wzorce projektowe; e) redukcję powierzchni ataku; f) strefy zaufania w projekcie; g) usuwanie portów diagnostycznych i dostępnych ścieżek dostępnych w produkcji lub z dokumentacji w celu ochrony przed nieautoryzowanym dostępem;
- ALC_LCD.1.1C (9)

- Weryfikuje dokumentację cyklu życia w celu określenia, czy zawiera etap przeglądu implementacji zabezpieczeń, na który składają się następujące działania określone w ALC_LCD.1.1C (9): a) identyfikacja wymagań bezpieczeństwa, które nie zostały prawidłowo zastosowane w trakcie implementacji; b) identyfikacja standardów bezpiecznego kodowania, które nie zostały poprawnie użyte podczas implementacji; c) użycie statycznej analizy kodu źródłowego SCA (Static code analysis) implementacji; d) przegląd implementacji i mapowanie do mechanizmów wspierających bezpieczne projektowanie i e) testowanie możliwości zagrożeń do wykorzystania interfejsów implementacji, stref zaufania i zasobów;

- ALC_LCD.1.1C (10)
  - Weryfikuje dokumentację cyklu życia w celu określenia, czy zawiera etap bezpiecznego wycofania produktu z użycia, na który składają się następujące działania określone w ALC_LCD.1.1C (10): a) wycofanie produktu ze środowiska operacyjnego; b) wytyczne do usunięcia powiazań i danych konfiguracyjnych zapisanych w środowisku operacyjnym; c) bezpieczne usunięcie danych z produktu; d) bezpieczna utylizacja produktu, w przypadku braku możliwości bezpiecznego usunięcia danych z produktu.
- ALC_SUM_EXT.1-1 (kwalifikowanie aktualizacji bezpieczeństwa)
  - Sprawdza dokumentację kwalifikowania aktualizacji bezpieczeństwa, czy zawiera potwierdzenie, że aktualizacje nie są sprzeczne z ograniczeniami operacyjnymi, bezpieczeństwa fizycznego lub kwestii prawnych oraz czy zawiera informacje określone w ALC_SUM_EXT.1-1C: a) aktualizacje dotyczące podatności; b) rezultaty weryfikacji potwierdzające, że bieżące aktualizacje nie powodują regresji poprzednich aktualizacji (wycofania lub uszkodzenia poprzednich aktualizacji) włącznie z poprawkami wprowadzonymi przez producenta lub dostawców komponentów);
  - Weryfikuje dokumentację, czy zawiera potwierdzenie, że wprowadzone do produktu poprawki nie powodują zakłócenia pracy urządzenia;
- ALC_SUM_EXT.2-1 (dokumentacja aktualizacji)
  - Weryfikuje, czy producent opracowuje dokumentację dotyczącą aktualizacji bezpieczeństwa dla użytkowników produktu;
  - Sprawdza, czy dokumentacja zawiera co najmniej następujące informacje określone w ALC_SUM_EXT.2.1C: a) wersja produktu; b) instrukcja instalacji zatwierdzonych poprawek; c) opis skutków na produkt, po zastosowaniu poprawki; d) instrukcja weryfikacji poprawki po instalacji; e) ryzyko niezastosowania poprawki lub użycia poprawki niezatwierdzonej;

- ALC_SUM_EXT.3-1 (dokumentacja aktualizacji komponentu zależnego lub systemu operacyjnego)
    - Weryfikuje, czy producent opracowuje dokumentację dotyczącą aktualizacji bezpieczeństwa komponentów zależnych lub systemów operacyjnych dla użytkowników produktu;
    - Sprawdza, czy dokumentacja zawiera co najmniej następujące informacje określone w ALC_SUM_EXT.3.1C: a) deklaracja, że produkt jest kompatybilny z aktualizacją komponentu zależnego lub systemu operacyjnego; b) środki zapobiegawcze w przypadku nieinstalowania aktualizacji niezatwierdzonej przez producenta;
- ALC_SUM_EXT.4-1 (dostarczanie aktualizacji bezpieczeństwa)
    - Weryfikuje, czy dokumentacja zawiera opis sposobów dostarczania aktualizacji i poprawek bezpieczeństwa do użytkowników oraz sposobów weryfikacji ich autentyczności;
- ALC_SUM_EXT.5-1 (terminowe dostarczanie poprawek bezpieczeństwa)
    - Weryfikuje dokumentację polityki terminowego dostarczania aktualizacji, czy uwzględnia następujące czynniki określone w ALC_SUM_EXT.5.1C: a) potencjalny wpływ podatności; b) publiczna wiedza o podatnościach; c) możliwości wykorzystania podatności (exploits); d) liczba wdrożonych produktów, których dotyczy podatność; e) dostępność innych skutecznych środków zmniejszających wpływ podatności w zastępstwie poprawki;

Zastosowanie powyższych WU pozwala na ocenę dokumentacji produktu, czy zawiera wymagania dla systemów IACS wyprowadzonych z następujących Praktyk (zob. Tabela 38):

- ASE – brak odpowiedniej praktyki, ponieważ stosuje się zadanie zabezpieczeń zgodnie z Common Criteria uzupełnione o informacje dotyczące IACS;
- AGD – Praktyka 8;
- ADV – Praktyka 3;
- ALC – Praktyki 1, 2, 3, 4, 6, 7, 8

Walidacja powyższych jednostek WU stosowanych w kroku 1 metody – ocena dokumentacji, potwierdziła możliwość ich praktycznego użycia do wydawania werdyktów z oceny komponentów SAR_EXT dostosowanych do wymagań przemysłowych.

W kolejnym podrozdziale zaprezentowano walidację jednostek WU wykorzystywanych w kroku 2 metody – testy funkcjonalne i niezależne.

6.2.2. Walidacja kroku 2 – testy funkcjonalne i niezależne

W tym kroku, zgodnie z rys. 20 oraz tabelą 30, zaprezentowano sposób oceny klasy ATE (Testy) w ramach rodzin ATE_FUN (Testy funkcjonalne), ATE_IND (Testy niezależne) oraz

rodziny rozszerzonej ATE_SVV_EXT (Testowanie w celu weryfikacji i walidacji bezpieczeństwa).

Ocena rodziny ATE_FUN

Tabela 36 zawiera pełny opis WU_EXT dla klasy ATE. Tabela 38 zawiera mapowanie komponentu rozszerzonego ATE_FUN.1 na wymagania przemysłowe, dla którego ewaluator wykonuje działania oceniające zdefiniowane w następujących jednostkach WU:

- ATE_FUN.1-1
    - Sprawdza, czy dokumentacja testów zawiera dowody, że testy zostały wykonane przez testerów niezależnych od konstruktorów testowanego produktu;
- ATE_FUN.1-2
    - Weryfikuje, czy plan testów opisuje scenariusze dla każdego rodzaju testów wymaganych przez FR oraz określone w ATE_FUN.1.2C: a) testy funkcjonalne wymagań bezpieczeństwa FR dla IACS; b) skalowalne testy wydajnościowe; c) testy brzegowe, testy obciążeniowe, testy z wartościami wejść poza zakresem lub wejściami zakłóconymi.

Ocena rodziny ATE_IND

Ewaluator wykonuje działania oceniające zdefiniowane w następujących jednostkach WU:

- ATE_IND.1-3
    - Ewaluator musi opracować zbiór testów dla funkcji zabezpieczających TSF implementujących wymagania SFR_EXT wyprowadzone na bazie wymagań FR dla komponentów IACS;
    - Ewaluator w dokumentacji testów musi opisać oczekiwane wyniki testów, otrzymane rzeczywiste wyniki testów oraz kryteria akceptacji wyników.

Jednostka oceny ATE_IND.1-3 została zastosowana i zweryfikowana w praktyce podczas pilotażowej oceny programowalnego sterownika zabezpieczenia odległościowego. Zgodnie ze zleceniem producenta, laboratorium wykonało badanie zgodności urządzenia z technicznymi wymaganiami bezpieczeństwa normy IEC 62443-4-2 na poziomie SL 1.

W trakcie pilotażu wykonano testy dla 50 wymagań CR na poziomie SL 1, a wyniki udokumentowano w sprawozdaniu z badań (zob. załącznik 2)[5].

Wynikiem działań zespołu ewaluatorów laboratorium ITSEF są plany testów z warunkami akceptacji i wynikami testów urządzenia dla każdego wymagania CR. Oznacza to, że ewaluator może wykonać test każdej funkcji TSF implementującej wymaganie SFR_EXT, które

[5] Załącznik 2 zawiera wersję skróconą sprawozdania ograniczoną do prezentacji wybranych wymagań CR, ze względu na objętość oryginalnego dokumentu, który zawiera 105 stron opisu testów i ich wyników dla wszystkich 50 wymagań CR.

producent opracował na bazie wymagań CR, SL 1 z normy IEC 62443-4-2 i włączył do zadania zabezpieczeń urządzenia IACS.

Wynikiem dodatkowym badań są tabele mapujące: 15 i 39, które mogą stanowić pomoc dla producentów podczas opracowywania wymagań SFR_EXT, zgodnych z technicznymi wymaganiami bezpieczeństwa normy IEC 62443-4-2. Przykładowo dla użytego w produkcie wymagania CR1.3 odnajdujemy w tabeli 39 odpowiadające mu wymaganie FMT_SMF.1.1 i używamy zaproponowany tekst uszczegółowienia.

Ponadto, tabela 39 w kolumnie „CC Evaluation activities (EAs)" zawiera propozycje testów oraz odnośniki do planów testów wymagań CR opisanych w sprawozdaniu z oceny pilotażowej. Należy zaznaczyć, że działania EA oraz testy są uzależnione od konkretnej implementacji produktu i kontekstu jego użycia, dlatego też w przypadku oceny innego urządzenia będą opracowywane nowe plany testów.

Ocena rodziny ATE_SVV_EXT

Ewaluator wykonuje działania oceniające zdefiniowane w następujących jednostkach WU:

- ATE_SVV_EXT.1-1 (testowanie łagodzenia zagrożeń)
    - Sprawdza, czy dokumentacja testów zawiera plany testów, wartości oczekiwane oraz rzeczywiste wyniki testowania możliwości zmniejszania zagrożeń;
    - Weryfikuje, czy dokumentacja testów zawiera przykłady zidentyfikowanych prób obchodzenia łagodzenia zagrożeń za pomocą podszywania się, manipulacji, naruszenia niezaprzeczalności, ujawnienia informacji, odmowa usługi (DoS), zwiększanie uprawnień;
    - Sprawdza, czy dokumentacja zawiera informację na temat zastosowania strategii ochrony warstwowej jako środek łagodzenia zagrożeń, a następnie sprawdza, czy strategie ochrony w głąb i łagodzenia zagrożeń są skuteczne.
- ATE_SVV_EXT.2-1 (testowanie podatności)
    - Sprawdza, czy dokumentacja testowania podatności zawiera opis potencjalnych podatności i wyniki analiz znanych podatności;
    - Weryfikuje, czy dokumentacja testowania podatności zawiera następujące analizy i testy: a) testowanie wejść; b) analiza powierzchni ataku; c) skanowanie znanych podatności typu czarna skrzynka (black box); d) analiza struktury oprogramowania; e) testowanie dynamicznego zarządzania zasobami podczas działania;
    - Sprawdza powyższe testy z punktów a) do e), czy zapewniają minimum niezbędnej informacji niezbędnej do dalszej analizy w procesie zarządzania usterkami bezpieczeństwa.
- ATE_SVV_EXT.3-1 (testy penetracyjne)

- Sprawdza, czy dokumentacja testów penetracyjnych zawiera wyniki testów potencjalnych podatności i znanych podatności;
- Weryfikuje, czy dokumentacja testów penetracyjnych zawiera wyniki testów podatności wykrytych podczas testowania podatności;
- Sprawdza wyniki testów penetracyjnych czy analizowana podatność została wykorzystana w drodze testu penetracyjnego.

Zastosowanie powyższych WU pozwala na ocenę testów funkcjonalnych i niezależnych zgodnych z wymaganiami Praktyki 5 (zob. Tabela 38).

Walidacja powyższych jednostek WU potwierdziła możliwość ich praktycznego użycia do wydawania werdyktów dla klasy ATE w kroku 2 metody.

W kolejnym podrozdziale zaprezentowano walidację kroku 3 metody – analiza podatności.

6.2.3. Walidacja kroku 3 – analiza podatności

W opracowanej metodzie oceny analiza podatności przebiega standardowo zgodnie z metodyką oceny CEM i jej aneksem B, dlatego też nie podlega walidacji.

Analiza podatności została opisana w rozdz. 5.3.3 opisującym krok 3 metody oceny. Należy zwrócić uwagę na możliwość wykorzystania tabeli 33 integrującej poziomy EAL oraz SL z wartościami potencjału ataku, co także zostało przedstawione w rozdz. 5.3.3.

Tabela 33 ułatwia ocenę spełnienia wymagań klasy AVA na podstawie weryfikacji, czy TOE na danym poziomie EAL lub SL jest odporne na ataki o wartości potencjału przypisanej do tego poziomu EAL lub SL.

Po wykonaniu wszystkich działań oceniających przewidzianych w metodzie oceny, ewaluator przechodzi do realizacji ostatniego etapu w procesie oceny, czyli sporządzenia raportu technicznego oceny ETR lub obserwacji OR w przypadku werdyktów negatywnych lub innych kwestii, które muszą być rozwiązane albo przez klienta, albo przez jednostkę certyfikującą.

6.3. Wyjściowe zadanie oceny

W tym etapie procesu oceny ewaluator opracowuje dwa rodzaje raportów: OR i ETR.

Struktura i zawartość raportów została opisana w rozdz. 5.2 opisującym model procesu oceny. Raporty tworzone są zgodnie z zaleceniami metodyki CEM i nie podlegają walidacji.

Podsumowując, walidacja metody dostarczyła dowodów na to, że działania ewaluatora, wyrażone za pomocą jednostek oceny CEM, dają się zastosować do oceny wymagań bezpieczeństwa urządzeń IACS zgodnie ze standardem Common Criteria.

Zgodnie z tabelą 24 dla ASE oraz tabelami 37, 38 dla klas: AGD, ADV, ALC oraz ATE wszystkie wymagania Praktyk standardu IEC 62443-4-1 zostały pokryte,

a ocena pilotażowa pozwoliła wykonać testy dla wszystkich wymagań CR dla standardu IEC 62443-4-2.

Pozytywny wynik walidacji oznacza, że cel szczegółowy C4 został osiągnięty.

W kolejnym rozdziale przedstawiono wnioski końcowe rozprawy doktorskiej oraz wskazano dalsze prace.

7. Wnioski i uwagi końcowe

W wyniku zrealizowanych prac badawczych osiągnięto **cel główny** pracy doktorskiej w postaci metody oceny bezpieczeństwa dla przemysłowych systemów automatyki i sterowania.

Metoda umożliwia wykonywanie ocen bezpieczeństwa urządzeń IACS zgodnie z poziomem uzasadnionego zaufania do oceny zabezpieczeń od EAL 1 do EAL 4 (Common Criteria) oraz zgodnie z przemysłowym poziomem bezpieczeństwa SL 1 (IEC 62443-4-2).

Dzięki temu, będzie można uzyskać certyfikat bezpieczeństwa poświadczający, że do wykonanej oceny można mieć uzasadnione zaufanie określone poziomem EAL. Innymi słowy będzie można mieć zaufanie, że funkcje bezpieczeństwa, spełniające wymagania poziomu przemysłowego SL, zadziałają zgodnie z deklaracją producenta.

Opracowana metoda stanowi rozwiązanie problemu badawczego, polegającego na braku metody oceny cyberbezpieczeństwa dla urządzeń IACS. Rozwiązanie tego problemu było możliwe dzięki realizacji celów szczegółowych pracy.

Pierwszy cel szczegółowy pozwolił na identyfikację potrzeb i wymagań bezpieczeństwa charakterystycznych dla rozwiązań przemysłowych. W toku badań zidentyfikowano inicjatywy i projekty badawcze mające na celu utworzenie europejskich ram certyfikacji dotyczących cyberbezpieczeństwa, w tym także dla bezpieczeństwa przemysłowych systemów sterowania i ich komponentów. Inicjatywy te, odpowiadając na potrzebę oceny zabezpieczeń, często wskazują na możliwość zastosowania do tego celu standardu Common Critieria – uznanej metodyki oceny zabezpieczeń teleinformatycznych. Dlatego też **drugim celem** szczegółowym pracy była ocena możliwości zastosowania tego standardu do oceny bezpieczeństwa komponentów przemysłowych.

Rezultaty badań potwierdziły, że standard Common Criteria wraz z metodyką oceny CEM mają duży potencjał adaptacji w zakresie definiowania i modyfikacji wymagań oraz działań oceniających, tzw. jednostek oceny wykonywanych przez ewaluatora. W pracy pokazano sposób adaptacji tych elementów, jak również opracowano gotowe zestawy odpowiednio zmodyfikowanych komponentów do użycia w kontekście oceny urządzeń przemysłowych.

W procesie oceny Common Criteria, najważniejszą rolę odgrywa metodyka oceny CEM. Dlatego poddano krytycznej ocenie i analizie możliwe warianty jej doskonalenia w kierunku możliwości wydawania werdyktów z oceny bezpieczeństwa dla komponentów IACS.

W wyniku analizy, wybrano wariant z dostosowaniem jednostek oceny CEM do wymagań IACS. W ten sposób otrzymano trzy udoskonalone elementy metodyki CC – wymagania na uzasadnione zaufanie do zabezpieczeń, wymagania na funkcjonalność zabezpieczeń oraz jednostki oceny tych wymagań. Następnie, elementy te zintegrowano w jednej metodzie oceny bezpieczeństwa, tym samym realizując **trzeci cel** szczegółowy pracy.

W ostatnim etapie badań wykonano walidację metody z wykorzystaniem wyników oceny pilotażowej programowalnego sterownika zabezpieczenia odległościowego. W trakcie walidacji zweryfikowano, czy za pomocą zdefiniowanych w metodzie działań oceniających da się ocenić wszystkie aspekty bezpieczeństwa przemysłowego.

Wyniki walidacji potwierdziły, że wybrany wariant doskonalenia metodyki CEM sprawdza się w praktyce i pozwala ocenić wszystkie wymagania bezpieczeństwa zdefiniowane w normach przemysłowych IEC 62443-4-1 i IEC 62443-4-2. W ten sposób został osiągnięty **czwarty cel** szczegółowy pracy.

Należy tutaj przypomnieć o **celu wdrożeniowym**, wynikającym z wdrożeniowego charakteru pracy doktorskiej,

Metoda oceny została częściowo wdrożona do działalności laboratorium oceny bezpieczeństwa ITSEF w Łukasiewicz – EMAG w zakresie oceny testów funkcjonalnych i niezależnych, które wykonano w pilotażowej ocenie. Pełne wdrożenie nastąpi po pilotażowej ocenie innego produktu, dla którego zostanie utworzone zadanie zabezpieczeń oraz kompletna dokumentacja zgodna z Common Criteria.

Dzięki realizacji celów szczegółowych osiągnięto cel główny, a walidacja metody pozwoliła potwierdzić w praktyce tezę pracy doktorskiej:

„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.”

Realizacja poszczególnych celów szczegółowych odbyła się zgodnie z kolejnymi etapami dochodzenia do koncepcji rozwiązania problemu badawczego zgodnie z metodyką „Concept development and experimentation” [31].

W pierwszym etapie, inicjującym badania, na podstawie analizy obecnego stanu wiedzy w kontekście certyfikacji cyberbezpieczeństwa, zidentyfikowano problem badawczy, który wynika z braku ustandaryzowanej metodyki oceny bezpieczeństwa dla urządzeń systemów IACS. Problem ten rodzi skutki w postaci słabo zabezpieczonych urządzeń, podatnych na coraz groźniejsze cyberataki. W celu zaradzenia temu problemowi, ale także problemowi rozproszenia rynku certyfikacji cyberbezpieczeństwa IT, instytucje europejskie podjęły inicjatywy utworzenia europejskich ram certyfikacji i opracowały szereg aktów prawnych, takich jak Akt o cyberbezpieczeństwie CSA [36] lub dyrektywa NIS2 [35]. Powstały także rekomendacje dotyczące utworzenia programu certyfikacji cyberbezpieczeństwa dla systemów IACS [42]. Analiza tych programów i inicjatyw prowadzi do konkluzji, że obecnie stosowany i sprawdzony od ponad 20 lat standard Common Criteria może być najlepszą podstawą do budowania programów certyfikacji dla różnych urządzeń IT, w tym także dla IACS.

W związku z tym należało uzyskać odpowiedź czy standard CC, do tej pory stosowany dla typowych rozwiązań informatycznych, rzeczywiście może stać się bazą dla metod oceny bezpieczeństwa komponentów przemysłowych. Badania w tej części pracy, skupiły się na wstępnym potwierdzeniu, że koncepcję rozwiązania można oprzeć na adaptacji standardu CC wspomaganego przez metodykę oceny CEM. W wyniku analizy dokumentów normatywnych standardu oraz na bazie wieloletniego doświadczenia doktoranta, wysnuto wniosek, mówiący, że standard da się dostosować do nowego zakresu wymagań specyficznych dla urządzeń przemysłowych. Następnie należało zidentyfikować źródła tych wymagań.

W celu identyfikacji specyficznych wymagań bezpieczeństwa dla IACS rozpoczęto od analizy najczęstszych zagrożeń i podatności, które w rezultacie są źródłem konkretnych potrzeb bezpieczeństwa, a dalej wymagań. Wymagania dotyczą ochrony części składowych systemów IACS, ich zasobów krytycznych oraz sposobów niwelowania obszarów występowania podatności i są zapisywanie w wielu różnych dedykowanych programach certyfikacji [58], wytycznych [19], metodach firmowych [87] czy wreszcie w standardach [11].

Problemem jaki z tego wynika jest rozproszenie wiedzy, stosowanie różnych podejść, utrudnione możliwości porównywania wyników. Znaleziono jedno źródło wymagań bezpieczeństwa, które mogło rozwiązać te problemy. Otóż jest to rodzina norm IEC 62443 o ugruntowanej międzynarodowej renomie, przedstawiająca wymagania w sformalizowany i uporządkowany sposób. Do dalszych badań wytypowano dwie części tej rodziny norm, otóż IEC 62443-4-1 [11] – zawierającą wymagania dla procesu wytwarzania bezpiecznego produktu oraz IEC 62443-4-2 [12] – określającą wymagania techniczne bezpieczeństwa. Znaleziono zatem źródło, jednak należało zweryfikować jakość tego źródła pod względem przydatności do jego wykorzystania w procesie adaptacji metodyki Common Criteria.

W celu oceny przydatności wytypowanych norm wykonano szereg porównań obydwu standardów względem różnych kryteriów. Tymi kryteriami były m.in. cechy charakteryzujące możliwości standardu CC dotyczące dokumentowania charakterystyki urządzenia, określania wymagań na funkcjonalność zabezpieczeń, określania wymagań na uzasadnione zaufanie do zabezpieczeń, prowadzenia testów niezależnych i analizy podatności. Z prowadzonych badań wynikało, że obydwa standardy prezentują podobną logikę inżynierii bezpieczeństwa. Porównanie norm pokazało, że w każdym ocenianym kryterium obydwie normy mają swoje odpowiedniki oraz elementy wspólne. W rezultacie przyjęto, że norma CC p.3 będzie doskonalona na podstawie wymagań normy IEC 62443-4-1, natomiast norma CC p.2 będzie doskonalona na podstawie wymagań normy IEC 62443-4-2.

Rezultaty porównania standardów wypadły pomyślnie, pozostała jeszcze kwestia metodyki oceny CEM i zakresu jej adaptacji. Otóż metodyka jest zasilana wynikami adaptacji norm CC wymienionych wyżej, ponieważ na ich podstawie, a w szczególności wymagań na

uzasadnienie zaufania powstają stowarzyszone z nimi jednostki oceny. Zatem otrzymano bazę wiedzy do adaptacji wyjściowej metody oceny opartej na CC i CEM.

Jednakże, z racji tego, że w ostatnim czasie wydano najnowszą czwartą część standardu CC p.4, która podaje sposób i strukturę tworzenia metod oceny w oparciu o CEM, to postanowiono wykorzystać dodatkowo ten fakt i zbadać, czy nowa część może przynieść jakieś korzyści na teraz lub w przyszłości.

Zatem dodatkowo wykonano porównanie obecnej metodyki CEM oraz CC p.4. W wyniku otrzymano bardzo ciekawe rezultaty. Odkryto po pierwsze, że zaadaptowane jednostki oceny CEM na potrzeby tej pracy doktorskiej, mogą stanowić źródło dla zmodyfikowanych jednostek oceny, które grupowane zgodnie z zasadami CC p.4, mogą stać się w przyszłości nowymi metodami oceny dla specyficznych typów urządzeń lub technologii.

A po drugie, odkryto, że działania oceniające utworzone w tej pracy doktorskiej, podczas modyfikacji wymagań funkcjonalnych z CC p.2 mogą być wykorzystane w przyszłości, zgodnie z zasadami CC p.4, jako działania oceniające włączane dla profili zabezpieczeń cPP np. sterowników PLC. W ten sposób konstruktorzy posługując się cPP zyskują źródło wymagań funkcjonalnych do projektowania urządzeń, natomiast ewaluatorzy otrzymują przepis, jak te wymagania sprawdzać.

Rezultat tych ostatnich badań jest znaczący z punktu widzenia kontynuowania dalszych prac nad opracowywaniem nowych sposobów podejścia do oceny z wykorzystaniem wyników niniejszej pracy doktorskiej.

Podsumowując, otrzymano źródła wzorcowe do adaptacji oraz wiedzę, co będzie rezultatem wyjściowym modyfikacji. Pojawił się tutaj kolejny problem, jak to wykonać w sposób efektywny i dający możliwie użyteczne w praktyce wyniki.

Była to najtrudniejsza, najdłuższa, żmudna i najbardziej wymagająca pod względem wiedzy merytorycznej o obydwu standardach, część badań pracy doktorskiej. Warto jednak było podjąć ten wysiłek, ponieważ w rezultacie opracowano kilka konkretnych tabel mapowania zawierających zbiory gotowych do użycia komponentów standardu CC i metodyki CEM, dostosowanych do wymagań przemysłowych.

Ale zanim te tabele można było wypełnić treścią, należało wykonać skrupulatne analizy budowy i struktury prezentacji wymagań w obydwu standardach: porównać wymagania, wykonać mapowania wstępne, dokładnie przeanalizować treść wymagań, aby wydobyć z nich cechy charakterystyczne, które wyjściowo zasiliły zmodyfikowane wymagania standardu CC i jednostki oceny w metodyce CEM.

W ten sposób otrzymano tabele mapujące zawierające uszczegółowione/rozszerzone wymagania, które w skrócie oznaczane są przyrostkiem EXT:

- tabele 24, 36, 37, 38 – zawierają wymagania uzasadniające zaufanie do zabezpieczeń SAR_EXT i jednostki oceny WU_EXT powstałe na bazie IEC 62443-4-1;

- tabele 15, 39 – zawierają odpowiednio mapowanie oraz listę zaadaptowanych wymagań SFR_EXT i działań oceniających EA utworzonych na bazie IEC 62443-4-2.

Podsumowując, ta część badań, potwierdziła możliwość adaptacji metodyki Common Criteria i CEM, poprzez wykonanie tej adaptacji w praktyce i która zaowocowała tabelami zawierającymi elementy gotowe do implementacji w metodzie oceny.

Przed rozpoczęciem prac nad metodą oceny, wykonano dodatkowe badanie mające ostatecznie potwierdzić słuszność wstępnej koncepcji rozwiązania zaproponowanego zgodnie z podejściem metodyki CD&E [31]. Ocena najlepszego wariantu dla opracowania metody oceny została poddana krytycznej ocenie i analizie, w wyniku której uzyskano potwierdzenie, że wstępna koncepcja, była słuszna z następujących powodów:

- metodyka CEM jest dedykowana dla standardu CC, który umożliwia modyfikację swoich elementów do specyficznych zastosowań;
- metodyka CEM jest znormalizowana i nie wymaga dodatkowej walidacji;
- metodyka CEM jest źródłem jednostek oceny, które można potencjalnie wykorzystać w przyszłości do tworzenia metod oceny zgodnie z CC p.4 i włączanych do cPP.

Uzyskując potwierdzenie wcześniej obranego kierunku doskonalenia standardu CC, przystąpiono do części pracy, w której zintegrowano wszystkie uzyskanie wcześniej wyniki w jednej metodzie oceny. Metoda została umiejscowiona w ogólnym procesie oceny zgodnym z CEM, który dzieli ocenę na zadanie wejściowe – przygotowanie do oceny, działania oceniające – etap stosowania metody oceny oraz zadanie wyjściowe – dokumentowanie wyników oceny.

Po drodze występuje jeszcze zadanie wykazania kompetencji technicznych przez zespół ewaluatorów. Demonstracja kompetencji jest niezbędna dla jednostki certyfikującej, która nadzoruje cały proces, w celu potwierdzenia utrzymania należytej jakości ocen zgodnie z wymaganiami standardu.

W wyniku integracji wszystkich elementów zaadaptowanej metodyki Common Criteria i CEM, otrzymano metodę oceny, która realizuje działania oceniające w kolejnych trzech krokach (rys. 15):

1. Ocena dokumentacji – ocenie podlegają: dokument zadania zabezpieczeń; dokumentacja użytkownika; dokumentacja instalacji i uruchamiania produktu; dokumentacja projektowa urządzenia; dokumentacja środowiska rozwojowego i cyklu życia produktu; dokumentacja bezpieczeństwa środowiska rozwojowego.
2. Testowanie funkcjonalne i niezależne – ocenie podlegają zakres testów, głębokość testowania, testy funkcjonalne klienta i niezależne wykonywane przez laboratorium.
3. Analiza podatności – ocenie podlega analiza odporności urządzenia na ataki o zadanym potencjale wynikającym z zadeklarowanego dla urządzenia poziomu uzasadnionego zaufania EAL oraz poziomu bezpieczeństwa SL.

Metoda oceny obejmuje wszystkie wymagane aspekty bezpieczeństwa zgodnie z Common Criteria oraz pokrywa wszystkie aspekty bezpieczeństwa wykazane w standardzie przemysłowym. Metoda umożliwia weryfikację spełnienia informatycznych i przemysłowych wymagań bezpieczeństwa na zadanym poziomie EAL dzięki zastosowaniu uszczegółowionych i rozszerzonych jednostek oceny, które definiują konkretne działania ewaluatora zgodnie z metodyką CEM. Uzyskane wyniki oceny dokumentowane są w raporcie technicznym oceny ETR, którego struktura i zawartość określone są w CEM. Metoda oceny oraz jej elementy składowe, aby mogły być użyte w rzeczywistych warunkach, muszą jeszcze przejść proces walidacji.

Walidacja metody miała na celu potwierdzenie, że jest odpowiednia do zastosowania w ocenie bezpieczeństwa komponentów przemysłowych.

Walidacja metody została zrealizowana poprzez weryfikację wszystkich uszczegółowionych/rozszerzonych jednostek oceny oraz wykonanie oceny pilotażowej programowalnego sterownika zabezpieczenia odległościowego w warunkach laboratorium ITSEF. Etap metody odpowiedzialny za analizę podatności nie podlegał walidacji, ponieważ jest on realizowany zgodnie z aneksem B metodyki CEM, opisującym sposób realizacji tego etapu.

Ocena pilotażowa była źródłem wyników dla walidacji etapu związanego z testami niezależnymi funkcji bezpieczeństwa zastosowanych w urządzeniu. Wykonane w laboratorium testy sterownika objęły wszystkie techniczne wymagania bezpieczeństwa CR (Component requirement) na poziomie SL 1 z normy IEC 62443-4-2. Wyniki tych testów wykorzystano do wydania werdyktu dla jednostki oceny testów niezależnych funkcji bezpieczeństwa wyrażonych za pomocą rozszerzonych wymagań funkcjonalnych SFR_EXT, a które zostały wyprowadzone z wymagań CR (tych samych, które zostały przetestowane w pilotażu).

Walidacja potwierdziła, że metoda oceny uwzględnia wszystkie aspekty bezpieczeństwa przemysłowego wskazanego w normach źródłowych oraz pozwala na wydanie werdyktów z oceny dla wszystkich uszczegółowionych/rozszerzonych wymagań Common Criteria.

Tym samym cel główny pracy doktorskiej został osiągnięty, a teza pracy potwierdzona.

Uzyskane w pracy doktorskiej wyniki należy rozpatrywać w kontekście certyfikacji cyberbezpieczeństwa produktów IT i IACS oraz obecnie prowadzonych prac zmierzających do ustanowienia ram certyfikacji dla obydwu obszarów zastosowań.

Opracowana metoda, integrując dwa podejścia do oceny bezpieczeństwa, reprezentowane przez standard Common Criteria oraz standard przemysłowy, przyczynia się do wzmocnienia kompatybilności pomiędzy nimi oraz do wzmocnienia bezpieczeństwa przemysłowego, które jest oceniane z punktu widzenia zagrożeń informatycznych. Tym samym podczas projektowania zabezpieczeń zgodnych z opracowanymi uszczegółowionymi/rozszerzonymi wymaganiami, metoda przyczynia się także do poprawy bezpieczeństwa w obydwu branżach.

Zaproponowane rozwiązanie stanowi wkład w dziedzinę informatyki, która dzięki temu zyskuje nowe, szersze możliwości projektowania, oceny i stosowania komplementarnych zabezpieczeń, chroniących przed atakami na systemy informatyczne i przemysłowe.

Wdrożenie metody oceny w laboratorium jest innowacją organizacyjną, ponieważ do realizacji ocen bezpieczeństwa będzie można wykorzystywać jedną, znormalizowaną metodę dla urządzeń informatycznych i przemysłowych, i która nie musi być dodatkowo walidowana na zgodność z ISO/IEC 17025. Ponadto, metoda posiada potencjał do tworzenia nowych metod oceny dla innych specyficznych urządzeń czy technologii. Klienci produktów IACS zyskują możliwość uzyskania dwóch certyfikatów bezpieczeństwa na normę Common Criteria i IEC 62443 podczas jednego procesu oceny, co stanowi istotną oszczędność czasu i kosztów.

Należy podkreślić, że zgodnie z aspektem wdrożeniowym doktoratu, zaproponowane rozwiązanie jest także zgodne i wpisuje się w strategię rozwoju Instytutu Łukasiewicz – EMAG oraz laboratorium ITSEF, która zakłada rozwijanie działalności w zakresie certyfikacji i oceny cyberbezpieczeństwa przemysłu 4.0 i systemów teleinformatycznych.

Opisane w pracy europejskie ramy certyfikacji cyberbezpieczeństwa dla produktów IT, IACS i innych, w tym przemysłowego Internetu rzeczy (ang. Industrial Internet of Things, IIoT) oraz nowe wydanie normy CC, wskazują na pewne trendy rozwoju certyfikacji i oceny.

Wskazują one, że programy certyfikacji budowane będą w oparciu o istniejące i sprawdzone w praktyce standardy i metodyki, poprzez ich udoskonalanie lub modyfikowanie w zależności od konkretnych potrzeb danej branży. Wydaje się, że jest to podejście nie tylko kosztowo zasadne, ale też najbardziej efektywne.

Ponadto, w Europie rozwijają się intensywnie tzw. lekkie programy oceny, które stosują ocenę zabezpieczeń w ograniczonym zakresie wymagań, ale w dalszym ciągu obejmującym najważniejsze aspekty analizy bezpieczeństwa, jak testowanie niezależne, analiza podatności i testy penetracyjne. Ten ograniczony zakres powoduje, że sama ocena trwa krócej i ma niższe koszty. W pracy doktorskiej wykonano analizę możliwości realizacji takiego podejścia w oparciu o najnowszą część normy CC p.4 i profile cPP i wydaje się, że jest to perspektywiczny kierunek dalszego rozwoju metod oceny dedykowanych dla danego typu produktu lub technologii.

Analiza stanu techniki i wiedzy, badanie potrzeb bezpieczeństwa dla systemów przemysłowych, wyniki projektów europejskich dotyczących rozwoju programów certyfikacji, a także prace legislacyjne w postaci Aktu o cyberbezpieczeństwie CSA, czy też dyrektywy NIS2, a także Aktu o cyberodporności (CRA) potwierdzają, że objęty w pracy doktorskiej kierunek pracy jest słuszny. Co więcej, zaproponowane możliwości przyszłego rozwijania metod w oparciu o cPP i normę CC p.4 potwierdzają sensowność kontynuacji prac.

Do mocnych stron rezultatów niniejszej pracy można zaliczyć opracowany kompletny zbiór wymagań uzasadnionego zaufania SAR oraz jednostek oceny, które w pełni pokrywają

wymagania bezpiecznego tworzenia produktu przemysłowego w myśl normy IEC 62443-4-1. Zbiór ten jest wystarczający do oceny wszystkich aspektów przemysłowych zgodnie z metodyką CEM i w ten sposób stanowi o kompletności opracowanej metody oceny dla IACS, ponieważ proces oceny w Common Criteria opiera się właśnie o wymagania SAR. Co więcej, wymagania te, pogrupowane w pakietach EAL, decydują o szczegółowości i rygoryzmie wykonanej oceny, a tym samym o poziomie zaufania do wyników oceny i samego produktu.

Inną mocną stroną rozwiązania są także zbiory rozszerzonych wymagań SFR dostosowanych do wymagań normy IEC 62443-4-2. Zbiory SFR_EXT mogą stanowić wsparcie konstruktora podczas opisu przemysłowych funkcji bezpieczeństwa, które należy włączyć do zadania zabezpieczeń. Zgodnie z CC, to konstruktor jest odpowiedzialny za samodzielne utworzenie rozszerzonych wymagań SFR zgodnie z wytycznymi CC, które są później weryfikowane zgodnie z CEM. W tym wypadku, opracowane w pracy tabele mapowania z wymaganiami SFR, zawierają przykłady gotowych do użycia komponentów.

Kolejną mocną stroną rozwiązania jest analiza sposobu tworzenia nowych metod oceny zgodnie z normą CC p.4. Podejście opisane w CC p.4 ułatwia proces, aczkolwiek niezbędne są do tego wyniki niniejszej pracy doktorskiej, która dostarcza jednostki oceny dla IACS, z których dalej wyprowadza się działania oceniające w normie CC p.4.

Ostatnią mocną stroną rozwiązania według autora, jest tabela 33 integrująca poziomy bezpieczeństwa zdefiniowane w CSA, poziomy EAL oraz SL z wartościami potencjałów ataków. Dzięki tej integracji dużo łatwiejsze jest prowadzenie analizy odporności urządzenia na ataki z uwzględnieniem poziomów EAL i SL, zadeklarowanych dla danego urządzenia.

Oczywiście, jak każde rozwiązanie także i to ma swoje słabe strony.

Zaliczam do nich ograniczony zbiór wymagań SFR_EXT, który powstał dla wybranego zestawu wymagań przemysłowych CR, choć w ocenie pilotażowej wykonano testy dla wszystkich 50 wymagań CR na poziomie SL 1. Opracowany ograniczony zbiór SFR_EXT nie wpływa na metodę oceny, gdyż komponenty SFR stosowane są przez konstruktorów do projektowania zabezpieczeń i nie są wykorzystywane do oceny wymagań. Dlatego też opracowany zbiór stanowi przykład, jak opracowywać wymagania bezpieczeństwa dla urządzeń przemysłowych.

Ograniczenie poziomu oceny pilotażowej do SL 1 także może być zaliczone do słabej strony, ale jest to raczej aspekt techniczny, nie wpływający na samą metodę oceny i możliwość wydawania werdyktów dla testów niezależnych urządzenia.

Słabą stroną, która może mieć wpływ na ostateczną postać metody oceny jest to, że dla oceny pilotażowej producent nie opracował dokumentacji produktu zgodnie z Common Criteria, w tym zadania zabezpieczeń, co wymagałoby z jego strony ogromnego wysiłku. W rezultacie, walidacja metody z zakresie oceny dokumentacji mogła się odbyć tylko poprzez weryfikację treści jednostek oceny, a nie na rzeczywistym przykładzie. Dla każdej jednostki

oceny postawiono pytanie, czy jest ona kompletna i gotowa do oceny odpowiadającej jej porcji materiału dowodowego bez względu na wydawany werdykt (Pass/Fail). W ramach ograniczonych zasobów w doktoracie, nie była możliwa ocena pełnego materiału dowodowego, gdyż nie był on dostępny. Przygotowanie takiej dokumentacji ze strony producenta to wielomiesięczna praca co najmniej kilkuosobowego zespołu przygotowanych merytorycznie specjalistów, wspomaganych zewnętrznymi konsultacjami, stąd tego typu praca nie była możliwa do zrealizowania. Dlatego też, w przyszłości w celu pełnej weryfikacji metody, należy wykonać dodatkową ocenę pilotażową z pełną dokumentacją produktu zgodną z CC.

Ograniczeniem dla szerszej interpretacji wyników doktoratu może być skoncentrowanie się na wariancie koncepcji opartej o adaptację standardu Common Criteria o wybraną normę przemysłową IEC 62443. Mimo, że podczas badania potrzeb bezpieczeństwa przemysłowego wykazano w pracy, że wybrana norma przemysłowa spełnia warunki, aby stać się głównym źródłem wymagań, to należałoby jednak szerzej spojrzeć na problem i zidentyfikować inne źródła wskazówek do adaptacji normy CC. Nawet, gdyby nie miałyby tak zgodnej z CC struktury i formy, jak wybrana norma IEC 62443.

Mimo to, uważam, że wykonane badania są ważne, gdyż zgodnie z założeniami metodyki CD&E oraz założeniem, że prace mają być w zasięgu realizacji doktoratu, to norma IEC spełnia je ze względu na zakres wymagań i strukturę ich prezentacji. Dzięki temu metoda oceny obejmuje zarówno wymagania dotyczące wytwarzania bezpiecznego produktu w całym cyklu życia, jak również techniczne wymagania bezpieczeństwa implementowane w tych produktach. Natomiast realizacja badań była efektywna ze względu na uporządkowaną i sformalizowaną strukturę normy, podobnie jak to ma miejsce w Common Criteria.

W przyszłości możliwe jest opracowanie rozszerzonej koncepcji rozwiązania problemu w oparciu o najnowszą aktualizację standardu wydaną w listopadzie 2022 r., a w szczególności jego część CC p.4 [17], która przedstawia model tworzenia metod oceny dla szczególnych typów TOE lub specyficznych technologii. Model ten daje możliwość tworzenia nowych jednostek oceny na bazie już istniejących.

W praktyce oznacza to, że ogólnie zdefiniowane jednostki oceny CEM są uszczegółowiane dla danego typu TOE lub technologii, a następnie grupowane w ramach nowej metod oceny przeznaczonej dla specyficznego produktu.

W związku z powyższym, rezultaty pracy doktorskiej mogą być zatem wykorzystane w przyszłości na dwa sposoby.

Pierwszy sposób może polegać na wykorzystaniu możliwości tworzenia metod oceny w oparciu o model przedstawiony w CC p.4. Metoda oceny opracowana w niniejszej pracy doktorskiej stanowi podbudowę pod kolejne etapy rozwoju metod oceny bezpieczeństwa w oparciu o metodykę CC. Autor pracy doktorskiej, definiując zbiory komponentów

rozszerzonych, komponentów uszczegółowionych oraz jednostek oceny, umożliwił ich wykorzystanie w przyszłości jako jednostki oceny wchodzące w skład metod budowanych zgodnie z CC p.4.

Drugi sposób umożliwia wykorzystanie opracowanych zestawów wymagań SAR i SFR do tworzenia profili zabezpieczeń cPP dla IACS. Dzięki zastosowaniu cPP projektowanie i ocena zabezpieczeń komponentów IACS będzie przebiegać szybciej i sprawniej, ponieważ projektanci urządzeń IACS otrzymają dokument cPP, w którym zawarte będą gotowe do implementacji zestawy wymagań bezpieczeństwa, a oceniający otrzymają dokument zawierający sposoby, jak weryfikować te wymagania.

Powyższe rozwiązania pozwolą na projektowanie oraz ocenę zabezpieczeń jednocześnie zgodnie z wymaganiami standardów informatycznego i przemysłowego z wykorzystaniem znormalizowanej metody oceny zabezpieczeń produktów informatycznych i przemysłowych.

Wśród produktów przemysłowych coraz częściej wymienia się komponenty przemysłowego Internetu rzeczy (ang. Industrial Internet of Things, IIoT). Analiza dostępnych metodyk, standardów i wytycznych dla tego rodzaju produktów mogłaby stanowić dodatkowe źródło wiedzy o wymaganiach, które należałoby uwzględnić podczas oceny bezpieczeństwa.

W celu pogłębienia analizy podatności wykonywanej zgodnie z CEM, można by wykonać badania przykładowych analiz wykonywanych przez producentów zgodnie z wymaganiami Praktyki 5. Wiedza pozyskana z wyników praktycznych testów penetracyjnych mogłaby pozwolić zidentyfikować nowe czynniki uwzględniane w obliczaniu potencjału ataku, które miałyby w ten sposób wpływ na otrzymywane wartości tego potencjału.

Dla pełnej weryfikacji metody należałoby wykonać pełny proces oceny produktu wraz z jego dokumentacją opracowaną zgodnie z normą Common Criteria na wyższych poziomach EAL oraz SL.

Ostateczna konkluzja niniejszej pracy doktorskiej jest zatem następująca: opracowana metoda oceny bezpieczeństwa dostarcza uniwersalny sposób zwiększania uzasadnionego zaufania do oceny zabezpieczeń przemysłowych i informatycznych oraz stanowi potencjał do dalszego rozwoju metod dla nowych typów produktów lub technologii.

Bibliografia

[1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. CCMB-2017-04-001, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components. CCMB-2017-04-002, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components. CCMB-2017-04-003, Version 3.1, Revision 5, April 2017.

[4] ISO/IEC 15408-1:2009(E) Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.

[5] ISO/IEC 15408-2:2008(E) Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components.

[6] ISO/IEC 15408-3:2008(E) Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components.

[7] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology. CCMB-2017-04-004, Version 3.1, Revision 5, April 2017.

[8] ISO/IEC 18045:2008 – Information technology – Security techniques – Methodology for IT security evaluation.

[9] R. Leszczyna, „Cybersecurity and privacy in standards for smart grids – A comprehensive survey," *O'Connor, R., Schummy, H. (eds.) Computer Standards & Interfaces*, tom vol. 56, pp. 62-73, 2018.

[10] R. Piggin, „Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security," w *IET Conference on Control and Automation 2013: Uniting Problems and Solutions*, Birmingham, 2013.

[11] „EN IEC 62443-4-1:2018 – Security for industrial automation and control systems, Part 4-1: Secure product development lifecycle requirements.," 2018.

[12] „EN IEC 62443-4-2:2019 – Security For Industrial Automation And Control Systems, Part 4-2: Technical Security Requirements For IACS Components," 2019.

[13] „IEEE 1686, IEEE Standard for Intelligent Electronic Devices (IED) Cyber Security Capabilities," 2013.

[14] „Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. CC:2022 Revision 1," CCRA, November 2022.

[15] „Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components. CC:2022 Revision 1," CCRA, November 2022.

[16] „Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components CC:2022 Revision 1," CCRA, November 2022.

[17] „Common Criteria for Information Technology Security Evaluation. Part 4: Framework for the specification of evaluation methods and activities. CC:2022 Revision 1," CCRA, November 2022.

[18] „Common Criteria for Information Technology Security Evaluation. Part 5: Pre-defined packages of security requirements. CC:2022 Revision 1," CCRA, November 2022.

[19] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams i A. Hahn, „NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security Revision 2,” 2015.

[20] ENISA, „Cybersecurity certification. EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS, V1.1.1,” ENISA, May 2021.

[21] P. Theron i A. Lazari, „The IACS Cybersecurity Certification Framework (ICCF). Lessons from the 2017 study of the state of the art. EUR 29237 EN,” Publications Office of the European Union, Luxembourg, 2018.

[22] „Projekt KSO3C,” [Online]. Available: https://www.kso3c.pl/. [Data uzyskania dostępu: 2022].

[23] „ PN-EN ISO/IEC 17025:2018-02 - wersja polska, Ogólne wymagania dotyczące kompetencji laboratoriów badawczych i wzorcujących.,” PKN, 2018.

[24] „PN-EN ISO/IEC 17065:2013-03 - wersja polska, Ocena zgodności -- Wymagania dla jednostek certyfikujących wyroby, procesy i usługi,” PKN, 2013.

[25] „PCA. Akredytowane podmioty, laboratoria badawcze,” [Online]. Available: https://www.pca.gov.pl/akredytowane-podmioty/akredytacje-aktywne/laboratoria-badawcze/AB%201781,podmiot.html. [Data uzyskania dostępu: 2022].

[26] „Mutual Recognition Agreement of nformation Technology Security Evaluation Certificates, Version 3.0,” Management Committee, SOG-IS, January 2010.

[27] „SOG-IS Senior Officials Group - Information Systems Security,” [Online]. Available: https://www.sogis.eu/index_en.html. [Data uzyskania dostępu: 2022].

[28] „CCRA – Arrangement on the Recognition of Common Criteria Certificates. In the field of Information Technology Security, July 2, 2014,” [Online]. Available: https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf. [Data uzyskania dostępu: 2023].

[29] C. Criteria, „CCRA Arrangement,” [Online]. Available: https://www.commoncriteriaportal.org/ccra/. [Data uzyskania dostępu: 2023].

[30] SOGIS, „Licensed ITSEFs,” [Online]. Available: https://www.sogis.eu/uk/labs_en.html#siec. [Data uzyskania dostępu: 2023].

[31] H. d. Nijs, „Concept Development and Experimentation Policy and Process: How Analysis Provides Rigour,” 2010.

[32] „DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/1148 z dnia 6 lipca 2016 r,” 2016.

[33] „USTAWA z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dz. U. 2018 poz. 1560,” 2018.

[34] „Think Tank Parlament Europejski,” [Online]. Available: https://www.europarl.europa.eu/thinktank/pl/document/EPRS_BRI(2021)689333. [Data uzyskania dostępu: 2022].

[35] M. Negreiro, „The NIS2 Directive. A high common level of cybersecurity in the EU,” EPRS - European Parliamentary Research Service, June 2022.

[36] „Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych,” 2019.

[37] „REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybesecurity Act),” 2019.

[38] J. Balcewicz i R. Babraj, „Analiza. Akt o cyberbezpieczeństwie - nowy mandat ENISA i certyfikacja cyberbezpieczeństwa,” NASK, Cyber POLICY, Warszawa, Maj 2019.

[39] „Joint Research Centre. European Reference Network for Critical Infrastructure Protection (ERNCIP),” ec.europa.eu, [Online]. Available: https://erncip-project.jrc.ec.europa.eu/networks/tgs/european-iacs. [Data uzyskania dostępu: 2023].

[40] „EU Science Hub,” [Online]. Available: https://joint-research-centre.ec.europa.eu/index_en. [Data uzyskania dostępu: 2022].

[41] P. THERON i S. BOLOGNA, „Proposals from the ERNCIP Thematic Group, Case studies for the cyber-security of Industrial Automation & Control Systems, for a European IACS Components Cyber-security Compliance & Certification scheme,” European Commission, EUR 27098 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen, 2014.

[42] P. THERON, J. F. RUIZ GUALDA, T. BOSWELL, J.-M. BRUN, R. CASCELLA, L. F. i e. all, „Recommendations for the Implementation of the Industrial Automation & Control Systems Components Cybersecurity Certification Scheme (ICCS),” European Commission, JRC121520, Ispra, 2020.

[43] „CEN/CENELEC,” [Online]. Available: https://standards.cencenelec.eu/. [Data uzyskania dostępu: 2023].

[44] „ENISA Cybersecurity Certification Conference 2022,” [Online]. Available: https://www.enisa.europa.eu/events/enisa-cybersecurity-certification-conference-2022/eccc2022-hybrid-conference. [Data uzyskania dostępu: 2022].

[45] „Wniosek. ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020,” Komisja Europejska, Bruksela, COM(2022) 454 final, 2022.

[46] „ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011,” Dziennik Urzędowy Unii Europejskiej, 2019.

[47] „ANNEXES 1 to 6. ZAŁĄCZNIKI do WNIOSKU DOTYCZĄCEGO ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniającego rozporządzenie (UE) 2019/1020,” Komisja Europejska, Bruksela, COM(2022) 454 final, 2022.

[48] A. Białas, Semiformal Common Criteria Compliant IT Security Development Framework, Studia Informatica vol. 29, Number 2B(77), Gliwice: Silesian University of Technology Press, 2008.

[49] A. Białas, Zastoswanie wzorców projektowych w konstruowaniu zabezpieczeń informatycznych zgodnych ze standardem Common Criteria, Katowice: Instytut Technik Innowacyjnych EMAG, ISBN 978-83-932737-2-0, 2011.

[50] D. Rogowski, „Software support for Common Criteria security development process on the example of a data diode," w *Proceedings of the Ninth International Conference DepCoS-RELCOMEX*, Brunów, 2014.

[51] D. Rogowski, „Software Implementation of Common Criteria Related Design Patterns," w *Proceedings of the 2013 Federated Conference on Computer Science and Information Systems (FedCSIS)*, Kraków, 2013.

[52] „CVE, Common Vulnerabilities and Exposures," [Online]. Available: https://www.cve.org/. [Data uzyskania dostępu: 2023].

[53] „Common Criteira Certified Products List - Statistics," [Online]. Available: https://www.commoncriteriaportal.org/products/stats/. [Data uzyskania dostępu: 2022].

[54] A. Białas, „Computer Support for Development of Biometric Systems with Claimed Assurance," w *Studia Informatica, Volume 40, Number 1 (138),* Gliwice, Silesian University of Technology Press, 2019, pp. 5-30.

[55] A. Białas, „Computer-Aided Sensor Development Focused on Security Issues," *Sensors,* 2016.

[56] A. Białas, „Vulnerability Assessment of Sensor Systems," *Sensors,* 2019.

[57] E. Knapp, Industrial Network Security. Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, Waltham: Elsevier Inc., 2011.

[58] F. Xie, Y. Peng, W. Zhao i e. al, „Evaluating Industrial Control Devices Security: Standards, Technologies and Challenges," w *13th IFIP TC8 International Conference on Computer Information Systems and Industrial Management Applications (CISIM 2014),* Ho Chi Minh, 2014.

[59] D. Rogowski, „Identification of Information Technology Security Issues Specific to Industrial Control Systems," w *Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J. (eds) Contemporary Complex Systems and Their Dependability. DepCoS-RELCOMEX 2018*, Brunów, 2018.

[60] E. J. M. Colbert i A. Kott, Cyber-security of SCADA and Ohter Industrial Control Systems. Advances in Information Security Volume 63, Fairfax, USA: Springer, 2016.

[61] „ISO/IEC TR 15446 Information technology — Security techniques — Guide for the production of Protection Profiles and Security Targets," ISO/IEC, Geneva, 2009.

[62] „Guidelines for Evaluation Reports according to Common Criteria Version 3.1," BSI, Bundesamt für Sicherheit in der Informationstechnik, Bonn, 2010.

[63] D. Rogowski, „Metodyka oceny zabezpieczeń teleinformatycznych," w *Studia Informatica, Zeszyty Naukowe Politechniki Śląskiej, Vol. 24, No 2B (54)*, Gliwice, Wydawnictwo Politechniki Śląskiej, 2003, pp. 251-264.

[64] „ISA International Society of Automation," [Online]. Available: https://www.isa.org/. [Data uzyskania dostępu: 2023].

[65] „ISA Global Cybersecurity Alliance," 2023. [Online]. Available: https://isaautomation.isa.org/cybersecurity-alliance/.

[66] „The ISAGCA Blog," [Online]. Available: https://gca.isa.org/blog. [Data uzyskania dostępu: 2023].

[67] I. o. blog, „Why are cyberattack shifting to ICS?,” [Online]. Available: https://gca.isa.org/blog/why-are-cyberattacks-shifting-to-ics. [Data uzyskania dostępu: 2023].

[68] Wikipedia, „Colonial Pipeline,” [Online]. Available: https://en.wikipedia.org/wiki/Colonial_Pipeline. [Data uzyskania dostępu: 2023].

[69] S. Karnouskos, „Stuxnet worm impact on industrial cyber-physical system security,” w *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, Melbourne, 2011.

[70] R. M. Lee, M. J. Assante i T. Conway, „Analysis of the Cyber Attack on the Ukrainian Power Grid,” E-ISAC, Electricity - Information Sharing and Analysis Center, Washington, 2016.

[71] „Wikipedia,” [Online]. Available: https://pl.wikipedia.org/wiki/WannaCry. [Data uzyskania dostępu: 2022].

[72] „CVE,” [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228. [Data uzyskania dostępu: 2022].

[73] B. Babu, M. P. Thafasal Ijyas i V. Justin, „Security issues in SCADA based industrial control systems,” w *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, (ICACC) (2017): 47-51..

[74] P. Theron, „Introduction to the European IACS components Cybersecurity Certification Framework (ICCF),” Publications Office of the European Union, Luxembourg, 2016.

[75] CyberX, „Global ICS & IIoT Risk Report. A data-driven analysis of vulnerabilities in our critical industrial infrastructure,” CyberX, October 2017.

[76] A. C. D. Agency, „Cybersecurity and Infrastructure Security Agency,” [Online]. Available: https://www.cisa.gov/. [Data uzyskania dostępu: 2023].

[77] ICS-CERT, „ICS-CERT Annual Assessment Report FY 2016,” US Department of Homeland Security, National Cybersecurity and Integration Center (NCCIC), 2016.

[78] „VERVE OT/ICS Endpoint Security Platform,” [Online]. Available: https://verveindustrial.com/. [Data uzyskania dostępu: 2023].

[79] VERVE, „2021 ICS Advisory Report,” [Online]. Available: https://verveindustrial.com/resources/2021-22-ics-advisory-report/. [Data uzyskania dostępu: 2023].

[80] „CVSS Common Vulnerability Scoring System SIG,” [Online]. Available: https://www.first.org/cvss. [Data uzyskania dostępu: 2023].

[81] „Common Vulnerability Scoring System version 3.1, Specification Document, Revision 1,” FIRST.Org, 2019.

[82] T. Macaulay i B. Singer, Cybersecurity for Industrial Control Systems, New York: CRC Press, 2011.

[83] I. Calvo, M. Etxeberria-Agiriano i P. González-Nalda, „Key Vulnerabilities of Industrial Automation and Control Systems and Actions to Prevent Cyber-Attacks,” *International Journal of Online Engineering (iJOE) vol. 12, no. 01*, p. pp. 9–16, 2016.

[84] X. Zhou, Z. Xu, L. Wang i K. Chen, „What should we do? A structured review of SCADA system cyber security standards,” w *2017 4th International Conference on*

Control, Decision and Information Technologies (CoDIT), Barcelona, Spain, 2017, pp. 0605-0614, doi: 10.1109/CoDIT.2017.8102661.

[85] T. Miyachi i Y. Tsutomu, „Current issues and challenges on cyber security for industrial automation and control systems," w *2014 Proceedings of the SICE Annual Conference (SICE) (2014): pp. 821-826*, Sapporo, Japan, 2014.

[86] EN ISO/IEC 27000:2020 - Information technology - Security techniques - Information security management systems - Overview and vocabulary, CEN/CLC/TC 13 - CYBERSECURITY AND DATA PROTECTION, 2020.

[87] S. Fritsch, T. Glemser, S. Heyde i H. Muehlbauer, „TeleTrusT Evaluation Method for IEC 62443-4-2. Security for Industrial Automation and Control Systems," IT Security Association Germany (TeleTrusT), Berlin, 2019.

[88] A. Białas, Komputerowe wspomaganie procesu rozwoju produktów informatycznych o podwyższonych wymaganiach bezpieczeństwa, Katowice: Wydawnictwo Instytutu Technik Innowacyjnych EMAG, ISBN 978-83-932737-8-2, 2012.

[89] „Collaborative Protection Profile (cPP) for Network Devices, Version 2.2," Network Device international Technical Community (ND iTC), 2019.

[90] „International Technical Communities and Collaborative Protection Profiles," Common Criteria, [Online]. Available: https://www.commoncriteriaportal.org/communities/technical_communities.cfm. [Data uzyskania dostępu: 2023].

[91] „Collaborative Protection Profiles (cPP) and Supporting Documents (SD)," Common Criteria, [Online]. Available: https://www.commoncriteriaportal.org/pps/?cpp=1. [Data uzyskania dostępu: 2023].

[92] „Technical Communities," Common Criteria, [Online]. Available: https://www.commoncriteriaportal.org/communities/index.cfm. [Data uzyskania dostępu: 2023].

[93] PN-EN IEC 62443-3-3:2020-01. Przemysłowe sieci komunikacyjne. Bezpieczeństwo sieci i systemów. Część 3-3: Wymagania dla systemu bezpieczeństwa i poziomów bezpieczeństwa, Warszawa: PKN, 2020.

[94] IEC TS 62443-1-1 Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models, IEC, International Electrotechnical Commission, 2009, Edition 1.0.

[95] „SOG-IS MRA. Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, v3.0," Mangement Committee of SOG-IS, 2010.

[96] „Text of the Agreement," SOG-IS, [Online]. Available: https://www.sogis.eu/documents/mra/20100107-sogis-v3.pdf. [Data uzyskania dostępu: 2023].

[97] ISO/IEC 15408-4:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities.

[98] E. D. Knapp i J. T. Langill, Industrial Network Security. Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Ohter Industrial Control Systems. Second Edition, Waltham, USA: Elsevier, 2015.

[99] R. Leszczyna, „Protecting Industrial Control Systems. Recommendations for Europe and Member States," European Network and Information Security Agency (ENISA), 2011.

[100] „Evaluation Activities for Network Device cPP, Version 2.2. Supporting Document, Mandatory Technical Document," CCDB, 2019.

Spis tabel

Spis rysunków

Słownik pojęć i akronimów

Tabela 35. Najważniejsze pojęcia i skróty użyte w pracy

Pojęcie/skrót	Definicja
CB	(ang. *Certification Body*) – Jednostka certyfikująca (JC) organizacja odpowiedzialna za realizowanie certyfikacji i ciągły nadzór nad działalnością Schematu Oceny i Certyfikacji, nadzoruje laboratoria ITSEF.
CC	(ang. *Common Criteria for Information Technology Security Evaluation*) - Wspólne Kryteria do oceny zabezpieczeń teleinformatycznych – metodyka do projektowania i oceny zabezpieczeń teleinformatycznych opisana także w międzynarodowej normie ISO/IEC 15408 [4].
CCRA	(ang. *Common Criteria Recognition Arrangement*) – międzynarodowe porozumienie [28] o wzajemnym uznawaniu certyfikatów CC do poziomu uzasadnionego zaufania EAL2, a w przypadku wspólnych profili zabezpieczeń (ang. cPP – collaborative Protection Profile) do poziomu EAL4
CEM	(ang. *Common Evaluation Methodology for IT Security Evaluation*) [7] – metodyka oceny zabezpieczeń uzupełniająca Wspólne Kryteria (CC) i opisana w normie ISO/IEC 18045, opisującej szczegółowo działania wykonywane podczas oceny zabezpieczeń produktów IT.
Certyfikacja	(ang. *Certification*) – proces realizowany przez *Jednostkę Certyfikującą* prowadzący do wydania certyfikatu.
cPP	(ang. *Collaborative Protection Profile*) - wspólny profil zabezpieczeń [90], [91] opracowany w ramach współpracy międzynarodowych komitetów technicznych (ang. *iTC – international Technical Communities*) [92] sprzedawców, laboratoriów testujących, krajów porozumienia CCRA.
CR	(ang. *Component Requirement*) – techniczne wymagania bezpieczeństwa dla komponentów budujących system IACS wg IEC 62443-4-2 [12]. Wymagania wywodzą się od technicznych wymagań bezpieczeństwa dla systemu IACS zdefiniowanych w normie IEC 62443-3-3 [93]. Wymaganie CR może zawierać rozszerzenia RE (ang. *Requirement Enhancement*). Kombinacja wymagania CR i jego rozszerzeń RE określają docelowy poziom bezpieczeństwa, który jest osiągalny dla komponentu IACS.
EA	(ang. *Evaluation activities*) – działanie oceniające wyprowadzone z oryginalnych jednostek WU z metodyki CEM w celu ich dostosowania do oceny SAR_EXT, SFR_EXT; stosowane w profilach cPP oraz do tworzenia zbiorów EA w postaci metody oceny zgodnie z normą CC p.4.
EAL	(ang. *Evaluation Assurance Level*) – poziom uzasadnionego zaufania (wiarygodności) do oceny zabezpieczeń; skala EAL jest siedmiostopniowa: EAL1 – EAL7; skład pakietów odpowiadających poziomom uzasadnionego zaufania (EAL) jest podany w normie ISO/IEC 15408-3 (CC Part 3) [3].
ETR	(ang. *Evaluation Technical Report*) – raport techniczny oceny, który przedstawia wynik całościowej oceny TOE wraz z uzasadnieniami dla poszczególnych werdyktów i jest dostarczany do jednostki certyfikującej celem jego walidacji.
Evaluation	Ocena – ocena PP, ST lub TOE, wg kryteriów określonych w CC p.3 i w sposób określony w metodyce CEM.
FR	(ang. *Foundational Requirment*) – wymaganie fundamentalne, jedno z siedmiu wymagań podstawowych zdefiniowanych w IEC TS 62443-1-1 [94]: 1) Identyfikacja i autoryzacja (IAC, Identification and Authentication Control), 2) Kontrola użycia (UC, Use Control), 3) Integralność systemu (SI, System

	Integrity), 4) Poufność danych (DC, Data Confidentiality), 5) Ograniczenie przepływu danych (RDF, Restricted Data Flow), 6) Czasowa odpowiedź na zdarzenia (TRE, Timely Response to Events), 7) Dostępność zasobów (RA, Resource Availability).
IACS	(*ang. Industrial Automation and Control System*) – system sterowania i automatyki przemysłowej, wg IEC 62443, to kombinacja personelu, sprzętu, oprogramowania, procedur i polityk zaangażowanych w działanie procesu przemysłowego, która może oddziaływać lub mieć wpływ na jego bezpieczne, pewne i niezawodne działanie.
ITSEF	(ang. *IT Security Evaluation Facility*) – akredytowana jednostka oceniająca (ang. *Accredited Evaluation Facility*), licencjonowana lub upoważniona do wykonywania ocen produktów IT w kontekście konkretnego schematu oceny i certyfikacji bezpieczeństwa informatycznego obowiązującego w danym kraju i nadzorowanego przez Jednostkę certyfikującą.
Klasa	(ang. *Class*) - klasa – zbiór rodzin CC, które odnoszą się do jednej dziedziny
Komponent	(ang. *Component*) – komponent CC - najmniejszy możliwy do wyboru zbiór elementów z danej rodziny wymagań, na których mogą być oparte wymagania
Komponent IACS	(ang. *IACS Component*) – komponent, urządzenie sprzętowe, sprzętowo-programowe, programowe, która jest częścią składową system automatyki i sterowania (IACS). Do komponentów zaliczane są takie kategorie urządzeń jak: aplikacja programowa (*ang. Software Application, SA*); urządzenie wbudowane (*ang. Embedde Device, ED*); urządzenie hosta (*ang. Host Device, HD*); urządzenie sieciowe (*ang. Network Device, ND*).
OR	(ang. Observation Report) - raport uwag (obserwacji), raport sporządzany przez ewaluatora, zawierający spostrzeżenia i niezgodności zidentyfikowane podczas oceny bezpieczeństwa TOE, dostarczany do klienta w celu wdrożenia działań korygujących lub wyjaśniających.
OSP	(*ang. Organizational Security Policy*) - polityka bezpieczeństwa organizacji – zbiór zasad bezpieczeństwa, procedur lub wytycznych danej instytucji; polityki mogą odnosić się do konkretnego środowiska operacyjnego produktu
Potencjał ataku	(ang. *Attack Potential*) – środki i ich siła stosowane w trakcie ataku na zasoby TOE (doświadczenie, motywacja, okno dostępu i narzędzia agenta zagrożenia).
PP	(ang. *Protection Profile*) – profil zabezpieczeń, zbiór wymagań bezpieczeństwa dla danego typu produktów IT, niezależny od sposobu implementacji.
Praktyka, P	*(ang. Practice*) – praktyka – wg IEC 62443-4-1 sposób postępowania dotyczący bezpiecznego projektowania, wytwarzania, testowania, utrzymywania i wycofania z użycia produktu w celu spełnienia wymagań dotyczących tworzenia bezpiecznych produktów.
Problem bezpieczeństwa	(ang. *Security problem*) – analiza, która określa charakter i zakres aspektów bezpieczeństwa w odniesieniu do TOE w postaci kombinacji zagrożeń, polityk bezpieczeństwa instytucji i założeń na środowisko operacyjne TOE.
RE	(ang. *Requirement Enhancement*) – rozszerzenie wymagania CR lub SR względem wymagania podstawowego poprzez dodanie nowych lub zwiększonych potrzeb bezpieczeństwa.
RR	(ang. *Requirement Refinement*) – w normie CC oznacza dodanie szczegółów do treści wymagania komponentu SAR lub SFR precyzujących lub zwiększających wymagania dla specyficznego zastosowania.
Rodzina	(*ang. Family*) – w normie CC oznacza zbiór komponentów SFR lub SAR, należących do danej klasy wymagań i posiadający podobny cel, ale różniących się rygoryzmem wymagań.
SAR	(ang. *Security Assurance Requirement*) – wymagania na uzasadnione zaufanie do zabezpieczeń.

SAR_EXT	(*ang. Extended*) – komponent dodatkowy SAR powstały wskutek braku odpowiedniego wymagania w normie CC p.3 dla danego TOE. W tej pracy oznacza także komponent SAR uszczegółowiony poprzez operację [*refinement*].
SFR	(ang. *Security Functional Requirement*) – wymagania na funkcjonalność zabezpieczeń.
SFR_EXT	(*ang. Extended*) – komponent dodatkowy SFR powstały wskutek braku odpowiedniego wymagania w normie CC p.2 dla danego TOE. W tej pracy oznacza także komponent SFR uszczegółowiony poprzez operację [*refinement*] lub operację [*assignement*].
SL	(ang. Security Level) – miara pewności (zaufania), że system IACS jest wolny od podatności i działa w zamierzony sposób [93].
SL – T	(ang. *Target Security Level*) – docelowy poziom bezpieczeństwa dla danego systemu wg normy IEC TS 62443-1-1 [94]. Zwykle wyznaczany w drodze szacowania ryzyka dla systemu i określeniu, że system wymaga danego poziomu bezpieczeństwa, aby zapewnić jego poprawne działanie.
SL – C	(ang. *Capability Security Level)* – osiągalny poziom bezpieczeństwa dla komponentu lub systemu IACS wg normy IEC TS 62443-1-1 [94], który określa jakie są możliwości spełnienia przez komponent wymagań danego poziomu bezpieczeństwa SL (Security Level), jeśli zostanie prawidłowo skonfigurowany. Poziom ten określa, że komponent lub system są w stanie osiągnąć docelowy poziom bezpieczeństwa (ang. Target Security Level, SL-T) bez dodatkowych uzupełniających (kompensujących) zabezpieczeń, gdy jest poprawnie skonfigurowany i zintegrowany.
SL – A	(ang. *Achieved Security Level*) – rzeczywisty, osiągnięty poziom bezpieczeństwa danego systemu. Poziom ten jest mierzony po zaprojektowaniu systemu lub jego uruchomieniu w miejscu pracy.
SR	(ang. *System Requirement)* - techniczne wymagania bezpieczeństwa dla całego systemu IACS wg IEC 62443-3-3 [93] powiązane z siedmioma wymaganiami fundamentalnymi (ang. *Foundational Requirements, FRs*) opisanymi w normie IEC TS IEC TS 62443-1-1 [94]. Wymaganie SR może zawierać rozszerzenia RE (ang. *Requirement Enhancement*). Kombinacja wymagania SR i jego rozszerzeń RE określają docelowy poziom bezpieczeństwa, który jest osiągalny dla systemu IACS.
SOG-IS	(ang. *Senior Officials Group – Information Systems Security*) [27] – Grupa Wysokich Urzędników ds. Bezpieczeństwa Systemów Informacyjnych powołana decyzją Rady UE z dnia 31 marca 1992 r. (92/242/EEC).
SOG-IS MRA	(ang. *SOG-IS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*) [95], [96] – porozumienie, które powstało na bazie grupy SOG-IS w dniu 8 stycznia 2010 r. Porozumienie skupia organizacje i instytucje rządowe z 11 krajów UE i EFTA (ang. *European Free Trade Association*) i dotyczy wzajemnego uznawania certyfikatów do poziomu uzasadnionego zaufania EAL4, a do poziomu EAL7 dla dwóch dziedzin technicznych: 1) karty inteligentne i podobne urządzenia (ang. *Smart Cards and Similar Devices*); 2) urządzenia sprzętowe z zabezpieczeniami (ang. *Hardware Devices with Security Boxes*).
SPD	(ang. *Security Problem Definition*) – definicja problemu bezpieczeństwa, część zadania zabezpieczeń (ST) lub profilu zabezpieczeń (PP) zawierająca opis problemu bezpieczeństwa, który będzie rozwiązany za pomocą zabezpieczeń TOE oraz zabezpieczeń środowiska operacyjnego TOE.

ST	(ang. *Security Target*) – zadanie zabezpieczeń, zbiór wymagań bezpieczeństwa ukierunkowany na określony sposób implementacji TOE zawierający deklarację poziomu uzasadnionego zaufania EAL.
TOE	(ang. *Target of Evaluation*) – przedmiot oceny, produkt IT w postaci sprzętowej, oprogramowania lub oprogramowania układowego (także ich kombinacja) wraz z jego dokumentacją podlegający ocenie w certyfikowanych laboratorium oceniającym CC.
TSF	(ang. *TOE security functionality*). Funkcjonalność zabezpieczeń TOE – połączenie funkcjonalności całego sprzętu, oprogramowania i oprogramowania układowego produktu, które zapewnia prawidłową realizację wymagań na funkcjonalność zabezpieczeń (SFR) opisanych w drugiej części normy CC.
TSFI	(ang. *TSF Interface*). Interfejs funkcji zabezpieczającej, za pomocą którego jednostki zewnętrzne (lub podmioty w TOE, ale spoza TSF) dostarczają dane do TSF, otrzymują dane z TSF i wywołują usługi TSF.
WU	(ang. *Work Unit*) – jednostka oceny, najmniejsze niepodzielne działanie oceniającego opisane w metodyce CEM umożliwiające wydanie jednoznacznego werdyktu (oceny) danego wymagania.
WU_EXT	(ang. *Extended WU*) – jednostka oceny WU, która powstała wskutek utworzenia komponentu SAR_EXT.
Uzasadnione zaufanie	(ang. *assurance*) – podstawa do zaufania, że oceniany produkt IT (TOE) realizuje zdefiniowane dla niego cele zabezpieczeń.

Załącznik 1. Komponenty wymagań wykorzystane w metodzie oceny IACS

Mapowanie Praktyk IEC 62443-4-1 na następujące wymagania Common Criteria:

- Oryginalne, niezmienione wymaganie SAR, czcionka czarna,
- SAR [*refinement*] po operacji uszczegółowienia, czcionka niebieska,
- SAR_EXT po zdefiniowaniu wymagania dodatkowego, czcionka zielona,
- WU jednostki oceny po adaptacji do wymagań SAR [*refinement*] i SAR_EXT
- kolorem czerwonym wyróżniono komponent wymagań, który został użyty do walidacji metody w trakcie pilotażowej oceny urządzenia IACS.

Tabela 36. Adaptacja wymagań SAR do Praktyk IEC 62443-4-1

Practice	Process requirement	SAR class, family, component	CC adapted SARs / [*refinement*]/ EXT	CC adapted Work Units (WU_EXT)
Practice 1 - Security management	SM-1: Development process	**ALC_LCD.1**	NA	NA
	SM-2: Identification of responsibilities			
	SM-3: Identification of applicability			
	SM-4: Security expertise	**ALC_LCD.1 [*refinement 1*] Developer defined life-cycle model**	**ALC_LCD.1.1C** [*The life-cycle definition documentation shall include evidence that the organization established a process for identifying and providing security training and assessment programs to ensure that personnel assigned to the organizational roles and duties have demonstrated security expertise appropriate for those processes of the life-cycle*]	ALC_LCD.1-1(1) Evaluation activities [*The evaluator shall examine the documented description of the life-cycle model used to determine that it covers that personnel involved in security-related processes have adequate expertise for the specific tasks to which they are assigned. Expertise can have been gained by training, experience, seminars, conferences, certifications, etc.]*
	SM-5: Process scoping	**ALC_LCD.1 [*refinement 2*] Developer defined life-cycle model**	**ALC_LCD.1.1C** [*The life-cycle definition documentation shall include justification by documented security analysis to identify the parts of IEC 62443-4-1 and IEC 62443-4-2 documents that are*	ALC_LCD.1-1(2) Evaluation activities [*The evaluator shall examine the documented description of the life-cycle model used to determine that it covers which parts of standards IEC 62443-4-1*

			applicable to a selected product development project]	*and IEC 62443-4-2 the product claims conformance*]
	SM-6: File integrity	**ALC_DEL.1**	NA	NA
	SM-7: Development environment security	**ALC_DVS.1**	NA	NA
	SM-8: Controls for private keys			
	SM-9: Security requirements for externally provided components	**ALC_CMS.1 [*refinement*] TOE CM coverage**	ALC_CMS.1.2C [*The configuration list shall uniquely identify the configuration items for externally provided components of the TOE. The list shall include supply chain security evidence that applies to components which are included within the product*] [*The configuration scope shall have evidence that third-party components conform to the requirements used in IEC 62443-4-1 when they can have an impact on security*]	ALC_CMS.1-2 Evaluation activities [The evaluator shall examine the configuration list to determine that it uniquely identifies each configuration items from external providers] [*The evaluator shall examine if external components claim conformance with requirements for IACS included in IEC 62443-4-1 and 4-2 standards*]
	SM-10: Custom developed components from third-party suppliers			
	SM-11: Assessing and addressing security related issues	**ALC_FLR.3 Systematic flaw remediation**	NA	NA
	SM-12: Process verification	**ALC_LCD.1 [*refinement 3*] Developer defined life-cycle model**	**ALC_LCD.1.1C** [*The life-cycle definition documentation shall include security development life-cycle verification whether it was applied and completed, prior to product release, with all applicable security-related processes required by the specification in Practice 1, SM-5 Process scoping requirement*] [*The security development life-cycle (SDL) documentation shall include processes for continuously*	ALC_LCD.1-1(3) Evaluation activities [*The evaluator shall examine the documented description of security development life-cycle (SDL) to determine that it includes the stages of verification and improvement SDL. This evidence is required to ensure that product vendors improve the rigor of their SDL over time for maintaining and improving product quality*]
	SM-13: Continuous improvement			

			improvement of the SDL] *justification by documented security analysis to identify the parts of IEC 62443-4-2 and IEC 62443-4-2 documents that are applicable to a selected product development project*]	
Practice 2 - Specification of security requirements	SR-1: Product security context	**ALC_LCD.1 [*refinement 4*] Developer defined life-cycle model**	**ALC_LCD.1.1C** [*The life-cycle definition documentation shall document the intended security context for the IACS component. The security context shall include information about product's location, security measures provided by the operational environment, isolation, and potential impact to the environment*]	**ASE_LCD.1-1(4)** Evaluation activities [*The evaluator shall examine the life-cycle definition documentation to determine that it describes the product security context which is to ensure that the minimum requirements of the environment and the assumptions about that environment are documented in order to achieve the security level (SL) for which the product was design*] [*The life-cycle definition documentation could describe: a) location in the network, b) physical or cyber security provided by the environment where the product will be deployed; c) isolation (form a network perspective), and d) if known, potential impact to the environment (for example, loss of life, injury, loss of production, etc.*)] [*The life-cycle definition documentation should document whether physical security is required provided by the operational environment*]

	SR-2: Threat model	**ALC_LCD.1 [*refinement 5*] Developer defined life-cycle model**	**ALC_LCD.1.1C** [*The life-cycle definition documentation for the current development scope of the product shall include a threat model specific to product*]	ALC_LCD.1-1(5) Evaluation activities [*The evaluator shall examine the documented description of the life-cycle model used to determine that it covers the threat model for the current development scope of the product*] [*The description of the threat model should include items a) to m) in Practice 2, SR-2 requirement*] [*The evaluator shall examine if the threat model is reviewed by the development team (at least one a year) for released products and updated if required in response to the emergence of new threats*]
	SR-3: Product security requirements SR-4: Product security requirements content SR-5: Security requirements review	**ALC_LCD.1 [*refinement 6*] Developer defined life-cycle model**	**ALC_LCD.1.1C** [*The life-cycle definition documentation shall include the security requirements related to the life-cycle of the product including installation, operation, maintenance and decommissioning*] [*The security requirements shall include: a) security privileges to install, operate, and maintain the product; b) security options, including removal of default passwords, used to install, configure, operate and maintain the product, and c) security actions associated with removing the product from use*] [*The security requirements shall include the information about: a) the scope and boundaries of the component or system; b) the required capability security level (SL-C)*	ALC_LCD.1-1(6) Evaluation activities [*The evaluator shall examine the documented description of the life-cycle model to determine that it covers the security requirements related to the life-cycle of the product*]

			of the product] [*The life-cycle definition shall document the process of requirements revision to ensure that requirements are valid, understood and verifiable*]	
Practice 3 - Secure by design	SD-1: Secure design principles	**ADV_FSP Functional specification** **ADV_TDS TOE design**	NA	NA
	SD-2: Defense in depth design	**ADV_ARC.1 [*refinement*] Security architecture description**	**ADV_ARC.1.1D** [*The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed. To achieve this feature the developer shall implement multiple layers of defense (in depth design) by using a risk-based approach based on the security problem definition*] **ADV_ARC.1.5C** [*The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality also by assigning responsibilities to each layer of defense*]	**ADV_ARC.1-5** Evaluation activities [*The evaluator shall examine the security architecture description to determine that it presents an analysis that adequately describes how the SFR-enforcing mechanisms cannot be bypassed by using layers with defense mechanisms*] [*The evaluator shall examine if each layer provides an additional defense mechanism, has a responsibility and provides attack surface reduction for the next layer so that the TSF behind this layer cannot be bypassed. In the in-depth design it is assumed that the layer in front of the next layer can be compromised*]
	SD-3: Security design review	**ALC_LCD.1 [*refinement 7*] Developer defined life-cycle model**	**ALC_LCD.1.1C** [*The life-cycle definition shall include a stage for the security design reviews for identifying, characterizing and tracking to closure security-related issues associated with each significant revision of the secure design. The stage of security design reviews shall include the following actions: a) identification of security requirements that were not adequately addressed by the*	**ALC_LCD.1-1(7)** Evaluation activity [*The evaluator shall examine the documented description of the life-cycle model used to determine that it covers the stage of security design reviews which consists of the actions listed in the content and presentation evidence element]*

			design, b) threats and their ability to exploit product interfaces, trust boundaries, and assets, c) identification of secure design practices that were not followed (for example, failure to apply principle of least privilege]	
	SD-4: secure design best practices	**ALC_LCD.1 [*refinement 8*] Developer defined life-cycle model**	**ALC_LCD.1.1C** [*The life-cycle definition with a stage for the security design shall document that secure design best practices are applied to the design process. Secure design practices should include: a) least privilege, b) using proven secure components, c) economy of mechanism (striving for simple design), d) using secure design patterns, e) attack surface reduction, f) documenting all trust boundaries as part of the design, and g) removing debug ports, headers and traces from circuit boards used during development from production hardware or documenting their presence and the need to protect them from unauthorized access]*	**ALC_LCD.1-1(8)** Evaluation activity [*The evaluator shall examine the documented description of the life-cycle model used to determine that it covers the stage of security design and that it includes the description of best practices used in that stage. The evaluator shall examine which best practices are implemented in the design phase and to ensure that guidance is provided to developers to help them avoid common pitfalls during design that could lead to later security issues]*
Practice 4 - Secure implementation	SI-1: Security implementation review	**ALC_LCD.1 [*refinement 9*] Developer defined life-cycle model**	**ALC_LCD.1.1C** [*The life-cycle definition shall include a stage for the security implementation reviews for identifying, characterizing and tracking to closure security-related issues associated with the implementation of the secure design. The stage of security implementation reviews shall include the following actions: a) identification of security requirements that were not adequately addressed by the implementation, b) identification of secure coding standards that were not followed, c) static code analysis (SCA) for source code, d) review of the implementation and its*	**ALC_LCD.1-1(9)** Evaluation activity [*The evaluator shall examine the documented description of the life-cycle model used to determine that it covers the stage of security implementation reviews which consists of the actions listed in the content and presentation evidence element]*

			traceability to the security capabilities defined to support the security design, and e) examination of threats and their ability to exploit implementation interfaces, trust boundaries and assets]	
	SI-2: Secure coding standards	**ALC_TAT.1 [*refinement*] Well-defined development tools**	**ALC_TAT.1.1C** [*Each development tool used for implementation shall be well defined in terms of incorporating security coding standards that are periodically rewired and updated and include at a minimum: a) avoidance of potentially exploitable implementation constructs, b) avoidance of banned functions and coding constructs/design patterns, c) automated tool use and settings, d) secure coding practices, e) validation of all inputs that cross trust boundary, f) error handling*]	**ALC_TAT.1-1** Evaluation activity [*The evaluator shall examine the development tool documentation provided to determine that each development tools are well-defined it means it includes at a minimum information listed in the content and presentation evidence*]
Practice 5 - Security verification and validation testing (*SAR_EXT family name - SVV*)	SVV-1: Security requirements testing	**ATE_FUN.1 [*refinement*] Functional testing** **ATE_IND.1 [*refinement*] Independent testing - conformance**	**ATE_FUN.1.2C** [*The test plan shall identify tests for verifying that the product handles error scenarios and invalid input correctly. Types of testing shall include: a) functional testing of security requirements defined by Foundational Requirements (FRs) for IACS, b) performance and scalability testing, and c) boundary/edge condition, stress and malformed or unexpected input tests*] **ATE_IND.1.2E** [*The evaluator shall test the TSFs to confirm they operate as specified by SFRs derived from Foundational Requirements (FRs) for IACS components*]	**ATE_FUN.1-2** Evaluation activity [*The evaluator shall examine the test plan to determine that it describes the scenarios for performing each type of tests according to Foundational Requirements (FRs) for IACS components*] **ATE_IND.1-3** Evaluation activity [*The evaluator shall devise a test subset for TSFs defined by SFRs derived from Foundational Requirements (FRs) for IACS components. The evaluator shall produce a test subset documentation which includes expected results, actual results, and acceptance criteria*]

	SVV-2: Threat mitigation testing (TMT) *(SAR_EXT component name)*	**ATE Tests**	**ATE_SVV_EXT.1 - Threat mitigation testing** ATE_SVV_EXT.1.1D [The developer shall test and document the effectiveness of the mitigation for the threats identified and validated in the threat model and security problem definition (SPD) in ST. The developer shall execute activities a) and b) from Practice 5, SVV-2 requirement] ATE_SVV_EXT.1.1C [The test documentation shall include the examples of threat mitigation testing such as: spoofing, tampering, repudiation, information disclosure, DoS and elevation of privilege] ATE_SVV_EXT.1.1E [The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence]	**ATE_SVV_EXT.1-1** Evaluation activities [The evaluator shall check that the test documentation includes test plans, expected test results and actual test results of threat mitigation testing] [The evaluator checks that the test documentation includes the examples of attempts to thwart mitigations identified using the spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege] [The evaluator checks the documentation if a layered defense strategy was used as a mitigation, then the evaluator checks the documentation to ensure that the product's defense in depth and threat mitigation strategies and capabilities are effective]
	SVV-3: Vulnerability testing (VUT) *(SAR_EXT component name)*	**ATE Tests**	**ATE_SVV_EXT.2 - Vulnerability testing** ATE_SVV_EXT.2.1D [The developer shall execute and document the process on identifying and characterizing potential security vulnerabilities in the product. Known vulnerability analysis and testing shall be based upon, at a minimum, recent contents of an established, industry-recognized, public source for known vulnerabilities] ATE_SVV_EXT.2.1C [The test documentation shall include the evidence of executing analysis and tests enumerated in details at points a) to e) in Practice 5, SVV-3 requirement: a) input	**ATE_SVV_EXT.2-1** Evaluation activities [The evaluator shall check that the vulnerability testing documentation includes potential security vulnerabilities and known vulnerabilities analysis results] [The evaluator checks that the vulnerability testing documentation includes the results of the following analysis and tests: a) input testing; b) attack surface analysis; c) black box known vulnerabilities scanning; d) software composition analysis; e) dynamic runtime resource management testing]

			testing; b) attack surface analysis; c) black box known vulnerabilities scanning; d) software composition analysis; e) dynamic runtime resource management testing] ATE_SVV_EXT.2.1E [The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence]	[The evaluator checks each, aforementioned in a) to e), vulnerability test according to details specified for each test in Practice 5, SVV-3 requirement whether they provide minimum necessary information to be processed further in security defect management process]
	SVV-4: Penetration testing (PNT) *(SAR_EXT component name)*	**ATE Tests**	**ATE_SVV_EXT.3 Penetration testing** ATE_SVV_EXT.3.1D [The developer shall execute and document penetration tests to proof that efforts have been taken to discover security-related issues in the product or product documentation that could allow the product to be exploited] ATE_SVV_EXT.3.1C [The penetration testing documentation shall consist of confirming that vulnerabilities discovered during vulnerability testing activity can be exploited and used to compromise security of the product] ATE_SVV_EXT.3.1E [The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence]	**ATE_SVV_EXT.3-1** Evaluation activities [The evaluator shall check that the penetration testing documentation includes tests for potential security vulnerabilities and known vulnerabilities analysis results] [The evaluator checks that the penetration testing documentation includes the results of the tests for vulnerabilities discovered during vulnerability testing evaluation activity] [The evaluator checks each penetration test results whether the penetration test exploited or not the vulnerability in question]
	SVV-5: Independence of testers	**ATE_FUN.1 [*refinement*] Functional testing**	**ATE_FUN.1.1C** [*The test documentation shall include a proof that individuals performing testing are independent from the developers who designed and implemented the IACS component*]	**ATE_FUN.1-1** Evaluation activity [*The evaluator shall check that the documentation includes a proof that tests were performed by testers who are independent from the developers of the product under test*]

	DM-1: Receiving notifications of security-related issues	**ALC_FLR.2 Systematic flaw remediation**	NA	NA
	DM-2: Reviewing security-related issues	**ALC_FLR.3 Systematic flaw remediation**	NA	NA
	DM-3: Assessing security-related issues			
	DM-4: Addressing security-related issues			
	DM-5: Disclosing security-related issues			
Practice 6 - Management of security-related issues	DM-6: Periodic review of security defect management practice	**ALC_FLR.1 [*refinement*] Basic flaw remediation**	**ALC_FLR.1.1D** [*The flaw remediation procedures and security-related issue documentation shall include the results of periodic reviews of the procedures and flaw management process*] **ALC_FLR.1.1C** [*The flaw remediation management process reviews shall include at a minimum: examination of flaws since the last periodic review to determine if the flaw management process was complete, efficient, and led to the resolution of each flaw. Periodic reviews documentation shall be created at least annually*]	**ALC_FLR.1-1** Evaluation activities [*The evaluator shall examine the flaw remediation procedures documentation to determine that it describes periodic review of the security-related issue procedures and management process*] [*The evaluator shall examine whether the periodic review examined flaws managed through the process since the last periodic review to verify if the review process was complete, efficient, and let to the resolution of the flaw*] [*The evaluator shall examine if the reviews are conducted at least annually*]

Practice 7 - Security update management (*SAR_EXT family name - SUM*)	SUM-1: Security update qualification (*SAR_EXT component name*)	**ALC Life-cycle support**	**ALC_SUM_EXT.1 - Security update qualification** ATE_SUM_EXT.1.1D [The developer shall provide documentation for security update qualification including confirmation that update is not contradicting to operational or legal constraints] ALC_SUM_EXT.1.1C [The documentation of security update qualification shall include 1) security updates created by the product developer addressing the intended security vulnerabilities; 2) the results of updates verification that they do not introduce regressions including patches created by: a) the product developer; b) suppliers of dependent components] ALC_SUM_EXT.1.1E [The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence]	**ALC_SUM_EXT.1-1** Evaluation activities [The evaluator shall check that the qualification documentation includes confirmation that updates do not contradict operational, safety or legal constraints] [The evaluator checks the qualification documentation whether there are evidence that security updates do not introduce regressions] [The evaluator checks the documentation if it includes a confirmation that patches applicable to the product are evaluated to ensure that they do not adversely affect operation of the product]
	SUM-2: Security update documentation (*SAR_EXT component name*)	**ALC Life-cycle support**	**ALC_SUM_EXT.2 - Security update documentation** ATE_SUM_EXT.2.1D [The developer shall provide the documentation for product users about the product security updates] ALC_SUM_EXT.2.1C [The documentation of security updates shall include: a) the product version, b) instructions on how to apply approved patches, c) description of any impacts the patch can have to the product, d) instruction on how to verify that an approved patch has been applied, e) risks of not applying the patch and using	**ALC_SUM_EXT.2-1** Evaluation activities [The evaluator shall check if the developer creates the documentation about updates for users of the product] [The evaluator checks the documentation whether it includes at minimum information listed in the content and presentation of evidence assurance element]

			the patch not approved by the asset owner] ALC_SUM_EXT.2.1E [The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence]	
	SUM-3: Dependent component or operating system security update documentation (*SAR_EXT component name*)	**ALC Life-cycle support**	**ALC_SUM_EXT.3 - Dependent component or operating system security update documentation** ATE_SUM_EXT.3.1D [The developer shall provide the dependent component or operating system security update documentation to product users] ALC_SUM_EXT.3.1C [The documentation of security updates for dependent component or operating system shall include: a) the statement whether the product is compatible with the dependent component or operating system security update, and b) for security updates that are unapproved by the product vendor, the mitigations that can be used in lieu of not applying the update] ALC_SUM_EXT.3.1E [The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence]	**ALC_SUM_EXT.3-1** Evaluation activities [The evaluator shall check if the developer creates the documentation about updates of dependent component or operating system for users of the product] [The evaluator checks the documentation whether it includes at minimum information listed in the content and presentation of evidence assurance element]

	SUM-4: Security update delivery (*SAR_EXT component name*)	**ALC Life-cycle support**	**ALC_SUM_EXT.4 - Security update delivery** ATE_SUM_EXT.3.1D [The developer shall provide a mechanism or technique that allows product users to verify the authenticity of patches] ALC_SUM_EXT.4.1C [The documentation of security updates delivery shall include description of a process that security updates for all supported products and product versions are made available to product users in a manner that facilitates verification that the security patch is authentic] ALC_SUM_EXT.4.1E [The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence]	**ALC_SUM_EXT.4-1** Evaluation activities [The evaluator checks the documentation whether it includes the description of updates and patches delivery to users and the way of verification of the authenticity of updates and patches]
	SUM-5: Timely delivery of security patches	**ALC Life-cycle support**	**ALC_SUM_EXT.5 - Timely delivery of security patches** ATE_SUM_EXT.3.1D [The developer shall provide a policy that specifies the timeframes for delivering and qualifying security updates to product users and to ensure that this policy is followed] ALC_SUM_EXT.5.1C [The policy for timely delivery of security patches shall consider the following factors: a) the potential impact of the vulnerability; b) public knowledge of vulnerability; c) whether published exploits exist for the vulnerability; d) the volume of deployed product that are affected, and e) the availability of an affective mitigation in lieu of the patch]	**ALC_SUM_EXT.5-1** Evaluation activities [The evaluator checks the policy documentation whether it considers factors enumerated in content and presentation evidence requirement element]

			ALC_SUM_EXT.5.1E [The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence]	
Practice 8 - Security guidelines	SG-1: Product defense in depth SG-2: Defense in depth measures expected in the environment SG-3: Security hardening guidelines	**AGD_PRE.1 [*refinement*] Preparative procedures**	**AGD_PRE.1.1D** [*The developer shall provide user documentation that describes how to integrate, configure and maintain the defense in depth strategy of the product in accordance with its product security context (operational environment as described in the ST) and the guidelines how to harden the product when installing and maintaining the product*] **AGD_PRE.1.2C** [*The documentation for the defense in depth strategy shall include measures how to harden the product during installation and keep it hardened during its lifetime of use. The documentation shall include: a) the residual threats; b) the security capabilities of the product to counter this threats; c) any compensating security controls/mitigations that can be used with the product to further protect the product; d) the security defense in depth measures expected to be provided by the external environment in which the product is to be used*] [*The guidelines for hardening the product shall include, but are not limited to, instructions, rationale and recommendations for the following information included in a) to h) options in Practice 8, SG-3 requirement*]	**AGD_PRE.1-2** Evaluation activities [*The evaluator shall examine the provided defense in depth strategy documentation to determine that it describes the steps necessary to harden the product during installation and keep it hardened during operation at the customer site*] [*The evaluator shall examine the provided documentation to determine that it describes security measures expected to be provided by the external environment in which the product is to be used in order to fulfill the defense in depth strategy*] [*The evaluator shall examine the provided hardening guidelines if it meets all requirements for content and presentation of evidence*]

	SG-4: Secure disposal guidelines	**ALC_LCD.1 [*refinement 10*] Developer defined life-cycle model**	**ALC_LCD.1.1C** [*The life-cycle definition documentation shall describe a stage for removing the product from use. The guidelines shall include: a) removing the product from its intended environment, b) recommendations for removing references and configuration data stored within environment; c) secure removal of data stored in the product, and d) secure disposal of the product to prevent potential disclosure of data contained in the product that could not be removed as described in c) above*]	ALC_LCD.1-1(10) Evaluation activity [*The evaluator shall examine the documented description of the life-cycle model used to determine that it covers the stage of secure removing the product from use*]
	SG-5: Secure operation guidelines	**AGD_OPE.1 Operational user guidance**	NA	NA
	SG-6: Account management guidelines			
	SG-7: Documentation review			

Skrócona tabela mapowania Praktyk IEC 62443-4-1 na wymagania SAR oraz jednostki oceny WU po adaptacji do wymagań przemysłowych

Tabela 37. Mapa skrócona Praktyk IEC 62443-4-1 do komponentów SAR, WUs i EAL

IEC 62443-4-1 Practices	Process requirements	CC SARs and SAR_EXT	CC adapted WU_EXT	EAL
Practice 1 - Security management	SM-1: Development process	**ALC_LCD.1**	NA	3, 4
	SM-2: Identification of responsibilities			
	SM-3: Identification of applicability			
	SM-4: Security expertise	ALC_LCD.1.1C [*refinement 1*]	ALC_LCD.1-1(1)	3, 4
	SM-5: Process scoping	ALC_LCD.1.1C [*refinement 2*]	ALC_LCD.1-1(2)	3, 4
	SM-6: File integrity	ALC_DEL.1	NA	2 - 4
	SM-7: Development environment security	ALC_DVS.1	NA	3, 4

	SM-8: Controls for private keys			
	SM-9: Security requirements for externally provided components	ALC_CMS.1.2C [*refinement*]	ALC_CMS.1-2	1 - 4
	SM-10: Custom developed components from third-party suppliers			
	SM-11: Assessing and addressing security related issues	ALC_FLR.3	NA	1 - 4
	SM-12: Process verification	ALC_LCD.1.1C [*refinement 3*]	ALC_LCD.1-1(3)	3, 4
	SM-13: Continuous improvement			
Practice 2 - Specification of security requirements	SR-1: Product security context	ALC_LCD.1.1C [*refinement 4*]	ALC_LCD.1-1(4)	3, 4
	SR-2: Threat model	ALC_LCD.1.1C [*refinement 5*]	ALC_LCD.1-1(5)	3, 4
	SR-3: Product security requirements	ALC_LCD.1.1C [*refinement 6*]	ALC_LCD.1-1(6)	3, 4
	SR-4: Product security requirements content			
	SR-5: Security requirements review			
Practice 3 - Secure by design	SD-1: Secure design principles	ADV_FSP ADV_TDS	NA	1 - 4
	SD-2: Defense in depth design	ADV_ARC.1.1D [*refinement*] ADV_ARC.1.5C [*refinement*]	ADV_ARC.1-5	2 - 4
	SD-3: Security design review	ALC_LCD.1.1C [*refinement 7*]	ALC_LCD.1-1(7)	3, 4
	SD-4: secure design best practices	ALC_LCD.1.1C [*refinement 8*]	ALC_LCD.1-1(8)	3, 4
Practice 4 - Secure implementation	SI-1: Security implementation review	ALC_LCD.1.1C [*refinement 9*]	ALC_LCD.1-1(9)	3, 4
	SI-2: Secure coding standards	ALC_TAT.1.1C [*refinement*]	ALC_TAT.1-1	4
Practice 5 - Security verification and validation testing	SVV-1: Security requirements testing	ATE_FUN.1.2C [*refinement*] ATE_IND.1.2E [*refinement*]	ATE_FUN.1-2 ATE_IND.1-3	2 - 4 1 - 4
	SVV-2: Threat mitigation testing	ATE_SVV_EXT.1	ATE_SVV_EXT.1-1	1 - 4
	SVV-3: Vulnerability testing	ATE_SVV_EXT.2	ATE_SVV_EXT.2-1	1 - 4
	SVV-4: Penetration testing	ATE_SVV_EXT.3	ATE_SVV_EXT.3-1	1 - 4
	SVV-5: Independence of testers	ATE_FUN.1.1C [*refinement*]	ATE_FUN.1-1	2 - 4

Practice 6 - Management of security-related issues	DM-1: Receiving notifications of security-related issues	ALC_FLR.2	NA	1 - 4
	DM-2: Reviewing security-related issues	ALC_FLR.3	NA	1 - 4
	DM-3: Assessing security-related issues			
	DM-4: Addressing security-related issues			
	DM-5: Disclosing security-related issues			
	DM-6: Periodic review of security defect management practice	ALC_FLR.1.1D [*refinement*] ALC_FLR.1.1C [*refinement*]	ALC_FLR.1-1	1 - 4
Practice 7 - Security update management	SUM-1: Security update qualification	ALC_SUM_EXT.1	ALC_SUM_EXT.1-1	1 - 4
	SUM-2: Security update documentation	ALC_SUM_EXT.2	ALC_SUM_EXT.2-1	1 - 4
	SUM-3: Dependent component or operating system security update documentation	ALC_SUM_EXT.3	ALC_SUM_EXT.3-1	1 - 4
	SUM-4: Security update delivery	ALC_SUM_EXT.4	ALC_SUM_EXT.4-1	1 - 4
	SUM-5: Timely delivery of security patches	ALC_SUM_EXT.5	ALC_SUM_EXT.5-1	1 - 4
Practice 8 - Security guidelines	SG-1: Product defense in depth	AGD_PRE.1.1D [*refinement*] AGD_PRE.1.1C [*refinement*]	AGD_PRE.1-2	1 - 4
	SG-2: Defense in depth measures expected in the environment			
	SG-3: Security hardening guidelines			
	SG-4: Secure disposal guidelines	ALC_LCD.1.1C [*refinement 10*]	ALC_LCD.1-1(10)	3, 4
	SG-5: Secure operation guidelines	AGD_OPE.1	NA	1 - 4
	SG-6: Account management guidelines			
	SG-7: Documentation review			

Tabela 38. Mapa skrócona komponentów SAR, WUs i EAL do Praktyk IEC 62443-4-1

CC Class	CC SAR [refinement]/ EXT	CC WU_EXT	EAL	IEC 62443-4-1
AGD	AGD_PRE.1.1D [*refinement*] AGD_PRE.1.1C [*refinement*]	AGD_PRE.1-2	1 - 4	P8 SG-1, 2, 3
ADV	ADV_ARC.1.1D [*refinement*] ADV_ARC.1.5C [*refinement*]	ADV_ARC.1-5	2 - 4	P3 SD-2
ALC	ALC_FLR.1.1D [*refinement*] ALC_FLR.1.1C [*refinement*]	ALC_FLR.1-1	1 - 4	P6 DM-6
	ALC_TAT.1.1C [*refinement*]	ALC_TAT.1-1	4	P4 SI-2
	ALC_CMS.1.2C [*refinement*]	ALC_CMS.1-2	1 - 4	P1 SM-9, 10
	ALC_LCD.1.1C [*refinement 1*]	ALC_LCD.1-1(1)	3, 4	P1 SM-4
	ALC_LCD.1.1C [*refinement 2*]	ALC_LCD.1-1(2)	3, 4	P1 SM-5
	ALC_LCD.1.1C [*refinement 3*]	ALC_LCD.1-1(3)	3, 4	P1 SM-12, 13
	ALC_LCD.1.1C [*refinement 4*]	ALC_LCD.1-1(4)	3, 4	P2 SR-1
	ALC_LCD.1.1C [*refinement 5*]	ALC_LCD.1-1(5)	3, 4	P2 SR-2
	ALC_LCD.1.1C [*refinement 6*]	ALC_LCD.1-1(6)	3, 4	P2 SR-3, 4, 5
	ALC_LCD.1.1C [*refinement 7*]	ALC_LCD.1-1(7)	3, 4	P3 SD-3
	ALC_LCD.1.1C [*refinement 8*]	ALC_LCD.1-1(8)	3, 4	P3 SD-4
	ALC_LCD.1.1C [*refinement 9*]	ALC_LCD.1-1(9)	3, 4	P4 SI-1
	ALC_LCD.1.1C [*refinement 10*]	ALC_LCD.1-1(10)	3, 4	P8 SG-4
	ALC_SUM_EXT.1	ALC_SUM_EXT.1-1	1 - 4	P7 SUM-1
	ALC_SUM_EXT.2	ALC_SUM_EXT.2-1	1 - 4	P7 SUM-2
	ALC_SUM_EXT.3	ALC_SUM_EXT.3-1	1 - 4	P7 SUM-3
	ALC_SUM_EXT.4	ALC_SUM_EXT.4-1	1 - 4	P7 SUM-4
	ALC_SUM_EXT.5	ALC_SUM_EXT.5-1	1 - 4	P7 SUM-5
ATE	ATE_FUN.1.1C [*refinement*]	ATE_FUN.1-1	2 - 4	P5 SVV-5
	ATE_FUN.1.2C [*refinement*]	ATE_FUN.1-2	2 - 4	P5 SVV-1
	ATE_IND.1.2E [*refinement*]	ATE_IND.1-3	1 - 4	P5 SVV-1
	ATE_SVV_EXT.1	ATE_SVV_EXT.1-1	1 - 4	P5 SVV-2
	ATE_SVV_EXT.2	ATE_SVV_EXT.2-1	1 - 4	P5 SVV-3
	ATE_SVV_EXT.3	ATE_SVV_EXT.3-1	1 - 4	P5 SVV-4

Tabela 39. Mapowanie i adaptacja wymagań SFR do IEC 62443-4-2 (SL 1)

IEC 62443-4-2 Foundational Requirements (FRs)	**IEC Component**	**CC SFR class, family, component**	**CC adapted SFR/ [*refinement*]/ [assignment]/EXT**	**CC Evaluation activities (EAs)**
FR 1 - Identification and authentication control (IAC)	Requirement Enhancements (REs) = (#)	SFRs from CC p.2 or SFR_EXT	Requirement Refinements (RRs) = (#)	EAs for collaborative Protection Profile (cPP)
Human user identification and authentication	CR1.1	**FIA - Identification and authentication** FIA_UAU.5 - User authentication Multiple authentication mechanisms FIA_UID.1 - User identification Timing identification FIA_UID.2 - User identification User identification before any action	All applicable operations	Evaluation activities: CR1.1 test plan in the pilot evaluation report
Software process and device identification and authentication	CR1.2 REs: (1) Security Level: CR1.2 - SL2 CR1.2(1) - SL3, SL4	**FFR - Function Foundational Requirement** **FFR_IAC_EXT.1** Software process and device identification and authentication	FFR_IAC_EXT.1.1 = CR1.2 RRs: (1) EAL level: FFR_IAC_EXT.1.1 - EAL1-3 (SL2) FFR_IAC_EXT.1.1(1) - EAL4 (SL3, SL4)	Evaluation activities: 1) All entities shall be identified and authenticated for all access to the control system 2) Tests shall verify methods such as passwords, tokens, or location (physical or logical)
Account management	CR1.3	**FMT - Security management** FMT_SMF.1 Specification of Management Functions	FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*assignment: list of management functions to be provided by the TSF*]	Evaluation activities: CR1.3 test plan in the pilot evaluation report

			assignment: account management	
Authenticator management	CR1.5	**FMT - Security management** **FMT_MSA** Management of security attributes	All applicable operations	Evaluation activities: CR1.5 test plan in the pilot evaluation report
Strength of password-based authentication	CR1.7	**FIA - Identification and authentication** **FIA_SOS** Specification of secrets	All applicable operations	Evaluation activities: CR1.7 test plan in the pilot evaluation report Requirements for mechanisms that enforce defined quality metrics on provided secrets and generate secrets to satisfy the defined metric
Unsuccessful login attempts	CR1.11	FMT_REV.1 - Revocation **FIA_AFL - Authentication failures** FMT_SAE.1 Time-limited authorization FIA_UAU.1 Timing of authentication	All applicable operations	Evaluation activities: CR1.11 test plan in the pilot evaluation report
FR 2 - Use control				
Authorization enforcement	CR2.1	**FIA_UAU - User authentication**	All applicable operations	Evaluation activities: CR2.1 test plan in the pilot evaluation report
Session lock	CR2.5	**FTA - TOE access** **FTA_SSL - Session locking and termination** FTA_SSL.1 TSF-initiated session locking FTA_SSL.2 User-initiated locking FTA_SSL.3 TSF-	FTA_SSL.1.1 The TSF shall lock an interactive session after [*assignment: time interval of user inactivity*] *Assignment operations:* - time interval of user inactivity	Evaluation activities: CR2.5 test plan in the pilot evaluation report

		initiated termination FTA_SSL.4 User-initiated termination	FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [*assignment: events to occur*] *Assignment operations*: - events to occur prior to unlocking	
Auditable events	CR2.8	**FAU - Security audit** FAU_SEL - Security audit event selection FAU_GEN.1 - Audit data generation	FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events: c) [*assignment*: *other specifically defined auditable events*] *Assignment of events*: a) access control, b) request errors, c) control system events; d) backup and restore event, e) configuration changes, and f) audit log events	Evaluation activities: CR2.8 test plan in the pilot evaluation report
Audit storage capacity	CR2.9	**FRU - Resource utilization** FRU_RSA - Resource allocation FAU_STG - Security audit event storage	All applicable operations	Evaluation activities: CR2.9 test plan in the pilot evaluation report
FR 3 - System integrity				
Communication integrity	CR3.1	**FPT - Protection of the TSF** FPT_ITI - Integrity of exported TSF data **FTP - Trusted path/channels** FTP_ITC.1 Inter-TSF trusted channel	All applicable operations	Evaluation activities: CR3.1 test plan in the pilot evaluation report
Security functionality verification	CR3.3	**FPT - Protection of the TSF** FPT_TEE - Testing	All applicable operations	Evaluation activities: CR3.3 test plan in

		of external entities FPT_TST - TSF self-test		the pilot evaluation report
Error handling	CR3.7	**FFR - Function Foundational Requirement** **SI - System integrity** FFR_SI_EXT.1 - Error handling	FFR_SI_EXT.1.1 = CR3.7 EAL level: FFR_SI_EXT.1.1 - no EAL	Evaluation activities: CR3.7 test plan, and: 1) verification whether IACS device handles error conditions in a manner that does not provide information that could be exploited by adversaries to attack the IACS device.
FR 4 - Data confidentiality				
Information confidentiality	CR4.1	**FDP - User data protection** FDP_UCT - Inter-TSF data confidentiality transfer protection FDP-ITT Internal TOE transfer **FPT - Protection of the TSF** FPT_ITC - Confidentiality of exported TSF data	All applicable operations	Evaluation activities: CR4.1 test plan in the pilot evaluation report
Use of cryptography	CR4.3	**FCS - Cryptographic support** FCS_CKM - Cryptographic key management FCS_COP - Cryptographic operation	All applicable operations	Evaluation activities: CR4.3 test plan in the pilot evaluation report
FR 5 - Restricted data flow				
Network segmentation	CR5.1	**FTP - Trusted path/channels** FTP_ITC - Inter TSF trusted channel	All applicable operations	Evaluation activities: CR5.1 test plan in the pilot evaluation report

		FTP_TRP - Trusted path		
FR 6 - Timely response to events				
Audit log accessibility	CR6.1	**FAU - Security audit** FAU_SAR - Security audit review FAU_SAA - Security audit analysis	All applicable operations	Evaluation activities: CR6.1 test plan in the pilot evaluation report
FR 7 - Resource availability				
Denial of service protection	CR7.1	**FRU – Resource utilization** FRU_RSA - Resource allocation	All applicable operations	Evaluation activities: CR7.1 test plan in the pilot evaluation report
Control system backup	CR7.3	**FMT - Security management** FMT_SMF - Specification of Management Functions	All applicable operations	Evaluation activities: CR7.3 test plan in the pilot evaluation report
Network and security configuration settings	CR7.6	**FFR - Function Foundational Requirement** RA **- Resource availability** FFR_RA_EXT.1 - Network and security configuration setting	FFR_SI_EXT.1.1 = CR7.6 EAL level: FFR_SI_EXT.1.1 - no EAL	Evaluation activities: CR7.6 test plan, and: 1) verification whether IACS component can be configured according to recommended network and security configurations as demanded by the control system supplier; 2) verification if the IACS component provides an interface to the currently deployed network and its security settings.

Załącznik 2. Sprawozdanie z pilotażowej oceny bezpieczeństwa

Wersja skrócona do wyników badań wybranych komponentów FR 1(IAC), poziom SL 1

Łukasiewicz
Instytut Technik
Innowacyjnych
EMAG

Wersja skrócona sprawozdania do celów rozprawy doktorskiej

Centrum Badań i Certyfikacji
Zespół Laboratoriów Badawczych
www.cbc.ibemag.pl, e-mail: cbc@emag.lukasiewicz.gov.pl, tel. 32 2007 512

LABORATORIUM
Oceny Bezpieczeństwa Produktów Teleinformatycznych ITSEF - EMAG

SPRAWOZDANIE Z BADAŃ Nr **1/ ITSEF/ 2022**

(Przeznaczone dla Jednostki Certyfikującej Wyroby)

Terminal zabezpieczeniowy [redacted] w konfiguracji zabezpieczenia odległościowego [redacted], nr seryjny [redacted]
wg normy PN-EN IEC 62443-4-2, poziom SL 1

Zamawiający:
Zakład [redacted] Sp. z o.o. ([redacted])
w [redacted]

Zlecenie: Nr [redacted] z dnia [redacted] - Dotyczy pilotażowego badania zgodności zabezpieczenia [redacted] wg normy PN-EN IEC 62443-4-2

Sprawozdanie opracował: P[redacted]l (Ewaluator)

Sprawozdanie sprawdził: J[redacted]i (Ewaluator)

Sprawozdanie autoryzował:
Dariusz Rogowski (Kierownik ITSEF)

Sprawozdanie zawiera stron:	26	Wersja wzoru M-005/3 w. 1	Egzemplarz nr	1

Spis treści

SPIS RYSUNKÓW

Spis rysunków

1 Przedmiot badań

(zawiera nazwę, charakterystykę, identyfikację obiektu badań oraz informację odnośnie pochodzenia/sposobu pobrania próbek jeśli dotyczy)

Zakład [redacted] Sp. z o.o. w [redacted] [1] przekazał do badań pilotażowych w laboratorium ITSEF Łukasiewicz – EMAG terminal zabezpieczeniowy [redacted] w konfiguracji zabezpieczenia odległościowego [redacted] [2] i wyposażony w moduł komunikacyjny [redacted]3] w wersji [redacted] [4].

Zgodnie z instrukcją producenta „terminal [redacted] pełni funkcje zabezpieczeń pola stacji elektroenergetycznej, a jego elastyczność umożliwia stosowanie go jako szereg różnych zabezpieczeń, a także jako sterownika polowego, który realizuje pomiary i sterowania w polach rozdzielni elektroenergetycznych" [2]. Przekazany do badań terminal został skonfigurowany sprzętowo z włączonymi funkcjami programu zabezpieczenia odległościowego, w skrócie nazywany jako zabezpieczenie odległościowe [redacted].

2 Zakres badań

(zawiera zakres oraz identyfikację zastosowanych metod badań wraz z informacją o posiadanej akredytacji i podwykonawstwie)

PN-EN IEC 62443-4-2:2019-08, Security Level 1 (SL 1), M-005, w. 1

Uwaga
Niektóre wymagania mogą zostać wyłączone z zakresu badań w zależności od typu urządzenia i kontekstu jego użycia, co będzie zaznaczone w sprawozdaniu z badań.

Uwaga 2
W przypadku problemów w interpretacji wymagań zawartych w Planie badań, pierwszeństwo mają definicje wymagań pochodzące z wersji angielskiej normy PN-EN IEC 62443-4-2:2019-08.

3 Opis badań

(zawiera sposób i warunki wykonania badań, stosowane wyposażenie, itp.)

Opis skrótów werdyktów:

P – Pozytywny wynik badań
N – Negatywny wynik badań
N. d. – Nie dotyczy badanego produktu

4 Podsumowanie wyników badań

4.1 Lista wymagań fundamentalnych

a) FR 1 – Identyfikacja i kontrola autoryzacji (Identification and Authentication Control, IAC)
b) FR 2 – Kontrola użycia (Use Control, UC)
c) FR 3 – Integralność systemu (System Integrity, SI)
d) FR 4 – Poufność danych (Data Confidentiality, DC)
e) FR 5 – Ograniczenie przepływu danych (Restricted Data Flow, RDF)
f) FR 6 – Czasowa odpowiedź na zdarzenia (Timely Response to Events, TRE)
g) FR 7 – Dostępność zasobów (Resource Availability, RA)

4.2 Podsumowanie werdyktów

Wymaganie fundamentalne	Wymaganie	Werdykt
FR 1		**N**
	CR 1.1	P
	CR 1.3	P
	CR 1.4	P
	CR 1.5	N
	NDR 1.6	N.d.
	CR 1.7	P
	CR 1.10	P
	CR 1.11	P
	CR 1.12	N
	NDR 1.13	N.d.
FR 2		**P**
	CR 2.1	P
	CR 2.2	N.d.
	SAR 2.4	N.d.
	EDR 2.4	N.d.
	HDR 2.4	N.d.
	NDR 2.4	N.d.
	CR 2.5	P
	CR 2.8	P
	CR 2.9	P
	CR 2.10	P
	CR 2.11	P
	CR 2.12	P
FR 3		**N**
	CR 3.1	P
	SAR 3.2	N.d.
	EDR 3.2	P

	HDR 3.2	N.d..
	NDR 3.2	N.d.
	CR 3.3	N
	CR 3.4	N
	CR 3.5	P
	CR 3.6	P
	CR 3.7	P
	EDR 3.10	P
	HDR 3.10	N.d.
	NDR 3.10	N.d.
	EDR 3.14	N
	HDR 3.14	N.d.
	NDR 3.14	N.d.
FR 4		**N**
	CR 4.1	N
	CR 4.3	P
FR 5		**P**
	CR 5.1	P
	NDR 5.2	N.d.
	NDR 5.3	N.d.
FR 6		**P**
	CR 6.1	P
FR 7		**N**
	CR 7.1	N
	CR 7.2	P
	CR 7.3	P
	CR 7.4	P
	CR 7.6	P
	CR 7.7	P

5 Badania dla FR 1

Wymaganie fundamentalne	Wymaganie	Werdykt
FR 1		N
	CR 1.1	P
	CR 1.3	P
	CR 1.4	P
	CR 1.5	N
	NDR 1.6	N.d.
	CR 1.7	P
	CR 1.10	P
	CR 1.11	P
	CR 1.12	N
	NDR 1.13	N.d.

5.1 CR 1.1

CR 1.1
Oceniający powinien sprawdzić, czy z wszystkich dostępnych interfejsów (zarówno fizycznych użytkownika, jak i komunikacyjnych), z których mogą korzystać użytkownicy (człowiek):

- Zapewniona jest możliwość identyfikacji i autoryzacji użytkowników,
- Identyfikacja i autoryzacja są wymuszane przed uzyskaniem dostępu do funkcjonalności,
- Identyfikacja i autoryzacja wspierają, zgodnie z przyjętymi dla produktu politykami bezpieczeństwa, możliwość stosowania podziału ról i uprawnień,
- Identyfikacja i autoryzacja nie utrudniają podjęcia działań w sytuacjach awaryjnych.

Uwagi:

- Zakres oceny obejmuje tylko interfejsy, z których mogą korzystać użytkownicy – ludzie, a nie dotyczy interfejsów przeznaczonych dla innych systemów, podsystemów i komponentów.

Warunki akceptacji
Zapewniona i wymuszona możliwość identyfikacji i autoryzacji użytkowników na wszystkich dostępnych dla użytkownika interfejsach (fizycznych i komunikacyjnych, itd.) potwierdzona wynikami testów lub uzasadnieniem na podstawie analizy dokumentacji.

Potwierdzone wynikami testów lub uzasadnieniem na podstawie analizy dokumentacji, że w żadnym z założonych scenariuszy awarii działanie procesu identyfikacji i autoryzacji urządzenia nie zostanie zakłócone w taki sposób, aby niemożliwe było podjęcie działań przynajmniej w stopniu podstawowym, niezbędnym w przypadku awarii.

Ewaluator(rzy)	[redacted]
Data	[redacted]
Werdykt	P

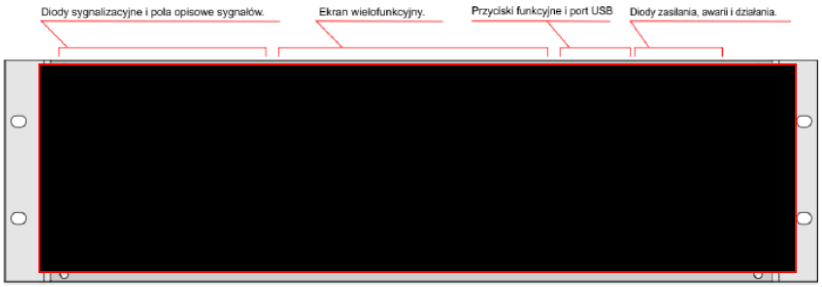
Plan testów:

1) Identyfikacja dostępnych interfejsów dostępnych dla użytkowników.
2) Sprawdzenie dla zidentyfikowanych interfejsów czy:
   a) jest wymuszana autoryzacja użytkowników przed uzyskaniem przez nich dostępu do funkcjonalności
   b) jest zaimplementowana możliwość przydziału użytkownikom ról i uprawnień
3) Opracowanie listy scenariuszy możliwych awarii urządzenia lub jego otoczenia, które mogą mieć wpływ na przeprowadzenie przez użytkownika procesu identyfikacji i autoryzacji użytkowników
4) Ocena dla wszystkich opracowanych scenariuszy, czy w przypadku zaistnienia sytuacji awaryjnej nie będzie ona miała wpływu na możliwość podjęcia podstawowych działań na urządzeniu.

Wykonane badania:

1) Identyfikacja dostępnych interfejsów dostępnych dla użytkowników.

Widok panelu czołowego [7] Rozdział 4.2:



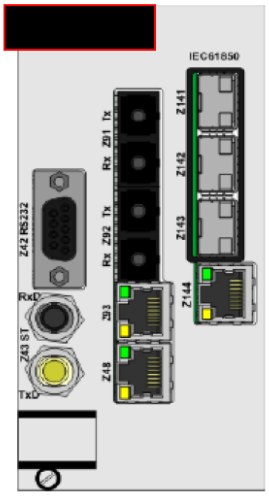
Rysunek 1 Panel czołowy urządzenia

Zidentyfikowane elementy panelu dostępne dla użytkowników:

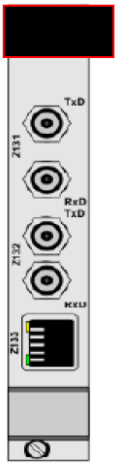
- Ekran dotykowy i przyciski (interfejs użytkownika)
- Port USB

Moduł komunikacyjny [redacted] + [redacted]:

Złącza interfejsu komunikacyjnego: (Na podstawie [4] Rozdział 1):



Rysunek 2 Panel złącz modułu M



Rysunek 3 Panel złącz modułu M12

Opis przeznaczenia poszczególnych złączy interfejsu komunikacyjnego (Rozdział 1 [4]):

Tabela 1 Wykaz interfejsów modułu M/S

Port	Łącze	Typ gniazda	Protokół	
Z42	RS232	D89 F	IEC 870-5-103 / [redacted]	
Z43	Szeregowe optyczne	ST	IEC 870-5-103 / [redacted]	
Z48	Ethernet / elektryczne	RJ45	[redacted]/NTP	
Z91	Ethernet / optyczne	SC	[redacted]/NTP	Wspólne IP
Z92	Ethernet / optyczne	SC	[redacted]/NTP	

Z93	Ethernet / elektryczne	RJ45	[redacted]/NTP	
Z141	Ethernet / optyczne	LC	IEC 61850/NTP	Wspólne IP
Z142	Ethernet / optyczne	LC	IEC 61850/NTP	
Z143	Ethernet / optyczne	LC	IEC 61850/NTP	
Z144	Ethernet / elektryczne	RJ45	IEC 61850/NTP	

Tabela 2 Wykaz interfejsów modułu M2

Port	Łącze	Typ gniazda	Protokół	
Z131	Szeregowe optyczne	ST	- nieczynne -	
Z132	Ethernet / optyczne	ST	[redacted]	Wspólne IP
Z133	Ethernet / elektryczne	RJ45	[redacted]	

Tabela 3 Zestawienie przeznaczenia i parametrów wszystkich dostępnych złącz komunikacyjnych

Port	Standard	Typ gniazda	Protokół warstwy L3	Protokół warstwy L4	Protokół warstwy L7
Z42	RS232	D89 F	-	-	-
Z43	Szeregowe optyczne	ST	-	-	-
Z48	Ethernet 100BASE-TX	RJ45	IP, ICMP	TCP	[redacted]* (port 4444)
Z91	Ethernet 100BASE-TX 1300nm	SC	IP, ICMP	TCP	[redacted]* (port 4444)
Z92	Ethernet 100BASE-TX 1300nm	SC	IP, ICMP	TCP	[redacted]* (port 4444)
Z93	Ethernet 100BASE-TX	RJ45	IP, ICMP	TCP	[redacted]* (port 4444)
Z141	Ethernet 100BASE-TX 1310nm	LC	IP, ICMP	TCP	IEC61850 MMS/GOOSE (port 102) [redacted]* (port 4444)
Z142	Ethernet 100BASE-TX 1310nm	LC	IP, ICMP	TCP	IEC61850 MMS/GOOSE (port 102) [redacted]* (port 4444)
Z143	Ethernet 100BASE-TX	LC	IP, ICMP	TCP	IEC61850 MMS/GOOSE (port 102) [redacted]* (port 4444)
Z144	Ethernet 100BASE-TX	RJ45	IP, ICMP	TCP	IEC61850 MMS (port 102) [redacted]* (port 4444)
Z131	Szeregowe optyczne	ST	-	-	-
Z132	Ethernet 100BASE-FX	ST	IP, ICMP	TCP	[redacted]* (port 4444)
Z133	Ethernet / elektryczne wewn. komunikacja	RJ45	-	-	-

Interfejsy korzystające z protokołów IEC 60870-5-103 oraz I-4 IEC 61850 przeznaczone są tylko do komunikacji pomiędzy komponentami systemu oraz innymi systemami i nie są wykorzystywany przez użytkowników, tak więc nie podlegają ocenie.
Zidentyfikowane interfejsy, które umożliwiają interakcję użytkownika z urządzeniem:

- panel użytkownika (ekran dotykowy, przyciski fizyczne)
- interesy komunikacyjne korzystające z protokołu [redacted] z wykorzystaniem aplikacji narzędzia „[redacted] Explorer”

2) Sprawdzenie dla zidentyfikowanych interfejsów czy:

a) jest wymuszana autoryzacja użytkowników przed uzyskaniem przez nich dostępu do funkcjonalności

Panel użytkownika:

Dostęp do funkcjonalności panelu użytkownika możliwy jest po wprowadzeniu kodu PIN.

Rysunek 4 Ekran wprowadzania kodu PIN

[7] Rozdział 9.5.:

„Pin" – sześciocyfrowy kod pin uniemożliwiający czynności rekonfiguracji urządzenia osobom niepowołanym. Funkcję można wyłączyć ustawiając kod pin na wartość „000000"'.

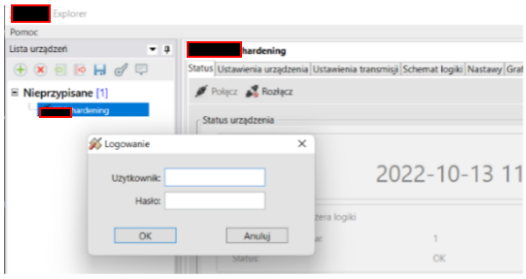
Protokół [redacted] (za pomocą aplikacji „Explorer"):

Dla przyjętego poziomu SL-1 można przyjąć, że użytkownicy z tego interfejsu będą korzystali tylko z w/w narzędzia, gdyż każdy inny sposób jego wykorzystania wymaga zaawansowanej wiedzy oraz dodatkowych specjalistycznych narzędzi wykraczających poza poziom SL-1.

[7] Rozdział 9.1:

„Przy pomocy przycisku „Logowanie do wybranego urządzenia" można przełączyć zalogowanego podczas nawiązywania połączenia użytkownika. Po naciśnięciu przycisku należy wprowadzić nową nazwę użytkownika i hasło. Po poprawnym zalogowaniu poziom uprawnień zostanie przełączony do poziomu przypisanemu przez administratora wprowadzonej nazwie użytkownika. Nieudana próba logowania spowoduje zakończenie sesji i zmianę poziomu uprawnień na podstawowy."

Po połączniu z urządzeniem za pomocą aplikacji pojawia się monit logowania:



Rysunek 5 Monit logowania w aplikacji Explorer

Użytkownik niezalogowany może tylko odczytać podstawowe informacje o urządzeniu (takie jak identyfikator urządzenia, czas) i nie ma możliwości podjęcia jakichkolwiek działań.

b) jest zaimplementowana możliwość przydziału użytkownikom ról i uprawnień.

Panel użytkownika:
Panel użytkownika nie umożliwia zarządzania konfiguracją użytkowników.
Istnieje możliwość zmiany kodu PIN.
Kod PIN daje pełen dostęp do funkcjonalności panelu użytkownika bez możliwości konfiguracji uprawnień.
Z poziomu panelu nie ma dostępu do pełnej funkcjonalności systemu.

Protokół [redacted] (za pomocą aplikacji „Explorer”):
[7] Rozdział 9.1:

„Każdemu użytkownikowi przypisany jest jeden z pięciu poziomów uprawnień, które opisano poniżej.
Poziom uprawnień podstawowy pozwala na:

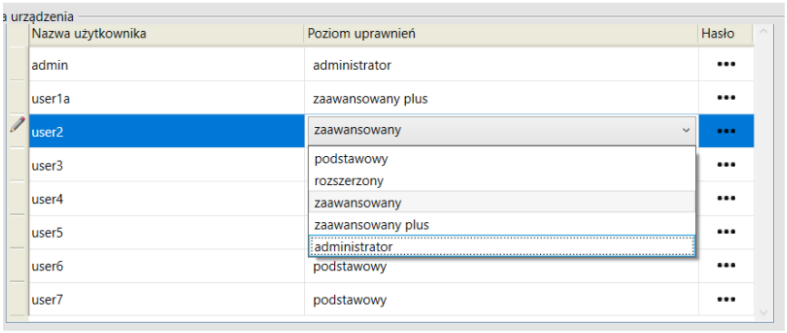
- *pogląd statusu urządzenia (stanów wejść binarnych, wirtualnych i analogowych, wyjść przekaźnikowych, pomiarów),*
- *podgląd schematu logiki, nastaw, synoptyki wyświetlacza,*
- *pogląd rejestratora zdarzeń oraz zakłóceń,*
- *pogląd konfiguracji SSiN.*

Poziom uprawnień rozszerzony dodatkowo pozwala na:

- *zmianę nastaw,*
- *sterowanie wejściami wirtualnymi (testowanie, blokowanie itp.),*
- *kasowanie sygnalizacji,*
- *zmianę nastaw transmisji,*
- *testowanie urządzenia np. test wejść, test wyjść, test logiki,*
- *edycję grafiki wyświetlacza,*
- *modyfikację konfiguracji SSiN.*

Poziom uprawnień zaawansowany dodatkowo pozwala na wykonywanie zmian w schemacie logicznym.
Uzupełniniem do powyższego poziomu uprawnień jest poziom uprawnień zaawansowany plus, który dodatkowo pozwala na wykonywanie zmian w nastawach serwisowych bloczków, które dla uprzednio wymienionych poziomów uprawnień są ukryte.

Najwyższym poziomem jest poziom uprawnień administrator, który daje możliwość zarządzania użytkownikami, ich hasłami oraz poziomami uprawnień (rolami). Pozwala on również na dostęp do sekcji „Log bezpieczeństwa" opisanej w podrozdziale 9.4.11."



Rysunek 6 Wybór poziomu uprawnień (roli) użytkownika urządzenia (aplikacja)

3) Opracowanie listy scenariuszy możliwych awarii urządzenia lub jego otoczenia, które mogą mieć wpływ na przeprowadzenie przez użytkownika procesu identyfikacji i autoryzacji użytkowników.

Urządzenie posiada rozbudowane możliwości komunikacyjne z tego powodu proponuje się rozpatrzenie następujących zwianych z tym scenariuszy awarii:

- Brak komunikacji sieciowej (na dowolnym interfejsie komunikacyjnym)

4) Ocena dla wszystkich scenariuszy, czy w przypadku zaistnienia sytuacji awaryjnej nie będzie ona miała wpływu na możliwość podjęcia działań na urządzeniu.

Scenariusz: Brak komunikacji sieciowej
Analiza skutków:
Efekt awarii: Dostęp do urządzenia możliwy jest tylko z wykorzystaniem panelu użytkownika.

Potencjalne skutki dla użytkowników zdalnych:

- Całkowity brak możliwości zdalnej komunikacji i z urządzeniem (podglądu stanu i podjęcia działań)

Potencjalne skutki dla użytkowników lokalnych:

- Brak – skutki w żadne sposób nie wpływają na możliwość interakcji użytkownika z urządzeniem, dostęp realizowany jest jak w przypadku braku awarii z wykorzystaniem kodu PIN (zapisanego w konfiguracji urządzenia)

Urządzenie posiada wewnętrzny mechanizm autoryzacji (nie wykorzystuje zewnętrznych systemów) i dzięki temu nie jest zależne od komunikacji sieciowej. Tym samym bez względu na stan komunikacji sieciowej możliwy jest:

- nieograniczony dostęp do urządzenia za pomocą panelu użytkownika,
- nieograniczony dostęp do urządzenia za pomocą aplikacji z wykorzystaniem portu USB na przednim panelu urządzenia.

Wyniki badań:

Werdykt: Pozytywny (P)

Uzasadnienie:

- Możliwość podjęcia działań przez użytkowania z wykorzystaniem panelu urządzenia wymaga autoryzacji za pomocą kodu PIN. Niezalogowany użytkownik ma możliwość tylko odczytu parametrów urządzenia (Pozytywny)
- Dostęp do urządzenia za pomocą protokołu [redacted] i aplikacji „[redacted] Explorer") wymaga autoryzacji za pomocą nazwy użytkownika i hasła. Użytkownik niezalogowany może tylko odczytać podstawowe informacje o rządzeniu. (Pozytywny)
- System umożliwia przydział użytkownikom ról z różnymi poziomami uprawnieniami (Pozytywny)
- System nie pozwala na zmianę uprawnień użytkownika korzystającego z panelu użytkownika, ale można użytkownika korzystającego z panelu traktować jako jedną z ról dostępu do systemu, gdyż nie jest to jedyny możliwy sposób interakcji użytkowników z urządzeniem (Pozytywny)
- Awaria komunikacji w żaden sposób nie wpływa na możliwość interakcji użytkownika z urządzeniem z wykorzystaniem panelu użytkownika. (Pozytywny)
- Awaria komunikacji w żaden sposób nie wpływa na możliwość interakcji użytkownika z urządzeniem z wykorzystaniem portu USB i aplikacji. (Pozytywny)
- Dostęp z wykorzystaniem kodu pin (6 cyfr) umożliwia bardzo szybkie zalogowanie się od systemu i podjęcie działań awaryjnych. (Pozytywny)

Obserwacje (jeśli N)

5.2 CR 1.3

CR 1.3
Oceniający powinien sprawdzić, czy:

- Jest zapewniona możliwość zarządzania wszystkimi kontami użytkowników,

A gdy komponent jest zintegrowany z wysokopoziomowym systemem, np. zewnętrzny system LDAP lub Active Directory, oceniający powinien sprawdzić dodatkowo, czy:

- Uwzględniono sytuację niedostępności tego systemu (np. w przypadku awarii komunikacji)

Uwagi:

- W przypadku, gdy system posiada tylko jednego użytkownika wymaganie to może sprowadzać się tylko do zapewnienia możliwości zmiany hasła.
- Istotna w ocenie jest możliwość odebrania uprawnienia użytkownikowi np. poprzez jego usunięcie, blokadę lub zmianę hasła.
- Ze względów rozliczalności system może nie posiadać możliwości usuwania kont, ale w takim przypadku musi być możliwość zablokowania lub dezaktywacji konta.

Warunki akceptacji
Zapewnienie możliwości odebrania dostępu użytkownikowi (zablokowanie lub usunięcie konta)

Wsparcie możliwości zarządzania użytkownikami: dodawanie, aktywacja, modyfikacja, blokowanie i usuwanie.

Zapewnienie możliwości zarządzania użytkownikami także w sytuacji niedostępności wysokopoziomowego systemu zarzadzania (jeśli jest wykorzystywany). Zapewnienie możliwości nadania i odebrania dostępu użytkownikowi (zablokowanie lub usunięcie konta) w sytuacji niedostępności systemu wysokopoziomowego.	
Ewaluator(rzy)	[redacted]
Data	[redacted]
Werdykt	P

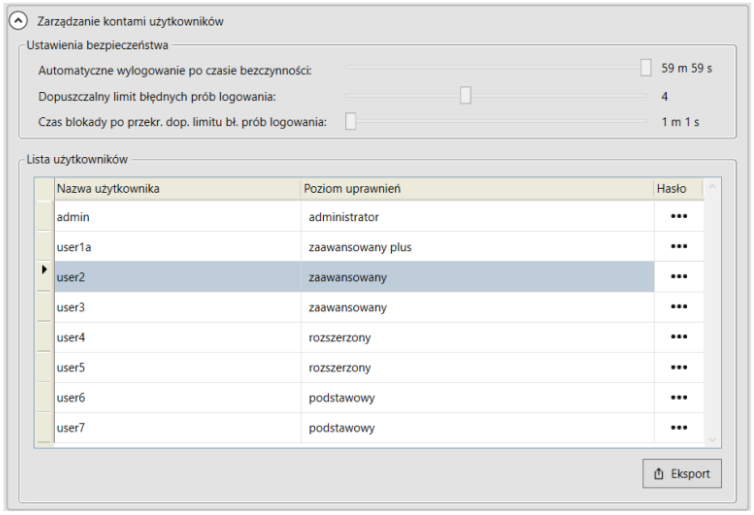
Plan testów:

1) Sprawdzenie funkcjonalności związanej z zarządzaniem użytkownikami ze szczególnym uwzględnieniem możliwości odebrania uprawnień.
2) Identyfikacja wykorzystywanych wysokopoziomowych systemów identyfikacji i autoryzacji.
3) Weryfikacja możliwości korzystania z urządzenia w przypadku niedostępności systemu wysokopoziomowego.

Wykonane badania:

1) Sprawdzenie funkcjonalności związanej z zarządzaniem użytkownikami ze szczególnym uwzględnieniem możliwości odebrania uprawnień.

Zarządzanie użytkownikami możliwe jest tylko z poziomu aplikacji „[redacted] Explorer" [7] Rozdział. 9.2 i 9.5.7.



Rysunek 7 Panel zarządzania użytkownikami

System posiada 8 (ośmiu) predefiniowanych użytkowników, a dla nich możliwe do wykonania są następujące operacje:

- Zmiana nazwy użytkownika
- Zmiana poziomu uprawnień użytkownika
- Zmian hasła użytkownika

Nazwa użytkownika musi być unikalna.
Nie ma możliwości dodania dodatkowych użytkowników.
Nie ma możliwości usunięcia użytkownika.
Zablokowanie użytkownika możliwe jest poprzez zmianę jego hasła na nieznane użytkownikowi lub ograniczenie uprawnień do podstawowych.
Nie ma możliwości bezpośredniego zablokowania dostępu dla użytkownika korzystającego z kodu PIN.
Zablokowanie użytkownika korzystającego z kodu PIN możliwe jest poprzez zmianę kodu na nieznany.

2) Identyfikacja wykorzystywanych wysokopoziomowych systemów identyfikacji i autoryzacji.
System nie wykorzystuje wysokopoziomowego systemu zarządzania użytkownikami.

3) Weryfikacja możliwości korzystania z urządzenia w przypadku niedostępności systemu wysokopoziomowego.
System nie wykorzystuje wysokopoziomowego systemu zarządzania użytkownikami.

Wyniki badań:
Werdykt: Pozytywny (P)
Uzasadnienie:

- System zapewnia możliwość zarzadzania użytkownikami w podstawowym zakresie i z pewnymi ograniczeniami takimi jak:
  - Ograniczona liczb użytkowników,
  - Bark możliwości usunięcia użytkownika,

  jednak ograniczenia te nie przeszkadzają w spełnieniu warunków akceptacji (możliwości odebrania dostępu użytkownikowi) (Pozytywny).
- System nie wykorzystuje wysokopoziomowego systemu zarządzania użytkownikami, dlatego jego brak nie wpływa na możliwość logowania (Pozytywny).

Obserwacje (jeśli N)

5.3 CR 1.5

CR 1.5
Oceniający powinien sprawdzić, czy komponent:

- Umożliwia ustawienie początkowej (inicjującej) zawartości danych uwierzytelniających (takie jak hasła, klucze, certyfikaty)
- Umożliwia wykrycie zmiany do domyślnych danych uwierzytelniających ustawionych podczas instalacji,
- Poprawnie realizuje funkcję okresowej zmiany/odświeżenia danych uwierzytelniających; i
- Zabezpiecza dane uwierzytelniające przed ich ujawnieniem i modyfikacją podczas przechowywania, używania i przesyłania.

Uwagi:

• Wskazane jest, aby system wymuszał zmianę domyślnych danych uwierzytelniających lub informowania podczas logowania, że domyślne dane uwierzytelniający (np. hasło) są domyślne i wymagają zmiany.
Warunki akceptacji Zapewnienie możliwości ustawienia początkowej (inicjującej) zawartości danych uwierzytelniających. Zapewnienie możliwości wykrycia zmiany do domyślnych danych uwierzytelniających podczas instalacji. Zapewnienie możliwości okresowej zmiany/odświeżenia danych uwierzytelniających. Zapewnienie należytej ochrony danych uwierzytelniających przed ich ujawnieniem i modyfikacją podczas przechowywania, używania i przesyłania.

Ewaluator(rzy)	[redacted]
Data	[redacted]
Werdykt	N

Plan testów:

1) Identyfikacja stosowanych danych uwierzytelniających.
2) Dla wszytkach zidentyfikowanych danych uwierzytelniających weryfikacja:
   a) możliwości ich okresowej zmiany/odświeżenia,
   b) zastosowanej ich ochrony przed ujawnieniem i modyfikacją podczas przechowywania, używania i przesyłania.

Wykonane badania:

1) Identyfikacja stosowanych danych uwierzytelniających.

[7] Rozdział 9.1:

„Domyślnie w konfiguracji fabrycznej dostępny jest użytkownik z uprawnieniami administratora o nazwie „admin" oraz haśle „Haslo_1234".

„Ze względów bezpieczeństwa nie ma procedury zdalnego odzyskiwania hasła administratora. W przypadku jego utraty niezbędna jest ingerencja serwisu firmy [redacted]"

Przeprowadzono następujące badania komunikacji sieciowej:

- Skan interfejsów urządzenia w poszukiwaniu otwartych portów – wykorzystane narzędzie: nmap.
- Analiza ruch sieciowego dla zidentyfikowanych usług (podczas komunikacji z oprogramowaniem) – wykorzystane narzędzie: wireshark.

Tabela 4 Wyniki badania komunikacji sieciowej

Port (na podstawie skanu)	Protokół (na podstawie dokumentacji)	Aplikacja użyta do połączenia (na podstawie testów)	Szyfrowanie komunikacji (test nasłuchu)	Autoryzacja (na podstawie testów)
102/tcp	IEC 61850	IED Explorer – udało się połączyć	Nie, możliwość podsłuchania, np. hasła	Tak – tylko hasło
4444/tcp	[redacted]	[redacted] Explorer – udało się połączyć	Tak, TLSv1.0	Tak – użytkownik i hasło

Urządzenie dostarczone jest z zainstalowanymi certyfikatami do połączeń SSL. Certyfikaty te nie są wykorzystywane do identyfikacji ani autoryzacji a jednie mają zapewnić kryptograficzną ochronę przesyłanych danych. Tak więc nie są traktowane jako dane uwierzytelniające i nie podlegają ocenie.
Zidentyfikowane dane uwierzytelniające:

- Dane logowania

2) Dla wszytkach zidentyfikowanych danych uwierzytelniających weryfikacja:
   a) możliwości ich okresowej zmiany/odświeżenia

Dane logowania:
System nie wymusza okresowej zmiany haseł, PINu, jednak daje możliwość samodzielnej zmiany przez użytkownika:
„Przewidziano możliwość zmiany haseł przez użytkownika (…). Aby zmienić hasło dla zalogowanego użytkownika należy w zakładce „Ustawienia urządzenia" przejść do sekcji „Opcje zabezpieczeń", podać stare hasło oraz dwukrotnie wprowadzić nowe hasło." [7] rozdz. 9.1.
„Sekcja 'Konfiguracja modułu wyświetlacza' umożliwia zmianę ustawień dotyczących wyświetlacza dostępnego na płycie czołowej (…): 'Pin' – sześciocyfrowy kod pin uniemożliwiający czynności rekonfiguracji urządzenia osobom niepowołanym." [7] rozdz. 9.5.9.
Okresowa zmiana może być realizowana poprzez zapisy proceduralne i ich egzekwowanie.

   b) zastosowanej ich ochrony przed ujawnieniem i modyfikacją podczas przechowywania, używania i przesyłania

Dane logowania:
Dane logowania przechowywane są w pamięci wewnętrznej urządzenia. Użytkownicy nie mają dostępu ani fizycznego, ani logicznego do pamięci urządzenia.
Na podstawie badania komunikacji (Tabela 4 Wyniki badania komunikacji sieciowej) stwierdzono, że dane logowania przesyłane protokołem:

- [redacted] – są chronione kryptograficznie przed ich ujawnieniem,
- IEC 61850 - nie są chronione przed ich ujawnieniem.

Wyniki badań:
Werdykt: Negatywny (N)
Uzasadnienie:

- System umożliwia przywrócenie domyślnego hasła poprzez kontakt z producentem (Pozytywny)
- System umożliwia zmianę domyślnych danych uwierzytelniających (Pozytywny)
- Instrukcja obsługi informuje o konieczności zmiany domyślnych danych uwierzytelniających – zabezpieczenie proceduralne (Pozytywny)
- Komunikacja z wykorzystaniem protokołu IEC 61850 nie zapewnia ochrony przesyłanych danych uwierzytelniania. (Negatywny)

Obserwacje (jeśli N):
Zastosowanie komunikacji IEC 61850 - Aktualnie zastosowana implementacja tej komunikacji nie jest bezpieczna bez dodatkowych rozwiązań. Powinna być niestosowana lub dopuszczalna tylko w kontrolowanych warunkach, gdy otoczenie zapewni bezpieczeństwo (np. ograniczony dostęp fizyczny, stosowanie dodatkowych zabezpieczeń typu szyfrowany kanał VPN).

5.4 CR 1.7

CR 1.7 Oceniający powinien sprawdzić, czy komponent stosujący uwierzytelnianie za pomocą haseł zapewnia: • Możliwość wymuszania złożoności haseł (np. minimalna długość hasła, rodzaje znaków) zgodnie z uznawanymi międzynarodowo i sprawdzonymi wytycznymi. **Uwagi:** • Zaleca się, aby kontrola złożoności haseł umożliwiła spełnienie ogólnie uznawanych praktyki i rekomendacji dotyczących złożoności haseł takich jak np. NIST SP 800-63B [8].
Warunki akceptacji Wymuszona kontrola złożoności stosowanych haseł.

Ewaluator(rzy)	[redacted]
Data	[redacted]
Werdykt	P

Plan testów:

1) Ocena i weryfikacja możliwości kontroli złożoności stosowanych haseł.

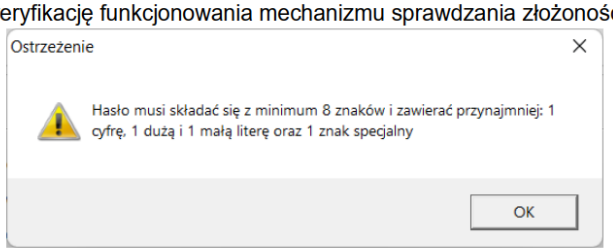
Wykonane badania:

1) Ocena i weryfikacja możliwości kontroli złożoności stosowanych haseł.

Na podstawie CR1.1 badań ustalono, że urządzenia umożliwia autoryzację z wykorzystaniem:

- Użytkownika i hasła (dla komunikacji z wykorzystaniem protokołu [redacted])
- Kodu PIN (dla panelu użytkownika)

Przeprowadzono weryfikację funkcjonowania mechanizmu sprawdzania złożoności haseł:



Rysunek 8 Komunikat informujący o wymaganiach dotyczących złożoności hasła

Badania wskazały, że system:

- Kontroluje złożoność haseł i nie pozwala na wprowadzenie hasła nie spełniającego wymagania,
- Nie pozwala na zmianę wymagań dotyczących złożoności hasła.

W [7] Rozdział 9.5. zawarto informację o długości kodu PIN: „Pin" – sześciocyfrowy kod pin uniemożliwiający czynności rekonfiguracji urządzenia osobom niepowołanym"

Badania potwierdziły, że zarówno w aplikacji jak i w panelu użytkownika, zmiana kodu PIN wymaga podania dokładnie 6 znaków.

Wyniki badań:

Werdykt: Pozytywny (P)

Uzasadnienie:

- System zapewnia kontrolę złożoności hasła i wymusza zastosowanie odpowiednio złożonego hasła (Pozytywny).
- System nie pozwala na zmianą wymagań złożoności hasła, jednak zastosowane przez producenta wymagania są wystarczająco restrykcyjne (biorąc pod uwagę poziom wymagań podlegających ocenie - SL1) (Pozytywny).
- System wymusza długość kodu PIN na 6 znaków. (Pozytywny).

Obserwacje (jeśli N)

5.5 CR 1.10

CR 1.10 Oceniający powinien sprawdzić, czy: • Generowane podczas procesu logowania komunikaty (w szczególności błędów) nie zawierają informacji ułatwiających przeprowadzenia ataku na proces uwierzytelniania (np. liczba gwiazdek w polu hasła zgodna z długością hasła, komunikaty błędnego logowania umożliwiające ustalenie, czy błędne było hasło, czy login).	
Warunki akceptacji Wyświetlane podczas procesu logowania informacje nie zawierają informacji ułatwiających przeprowadzenie ataku na proces uwierzytelniania.	
Ewaluator(rzy)	[redacted]
Data	[redacted]
Werdykt	P

Plan testów:

1) Identyfikacja stosowanych interfejsów umożliwiających logowanie oraz wykorzystanych metod logowania.
2) Weryfikacja dla wszystkich zidentyfikowanych interfejsów i metod logowania czy informacje zwrotne z systemu nie ujawniają informacji mogących ułatwić atak na proces uwierzytelniania.

Wykonane badania:

1) Identyfikacja stosowanych interfejsów umożliwiających logowanie oraz wykorzystanych metod logowania.

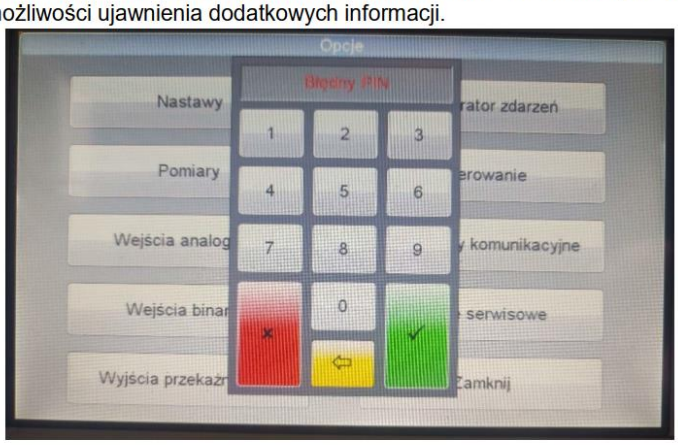
Zidentyfikowane w CR1.1 interfejsy, które umożliwiają interakcję użytkownika z urządzeniem:

- panel użytkownika (ekran dotykowy, przyciski fizyczne)
- interesy komunikacyjne korzystające z protokołu [redacted] z wykorzystaniem aplikacji narzędzia „[redacted] Explorer”

2) Weryfikacja dla wszystkich zidentyfikowanych interfejsów i metod logowania czy informacje zwrotne z systemu nie ujawniają informacji mogących ułatwić atak na proces uwierzytelniania.

Panel użytkownika (ekran dotykowy, przyciski fizyczne):

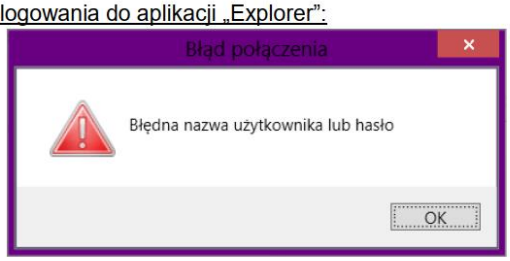
Autoryzacja kodem PIN nie wymaga podania nazwy użytkownika komunikat błędu dotyczy więc tylko kodu i nie ma możliwości ujawnienia dodatkowych informacji.



Rysunek 9 Komunikat dla błędnego kodu PIN

Interfejsy komunikacyjne korzystające z protokołu [redacted] z wykorzystaniem aplikacji narzędzia „Explorer":

Próba nieprawidłowego logowania do aplikacji „Explorer":



Rysunek 10 Komunikat błędu logowania w aplikacji

W celu dokładniejszego sprawdzenia przeprowadzono badania.
Weryfikacja komunikatów wyświetlanych dla następujących przypadków poświadczeń.

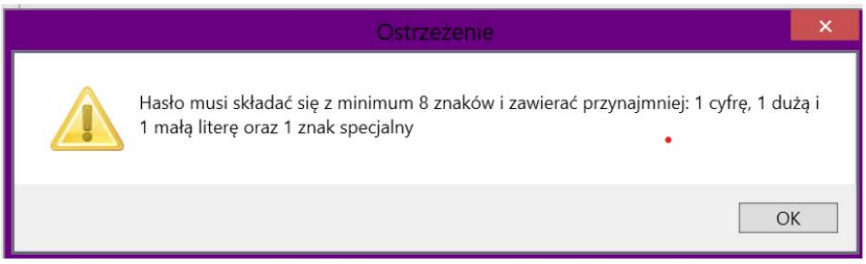
Tabela 5 Weryfikacja komunikatów wyświetlanych dla różnych przypadków

Badana sytuacja błędna	Wynik badania
Nazwa istniejącego użytkownika ('admin'), nieistniejące hasło	Poprawny komunikat (Rysunek 10 Komunikat błędu logowania w aplikacji)
Nazwa istniejącego użytkownika ('user6'), hasło przypisane do innego użytkownika (hasło konta 'admin')	Poprawny komunikat (Rysunek 10 Komunikat błędu logowania w aplikacji)
Nazwa nieistniejącego użytkownika, hasło przypisane do jednego z użytkowników (hasło konta 'admin')	Poprawny komunikat (aplikacji)
Nazwa nieistniejącego użytkownika, nieistniejące hasło	Poprawny komunikat (Rysunek 10 Komunikat błędu logowania w aplikacji)

Weryfikacja komunikatów w przypadku ustawiania hasła niezgodnego z wymaganiami określonymi w wymaganiach z uwzględnieniem następujących przypadków.

Tabela 6 Weryfikacja komunikatów w przypadku ustawiania hasła niezgodnego z wymaganiami

Badana sytuacja błędna	Wynik badania
Hasło zawierające wszystkie wymagane znaki, ale krótsze niż wymagane ('Haslo_1')	Wynik poprawny (Rysunek 11 Komunikat przy braku spełnienia wymagań na złożoność i długość hasła).
Hasło nie zawierające jednego z wymienionych rodzajów znaków, dłuższe od wymaganego ('Haslo1234')	Wynik poprawny (Rysunek 11 Komunikat przy braku spełnienia wymagań na złożoność i długość hasła).
Hasło nie zawierające jednego z wymienionych rodzajów znaków, krótsze od wymaganego ('Haslo12')	Wynik poprawny (Rysunek 11 Komunikat przy braku spełnienia wymagań na złożoność i długość hasła).



Rysunek 11 Komunikat przy braku spełnienia wymagań na złożoność i długość hasła

W celu sprawdzenia, czy w przypadku błędnego kodu PIN komunikat nie stanowi potencjalnej informacji przydatnej do przeprowadzenia ataku przeprowadzono badanie polegające na użyciu w powyższych sytuacjach następujących kodów.

Tabela 7 Weryfikacja komunikatu w przypadku błędnego kodu PIN

Badana sytuacja błędna	Wynik badania
Błędny, o prawidłowej długości	Wynik poprawny (Rysunek 9 Komunikat dla błędnego kodu PIN)
Błędny, o mniejszej niż wymagana długości	Wynik poprawny (Rysunek 9 Komunikat dla błędnego kodu PIN)
Błędny, o większej niż wymagana długości (jeżeli możliwy do wprowadzenia)	Brak możliwości wprowadzenia. Okno na panelu nie przyjmuje więcej niż 6 cyfr.
Pierwsze 5 cyfr poprawnego kodu	Wynik poprawny (Rysunek 9 Komunikat dla błędnego kodu PIN)
Złożony z poprawnego kodu i jednej nadmiarowej cyfry (jeżeli możliwy do wprowadzenia)	Brak możliwości wprowadzenia. Okno na panelu nie przyjmuje więcej niż 6 cyfr.

Wyniki badań:

Werdykt: Pozytywny (P)

Uzasadnienie:

- Proces logowania i komunikaty podczas procesu logowania nie ujawniają informacji mogących ułatwić atak na ten proces (Pozytywny).

Obserwacje (jeśli N)

5.6 CR 1.11

CR 1.11 Oceniający powinien sprawdzić, czy komponent umożliwia: • Wymuszenie limitu liczby nieudanych, kolejnych prób logowania przez dowolny podmiot (użytkownik, proces programowy lub urządzenie) w określonym, konfigurowalnym przedziale czasu, i • Automatyczne blokowanie dostępu na określony czas lub do momentu odblokowania przez administratora, po osiągnięciu limitu nieudanych prób logowania, • Możliwość odblokowania konta przez administratora przed upływem czasu blokady. **Uwagi**: • Zaleca się, aby stosowane rozwiązania zabezpieczające przed atakami typu DoS, czy siłowymi próbami uzyskania dostępu, nie blokowały dostępu administratorowi w przypadku konieczności podjęcia działań w sytuacjach awaryjnych.
Warunki akceptacji Zapewnienie możliwości konfiguracji limitu nieudanych prób logowania w określonym przedziale czasu. Zapewnienie blokady możliwości logowania po przekroczeniu limitu nieudanych prób logowania w określonym przedziale czasu.

Ewaluator(rzy)	[redacted]
Data	[redacted]
Werdykt	P

Plan testów:

1) Identyfikacji stosowanych interfejsów umożliwiających logowanie i wykorzystanych metod logowania.
2) Badanie stosowanych rozwiązań (podejmowanych przez system akcji) na wypadek nieudanych logowań dla wszystkich interfejsów dostępnych dla użytkowników.

Wykonane badania:

1) Identyfikacji stosowanych interfejsów umożliwiających logowanie i wykorzystanych metod logowania.

Zidentyfikowane w CR1.1_1 interfejsy, które umożliwiają interakcję użytkownika z urządzeniem:

- panel użytkownika (ekran dotykowy, przyciski fizyczne)
- interesy komunikacyjne korzystające z protokołu [redacted] z wykorzystaniem aplikacji narzędzia „[redacted] Explorer”

2) Badanie stosowanych rozwiązań (podejmowanych przez system akcji) na wypadek nieudanych logowań dla wszystkich interfejsów dostępnych dla użytkowników.

Kod PIN na panelu użytkownika:

Nie ma ograniczenia ilości błędnych prób logowania na panelu użytkownika za pomocą kodu PIN.

7.10 CR 3.7

CR 3.7 Oceniający powinien sprawdzić, czy: • Komponent identyfikuje i obsługuje stany błędów w sposób, który nie dostarcza informacji, jakie mogłyby zostać wykorzystane do zaatakowania systemu IACS. **Uwagi:** • Komunikaty generowane przez komponent powinny zapewniać użyteczną informację we właściwym czasie, ale nie ujawniając potencjalnie szkodliwych informacji, które mogłyby być wykorzystane do przeprowadzenia ataku. • Przykładowy komunikat o błędzie podczas logowania wskazujący na nieprawidłową nazwę lub nieprawidłowe hasło może być pomocny w przeprowadzeniu ataku; • Analiza powinna uwzględniać komunikaty generowane przez komponent z wykorzystaniem różnych interfejsów, możliwość lokalizacji komunikatów wkompilowanych w kod i/lub znajdujących się poza aplikacją, przechowywanych w postaci jawnej i/lub zakodowanej. • Zobacz również wymaganie CR 1.10.	
Warunki akceptacji Dla wszystkich zidentyfikowanych interfejsów i komunikatów generowanych przez komponent dla obsługi stanów błędów nie następuje dostarczanie informacji, jakie mogłyby zostać wykorzystane do zaatakowania systemu IACS.	
Ewaluator(rzy)	[redacted]
Data	[redacted]
Werdykt	P

Plan testów:

1) Identyfikacja wszystkich interfejsów, które mogą być wykorzystywane do generowania komunikatów.
2) Dla zidentyfikowanych interfejsów, identyfikacja wszystkich komunikatów dotyczących stanów błędów oraz ich analiza w kontekście bezpieczeństwa, z uwzględnieniem okoliczności ich generowania przez komponent, ich treści i zawartych parametrów.

Wykonane badania:

1) Identyfikacja wszystkich interfejsów, które mogą być wykorzystywane do generowania komunikatów.

Podczas badania wymagania CR 1.1 zidentyfikowano następujące interfejsy urządzenia:

- panel użytkownika (ekran dotykowy, przyciski fizyczne)
- interfejsy komunikacyjne korzystające z protokołu IEC 60870-5-103, IEC 61850 oraz ZP-6 z wykorzystaniem aplikacji narzędzia.

Ze względu na poziom SL-1 i związany z nim niski potencjał ataku (brak specjalistycznej wiedzy oraz narzędzi) komunikaty błędów, jakie mogą pojawić się podczas komunikacji protokołami IEC 60870-5-103, IEC 61850 nie będą analizowane, gdyż można przyjąć, że atakujący na poziomie SL-1 nie będzie w stanie uzyskać dostępu i przeprowadzić komunikacji z wykorzystaniem tych interfejsów i protokołów.

Dla protokołu ZP-6, także ze względu na poziom SL-1, można przyjąć, że użytkownik będzie korzystał z tego interfejsu tylko z poziomu aplikacji [redacted], gdyż protokół ten nie jest jawny i jego wykorzystanie w inny sposób wymaga bardzo specjalistycznej wiedzy i narzędzi znacznie wykraczających poza potencjał ataku dla poziomu SL-1.
W wyniki identyfikacji i wstępnej analizy, do dalszych rozważań pozostawiono następujące interfejsy:

- panel użytkownika (ekran dotykowy, przyciski fizyczne)
- komunikacja protokołem ZP-6 w z wykorzystaniem aplikacji [redacted].

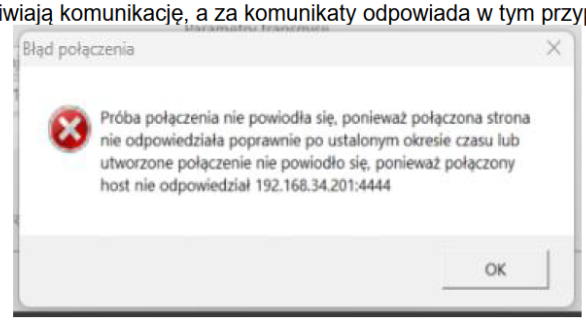
Dodatkowo podczas analizy tych interfejsów stwierdzono, że użytkownik niezalogowany posiada tylko podstawową funkcjonalność umożliwiającą przeglądanie części danych oraz możliwość zalogowania się. Tak więc analizę komunikatów błędu można ograniczyć do informacji o błędach dostępnych bez logowania oraz komunikatów błędów związanych z procesem autoryzacji, zarówno na panelu użytkownika, jak i w aplikacji [redacted]

2) Dla zidentyfikowanych interfejsów, identyfikacja wszystkich komunikatów dotyczących stanów błędów oraz ich analiza w kontekście bezpieczeństwa, z uwzględnieniem okoliczności ich generowania przez komponent, ich treści i zawartych parametrów.

Analiza komunikatów błędów związanych z procesem autoryzacji zarówno na panelu użytkownika została przeprowadzona w ramach badania wymagania CR 1.10 i zakończyła się wynikiem pozytywnym.
Analiza dostępnych informacji o błędach dla niezalogowanych użytkowników.
Panel użytkownika:
Niezalogowany użytkownik nie ma możliwości podjęcie żadnych działań, a tym samym możliwości wygenerowania błędów. Jedyna możliwość uzyskania dodatkowych możliwości to przegląd konfiguracji urządzenia oraz rejestru zdarzeń. Podczas oceny zawartości informacji w rejestrze zdarzeń nie stwierdzono w nim informacji mogących być uznanych za wrażliwe czy ułatwiających przeprowadzenie ataków. (Zobacz wymaganie CR 2.8)
Aplikacja [redacted]
W aplikacji niezalogowany użytkownik ma możliwość:

- przeglądu rejestru zdarzeń
- zmian parametrów konfiguracyjnych aplikacji (umożliwiających połączenie z uprzedzeniem)

Podczas oceny zawartości informacji w rejestrze zdarzeń nie stwierdzono w nim informacji mogących być uznanych za wrażliwe czy ułatwiających przeprowadzenie ataków (zobacz poprzedni akapit oraz badanie CR 2.8)
Błędne parametry logowania nie skutkują komunikatami bezpośrednio z urządzenia, gdyż błędne parametry uniemożliwiają komunikację, a za komunikaty odpowiada w tym przypadku aplikacja.

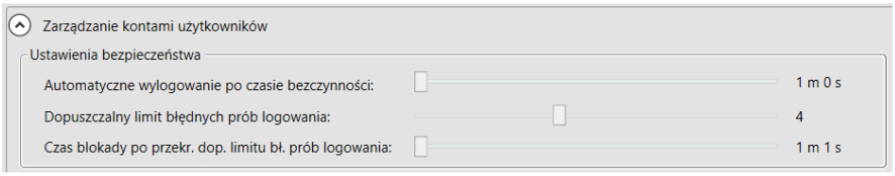


Rysunek 42 Komunikat błędu połączenia w aplikacji

Wyniki badań:
Werdykt: Pozytywny (P)

Długość kodu PIN (6 cyfr) oraz możliwość tylko ręcznego jego wprowadzania przez użytkownika oraz ograniczony dostęp atakującego do urządzenia w znaczący sposób utrudniają możliwość przeprowadzenia skutecznego ataku siłowego na ten kanał ataku.
Logowanie z wykorzystaniem protokołu [redacted] oraz aplikacji „[redacted] Explorer":
Panel zarządzania użytkownikami umożliwia ustawienie restrykcji związanych z nieudanymi próbami logowania. Możliwe jest:

- Określenie liczby nieudanych logować skutkujące zablokowaniem kolejnych prób w zakresie 1-10 prób
- Określenie czasu blokady kolejnych prób po przekroczeniu limitu nieudanych prób w zakres 1s – 1h



Rysunek 12 Panel konfiguracji bezpieczeństwa logowania (dla protokołu [redacted] i aplikacji)

Wyniki badań:
Werdykt: Pozytywny (P)
Uzasadnienie:

- System zapewnia możliwość konfiguracji limitu nieudanych prób logowania w określonym przedziale czasu (Pozytywny).
- System umożliwia po przekroczeniu nieudanej liczby prób automatyczne zablokowanie kolejnych prób logowania na konfigurowalny okres (Pozytywny).

Obserwacje (jeśli N)

6 Badania wykonał(li):

1. [redacted]
2. [redacted]
3. [redacted]
4. [redacted]

****

Wersja skrócona sprawozdania do celów rozprawy doktorskiej - pozostałe strony zostały usunięte

7 Załączniki

Bibliografia

[1] „[redacted] Sp. z o.o.," [Online]. Available: https://www.[redacted].pl/. [Data uzyskania dostępu: październik 2022].

[2] Zakład [redacted], „[redacted] Terminale zabezpieczeniowe. Instrukcja [redacted]; wyd. 6," [redacted] Sp. z o.o., [redacted], listopad 2021.

[3] Zakład [redacted], „[redacted] [redacted]komunikacyjne. Załącznik do instrukcji," [redacted] Sp. z .o.o, [redacted], 2021.

[4] [redacted] Sp z o.o., „Opis komunikacji z zabezpieczeniem [redacted] wyposażonym w moduł komunikacyjny [redacted]," [redacted] Sp z o.o., [redacted], 02.09.2022.

[5] Fachowy Elektryk, „Badanie zabezpieczeń odległościowych - urządzenia serii Freja 500," [Online]. Available: https://www.fachowyelektryk.pl/technologie/pomiary/2520-badanie-zabezpieczen-odleglosciowych-urzadzenia-serii-freja-500.html. [Data uzyskania dostępu: październik 2022].

[6] „PN-EN IEC 62443-4-2 Bezpieczeństwo w systemach sterowania i automatyki przemysłowej Część 4-2: Wymagania techniczne bezpieczeństwa dla komponentów IACS".

[7] „[DOC_User] Dokumentacja użytkownika".

[8] N. S. 800-63B, *Digital Identity Guidelines - Authentication and Lifecycle Management.*

[9] NIST SP 800-92, *Guide to Computer Security Log Management.*

[10] „OWASP Code Review Guide".

[11] NIST SP 800-57, *Recommendation for Key Management - Part 1: General.*

[12] FIPS 140-2, *Security Requirements for Cryptographic Modules.*

[13] ISO/IEC 19790, *Information Technology - Security techniques - Security requirements for cryptographic modules.*

K O N I E C S P R A W O Z D A N I A Z B A D A Ń