WYTYCZNE NR 9
PREZESA URZĘDU LOTNICTWA CYWILNEGO

z dnia 13 lipca 2011 r.

w sprawie wprowadzenia do stosowania zasad oceny bezpieczeństwa oprogramowania stosowanego w systemach będących częścią składową europejskiej sieci zarządzania ruchem lotniczym

Na podstawie art. 21 ust. 2 pkt 16 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2006 r. Nr 100, poz. 696, z późn. zm.[1)]) zarządza się, co następuje:

§ 1.1. W celu podniesienia poziomu bezpieczeństwa operacyjnego służb żeglugi powietrznej wykorzystujących systemy informatyczne zaleca się stosowanie „*Zasad oceny bezpieczeństwa oprogramowania stosowanego w systemach będących częścią składową europejskiej sieci zarządzania ruchem lotniczym*".

2. Zasady, o których mowa w ust. 1, stanowią załącznik do wytycznych[2)].

§ 2. Wytyczne wchodzą w życie z dniem podpisania.

Prezes Urzędu Lotnictwa Cywilnego
Grzegorz Kruszyński

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2006 r. Nr 104, poz. 708 i 711, Nr 141, poz. 1008, Nr 170, poz. 1217 i Nr 249, poz. 1829, z 2007 r. Nr 50, poz. 331 i Nr 82, poz. 558, z 2008 r. Nr 97, poz. 625, Nr 144, poz. 901, Nr 177, poz. 1095, Nr 180, poz. 1113 i Nr 227, poz. 1505, z 2009 r. Nr 18, poz. 97 i Nr 42, poz. 340, z 2010 r. Nr 47, poz. 278 i Nr 182, poz. 1228 oraz z 2011 r. Nr 80, poz. 432 i Nr 106, poz. 622.

[2)] Załącznik do niniejszych wytycznych jest dostępny na stronie internetowej Urzędu Lotnictwa Cywilnego www.ulc.gov.pl oraz w Ośrodku Informacji Naukowej, Technicznej i Ekonomicznej Urzędu Lotnictwa Cywilnego, ul. Marcina Flisa 2, 02-247 Warszawa, tel. (22) 520 73 14, (22) 520 73 15.

Załącznik do Wytycznych nr 9
Prezesa Urzędu Lotnictwa Cywilnego
z dnia 7 lipca 2011 r.

ZASADY OCENY BEZPIECZEŃSTWA OPROGRAMOWANIA STOSOWANEGO W SYSTEMACH BĘDĄCYCH CZĘŚCIĄ SKŁADOWĄ EUROPEJSKIEJ SIECI ZARZĄDZANIA RUCHEM LOTNICZYM

Warszawa, 2011

Preambuła

„*Zasady oceny bezpieczeństwa oprogramowania stosowanego w systemach będących częścią składową europejskiej sieci zarządzania ruchem lotniczym*" są zbiorem informacji oraz zaleceń Prezesa Urzędu Lotnictwa Cywilnego kierowanym do instytucji zapewniających służby żeglugi powietrznej, zwanych dalej „instytucjami", stosownie do postanowień Rozporządzenia Komisji (WE) nr 482/2008 z dnia 30 maja 2008 r. ustanawiającego system zapewnienia bezpieczeństwa oprogramowania do stosowania przez instytucje zapewniające służby żeglugi powietrznej oraz zmieniającego załącznik II do rozporządzenia (WE) nr 2096/2005 (*Dz. Urz. L 141 z 31.5.2008, str. 5—10*).

Na podkreślenie zasługuje fakt, iż wytyczne nie są źródłem prawa, a jedynie określeniem dobrych praktyk oraz zaleceń, które mogą pozytywnie wpłynąć na jakość usług świadczonych przez instytucje dostarczające ATS, CNS lub zapewniające ATFM lub ASM, przyczyniając się do poprawy bezpieczeństwa operacyjnego w systemie zarządzania ruchem lotniczym.

Wytyczne zostały opracowane na podstawie standardów oraz zalecanych metod postępowania Europejskiej Organizacji do Spraw Bezpieczeństwa Żeglugi Powietrznej (EUROCONTROL), a także doświadczeń zebranych przez inspektorów Departamentu Żeglugi Powietrznej Urzędu Lotnictwa Cywilnego.

Publikacja niniejszego dokumentu ma na celu poprawę standardów pracy w zakresie bezpieczeństwa oprogramowania wykorzystywanego w systemie zarządzania ruchem lotniczym.

Dokumenty normatywne

Lp.	Tytuł dokumentu	Numer Dziennika Urzędowego UE	Skrót użyty w tekście
1.	Rozporządzenie Komisji (WE) nr 482/2008 z dnia 30 maja 2008 r. ustanawiające system zapewnienia bezpieczeństwa oprogramowania do stosowania przez instytucje zapewniające służby żeglugi powietrznej oraz zmieniające załącznik II do rozporządzenia (WE) nr 2096/2005	L 141/5-10	rozporządzenie nr 482/2008
2.	Rozporządzenie Komisji (WE) nr 2096/2005 z dnia 20 grudnia 2005 r. ustanawiającym wspólne wymogi dotyczące zapewniania służb żeglugi powietrznej	L 335/13-30	rozporządzenie nr 2096/2005
3.	Rozporządzenie (WE) nr 552/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. w sprawie interoperacyjności Europejskiej Sieci Zarządzania Ruchem Lotniczym (Rozporządzenie w sprawie interoperacyjności), zmienione przez Rozporządzenie (WE) nr 1070/2009 Parlamentu Europejskiego i Rady z dnia 21 października 2009 r.	L 96/26-42	rozporządzenie nr 552/2004
4.	Rozporządzenie Komisji (WE) nr 1315/2007 z dnia 8 listopada 2007 r. w sprawie nadzoru nad bezpieczeństwem w zarządzaniu ruchem lotniczym oraz zmieniające rozporządzenie (WE) nr 2096/2005	L 291/16-22	rozporządzenie nr 1315/2007

Stosowane określenia i definicje

W niniejszym dokumencie przyjęto definicje określone w art. 2 rozporządzenia nr 482/2008.
Ponadto zastosowanie mają niżej wymienione definicje i określenia:

Wyposażenie

Wyposażenie to platforma sprzętowa wraz z zainstalowanym na niej oprogramowaniem.

Oprogramowanie istniejące

Oprogramowanie istniejące to wszelkie oprogramowanie, które nie jest napisane specjalnie dla danej aplikacji, jednakże jest wykorzystywane w kodzie źródłowym lub bierze udział w procesie tworzenia kodu wynikowego. Z reguły jest to oprogramowanie typu COTS. Typowymi przykładami takiego oprogramowania są:

- systemy operacyjne (Windows, Linux, OpenVMS itp.)

– silniki baz danych (Oracle RDBM, PostgreSQL, MySQL, SQL Server itp.)
– serwery aplikacji (middleware)
– środowiska uruchomieniowe (Java Virtual Machine itp.)

Oprogramowanie typu CUSTOM

Oprogramowanie typu CUSTOM to oprogramowanie tworzone przez zewnętrznego lub wewnętrznego dostawcę na indywidualne zamówienie użytkownika, przy czym w obu przypadkach może wykorzystywać oprogramowanie istniejące.

Oprogramowanie typu COTS $1x10^{-4}$

Oprogramowanie typu COTS $1x10^{-4}$ to oprogramowanie, dla którego określona w drodze analizy bezpieczeństwa maksymalna dopuszczalna liczba usterek wyposażenia przypadająca na jedną godzinę pracy jest równa $1x10^{-4}$ bądź większa. Przy czym wyposażenie to musi stanowić moduł możliwy do bezpośredniego wyodrębniania z systemu. Przykładami takiego wyposażenia mogą być: hub, switch, router, modem, system zobrazowania danych radarowych.

Oprogramowanie typu COTS $1x10^{-5}$

Oprogramowanie typu COTS $1x10^{-5}$ to oprogramowanie, dla którego określona w drodze analizy bezpieczeństwa maksymalna dopuszczalna liczba usterek wyposażenia przypadająca na jedną godzinę pracy jest równa $1x10^{-5}$ bądź mniejsza. Przy czym wyposażenie to musi stanowić moduł możliwy do bezpośredniego wyodrębniania z systemu. Przykładami takiego wyposażenia mogą być: hub, switch, router, modem, system zobrazowania danych radarowych.

AEL (Assurance Evidence Level) – Poziom Zapewniania Dowodów

AEL określa minimalny zestaw dowodów niezbędnych do potwierdzenia spełnienia wymagań bezpieczeństwa. AEL jest przydzielany zgodnie z sekcją 4 punktu 3.2.4 załącznika II do rozporządzenia (WE) nr 2096/2005 – odzwierciedloną w poniższej tabeli (Tab. A) w drodze analizy zagrożeń jakie niosą za sobą awarie oprogramowania z punktu widzenia działania systemu.
Zaleca się przeprowadzanie analizy zagrożeń w ramach analizy bezpieczeństwa, zgodnej z wymaganiami ESARR 4.

Tab. A. Zależność AEL od wagi zagrożenia

Poziom AEL	**1**	**2**	**3**	**4**	**5**
Waga zagrożenia	Wypadek	Poważny incydent	Większy incydent	Znaczący incydent	Bez bezpośredniego wpływu na bezpieczeństwo

Postanowienia ogólne

Cel wydania zasad

Niniejsze zasady mają na celu zapewnienie ograniczenia ryzyka związanego z wykorzystaniem oprogramowania w Europejskiej Sieci Zarządzania Ruchem Lotniczym (oprogramowanie „EATMN"), do akceptowalnego poziomu.
Przepis art. 3 ust. 3 rozporządzenia nr 482/2008 nakłada na instytucje obowiązek złożenia zapewnienia krajowej władzy lotniczej, że ustanowiony przez nie system bezpieczeństwa oprogramowania gwarantuje prawidłowość procesów zachodzących w cyklu życia oprogramowania.
W celu spełnienia tego obowiązku zaleca się, aby instytucja przedstawiła Prezesowi Urzędu Lotnictwa Cywilnego – jako krajowej władzy lotniczej – dokument potwierdzający pozytywne zakończenie oceny bezpieczeństwa oprogramowania.
Niniejsze zasady określają dobre praktyki pomocne przy opracowywaniu przez instytucje szczegółowych procedur i sposobów oceny bezpieczeństwa oprogramowania stosowanego w systemie zarządzania ruchem lotniczym.
Niniejsze zasady nie wykluczają stosowania przez instytucje innych procedur i sposobów oceny bezpieczeństwa oprogramowania, z zastrzeżeniem art. 3 ust. 3 rozporządzenia nr 482/2008.

Zakres stosowania

Zgodnie z rozporządzeniem nr 482/2008 od dnia 1 stycznia 2009 r. nowe oprogramowanie, a od dnia 1 lipca 2010 r. dokonywane zmiany w oprogramowaniu działających na ten dzień systemów ATS, ASM, ATFM oraz CNS – wymagają stosownej weryfikacji.
W związku z powyższym zaleca się stosowanie niniejszych zasad do wszelkich oprogramowań wykorzystywanych operacyjnie w systemach ATS, ASM, ATFM oraz CNS, będących częścią EATMN.

Działania instytucji związane z oceną bezpieczeństwa oprogramowania

Zaleca się, aby wykonanie przez instytucję oceny bezpieczeństwa każdego oprogramowania wykorzystywanego operacyjnie w systemach ATS, ASM, ATFM oraz CNS będących częścią składową EATMN było potwierdzone przez wydanie „Deklaracji bezpieczeństwa oprogramowania".

Zalecane metody oceny bezpieczeństwa oprogramowania

Określenie dowodów i argumentów dla oprogramowania typu CUSTOM

W przypadku gdy oprogramowanie typu CUSTOM wykorzystuje oprogramowanie istniejące, proces oceny bezpieczeństwa musi obejmować funkcjonalną całości oprogramowania.

Potwierdzenie zasadności wymagań bezpieczeństwa

Dla wykazania, że dostępne argumenty i dowody prawidłowo identyfikują wymogi konieczne i wystarczające do osiągnięcia dopuszczalnego poziomu bezpieczeństwa oprogramowania w ramach systemu, powinno się ustalić czy:

1) wymagania bezpieczeństwa oprogramowania pozostają ważne na poziomie wymagań bezpieczeństwa systemu;
2) wymagania bezpieczeństwa oprogramowania określają bezpieczne zachowania oprogramowania;
3) wymagania bezpieczeństwa oprogramowania obejmują:
   a) specyfikację dla każdego z atrybutów zachowań oprogramowania w postaci wymagań funkcjonalnych i niefunkcjonalnych (wymagania czasowe, odporność na nietypowe warunki operacyjne, niezawodność, dokładność, wykorzystanie zasobów docelowej platformy sprzętowej i tolerancja na przeciążenia),
   b) potwierdzenie, że dany atrybut nie ma zastosowania;
4) wszystkie rodzaje niebezpiecznych awarii oprogramowania zostały określone:
   a) dla AEL 1,2,3,4,5 – w wymaganiach oprogramowania,
   b) dla AEL 1,2,3,4 – w architekturze wewnętrznej,
   c) dla AEL 1,2 – na poziomie kodu źródłowego;
5) wszystkie rodzaje niebezpiecznych awarii, które zostały zidentyfikowane na każdym z poziomów projektowych lub w czasie implementacji oprogramowania odnoszą się do wymagań bezpieczeństwa oprogramowania, platformy sprzętowej i systemu operacyjnego lub udokumentowano, że nie ma takiej potrzeby;
6) wymagania bezpieczeństwa oprogramowania zostały określone w sposób wyraźny oraz taki, aby były łatwe do odróżnienia od innych wymagań;
7) wymagania bezpieczeństwa oprogramowania zostały określone w sposób wystarczająco szczegółowy i przejrzysty, aby umożliwić opracowanie i wdrożenie wymaganego poziomu bezpieczeństwa;
8) dostępne są pośrednie dowody i argumenty wykazujące, że:
   a) zapisy (notacje) specyfikacji wspierają identyfikację awarii oprogramowania, które powodują zagrożenie na poziomie systemu,
   b) zastosowano najlepsze dostępne metody i techniki analityczne dla atrybutów wymagań bezpieczeństwa oprogramowania,
   c) narzędzia, wykorzystywane w procesach analizy, zostały sprawdzone i zatwierdzone przez instytucję,
   d) narzędzia, użyte do dostarczenia i/lub przedstawienia wymagań bezpieczeństwa oprogramowania, zostały sprawdzone i zatwierdzone przez instytucję.

Potwierdzenie spełnienia wymagań bezpieczeństwa

Zaleca się, aby potwierdzenie spełnienia wymagań bezpieczeństwa odbywało się poprzez dostarczenie dowodów i argumentów w postaci dokumentów, których formy są zgodne z tabelą nr 1 określoną w pkt. 5 niniejszych zasad.
Zaleca się również, aby źródła dowodów dla każdego z atrybutów zachowań oprogramowania były zgodne z tabelą nr 2 określoną w pkt. 5 niniejszych zasad.

Jednocześnie zaleca się korzystanie z tabeli nr 3 określonej w pkt. 5 niniejszych zasad przy ustalaniu zakresu testów i analiz przeprowadzanych dla każdego z atrybutów zachowań oprogramowania.

Potwierdzenie możliwości śledzenia wymagań bezpieczeństwa

Bezpośrednie dowody i argumenty na spełnienie wymogu możliwości śledzenia wymagań bezpieczeństwa oprogramowania powinny wykazać, że każdy wymóg bezpieczeństwa wprowadzony na każdym poziomie projektowym był śledzony

do tego poziomu, na którym wykazane zostało jego spełnienie - także w powiązaniu z wymaganiem w zakresie bezpieczeństwa systemu.

Pośrednie dowody i argumenty potwierdzające możliwości śledzenia wymagań bezpieczeństwa powinny wykazać, że:

1) zapis (notacja) śledzenia wymagań bezpieczeństwa oprogramowania jest jednoznaczny i stosowany konsekwentnie;
2) monitorowanie obejmuje wszystkie oprogramowania istniejące wchodzące w skład nowotworzonego oprogramowania oraz aplikacje, do których się ono odwołuje;
3) zapis (notacja) śledzenia wymagań bezpieczeństwa oprogramowania umożliwia śledzenie wymagań zarówno w przód jak i wstecz;
4) wykorzystane procedury i narzędzia zapewniają, że jakakolwiek utrata śledzenia lub jego nieprawidłowość zostaną wykryte i skorygowane;
5) wszelkie narzędzia wykorzystywane do śledzenia zostały zweryfikowane i zatwierdzone przez instytucję.

Potwierdzenie spójności konfiguracji

Zaleca się by narzędzia wykorzystywane do tworzenia i utrzymania spójności konfiguracji zostały zweryfikowane i zatwierdzone przez instytucję, a przeprowadzona kontrola zachodzących zmian konfiguracji oraz system zarządzania konfiguracją umożliwiał zachowanie spójności konfiguracji podczas całego cyklu życia oprogramowania.

Dowody i argumenty potwierdzające spójność konfiguracji to:

1) kod obiektowy;
2) kod źródłowy;
3) ustalone wymagania (wymagania systemu, wymagania bezpieczeństwa oprogramowania, inne wymagania dotyczące oprogramowania);
4) opracowane instrukcje obsługi i inne instrukcje związane z oprogramowaniem;
5) dane z badań, skrypty testowe, programy;
6) dane na temat wersji sprzętu używanego przy generowaniu danych testowych, stymulacji badań i rejestrowaniu wyników badań;
7) opisy pośrednich stanów projektowania oprogramowania, zarówno w języku naturalnym lub formalnych lub półformalnych notacji;
8) wyniki analiz bezpieczeństwa podejmowanych w sprawie systemu i oprogramowania;
9) dane na temat wersji systemu oraz innych narzędzi programistycznych służących do kompilacji, w tym dane na temat konfiguracji sprzętu.

Powyższe dowody i argumenty powinny dotyczyć weryfikowanej wersji oprogramowania lub zawierać argumenty potwierdzające relacje zachodzące pomiędzy nimi a weryfikowaną wersją oprogramowania. Ponadto dowody i argumenty powinny być sformułowane klarownie i jednoznacznie zidentyfikowane, a ich zmiany powinny mieć uzasadnienie i być widoczne.

Potwierdzenie braku interferencji funkcji związanych z bezpieczeństwem z innymi funkcjami

Brak interferencji powinien być potwierdzony poprzez wykazanie, iż:

1) wszelkie funkcje oprogramowania nie wynikające z wymagań bezpieczeństwa nie zakłócają działania funkcji związanych z bezpieczeństwem oprogramowania;
2) notacje używane w analizie interferencji są w stanie wspierać wykrywanie i korygowanie wszystkich istotnych mechanizmów interferencji;
3) stosowane metody i techniki analityczne są właściwe dla identyfikacji i analizy mechanizmów zakłóceń/interferencji;
4) założenia przyjęte do analizy (np. środowisko operacyjne, sprzęt, system operacyjny, interfejsy) zostały zatwierdzone przez instytucję;
5) modele wykorzystane do analizy są adekwatną reprezentacją architektury oprogramowania;
6) zastosowano procedury i/lub narzędzia wykrywające i korygujące interferencję;
7) narzędzia wykorzystywane do wspierania wykrywania lub korekcji interferencji nie miały negatywnego wpływu na wyniki lub operacyjność systemu;
8) narzędzia wykorzystywane do wykrywania lub korygowania interferencji zostały zweryfikowane i zatwierdzone przez instytucję.

Dowody i argumenty dla oprogramowania typu COTS

Zaleca się ocenę bezpieczeństwa oprogramowania typu COTS według systemu punktacji przedstawionego w tabeli Tab. 4 określonej w pkt. 5 niniejszych zasad - dla oprogramowania typu COTS $1x10^{-4}$ oraz w Tab. 5 określonej w pkt. 5 niniejszych zasad - dla oprogramowania typu COTS $1x10^{-5}$. Zaproponowany system przewiduje uzyskanie co najmniej 100 punktów świadczących o pomyślnie zakończonej ocenie bezpieczeństwa oprogramowania.

Ponadto dla oprogramowania typu COTS $1x10^{-5}$ zaleca się uzyskanie potwierdzenia:

1) zasadności wymagań bezpieczeństwa;
2) spójności konfiguracji;
3) braku interferencji funkcji związanych z bezpieczeństwem z innymi funkcjami.

Potwierdzenie zasadności wymagań bezpieczeństwa

Dla wykazania, że dostępne argumenty i dowody prawidłowo identyfikują wymogi konieczne i wystarczające do osiągnięcia minimalnego dopuszczalnego poziomu bezpieczeństwa oprogramowania w ramach systemu, zaleca się prowadzenie dokumentacji poświadczającej, że:

1) przeprowadzono analizę bezpieczeństwa systemu, podczas której zidentyfikowano wymagania bezpieczeństwa systemu na poziomie wyposażenia;
2) przeprowadzono analizę wymagań bezpieczeństwa wyposażenia, w celu identyfikacji wymagań bezpiecznych zachowań oprogramowania;
3) przeprowadzono analizę bezpieczeństwa specyfikacji wyposażenia, w celu identyfikacji zachowań zawartych w wymaganiach bezpiecznych zachowań oprogramowania i ustalono, czy nie istnieją inne, dalsze wymagania bezpieczeństwa;
4) stworzono i oceniono macierz zależności pomiędzy analizą bezpieczeństwa specyfikacji wyposażenia a specyfikacją wyposażenia;
5) stworzono i oceniono macierz zależności pomiędzy specyfikacją wyposażenia a specyfikacją oprogramowania.

Potwierdzenie spójności konfiguracji

Dla wykazania spójności konfiguracji zaleca się:

1) jednolite zidentyfikowanie wyposażenia i dokumentów (muszą posiadać unikalne identyfikatory);
2) sporządzenie oświadczenia, że przedstawione dokumenty odnoszą się do weryfikowanej wersji wyposażenia lub, że dokumenty odnoszące się do innej wersji pozostają ważne dla wersji weryfikowanej (wraz z uzasadnieniem).

Potwierdzenie braku interferencji funkcji związanych z bezpieczeństwem z innymi funkcjami

Dla wykazania braku interferencji funkcji związanych z bezpieczeństwem z innymi funkcjami zaleca się prowadzenie dokumentacji poświadczającej:

1) przeprowadzenie testów na poziomie wyposażenia, w tym w zakresie oczekiwanych działań;
2) reputację dostawcy;
3) wysoki poziom szczegółowości przewidywanych zachowań w specyfikacji wyposażenia;
4) prowadzenie wykazów: ujawnionych błędów, znanych problemów, etc.;
5) stosowanie norm i standardów używanych w procesie tworzenia oprogramowania;
6) przeprowadzenie testów interfejsów na różnych poziomach projektu.

Zaleca się uzyskanie od dostawcy oprogramowania dokumentacji na temat stosowanych mechanizmów przeciwdziałających interferencji, w szczególności

1) stosowanych technik unikania wad;
2) stosowanych technik wykrywania wad;
3) używania jednostek zarządzania pamięcią;
4) stosowania „niskich sprzężeń" (*low coupling*) w architekturze oprogramowania;
5) tworzenia oddzielnych zadań dla oprogramowania;
6) wyłączania zbędnych funkcji w systemie operacyjnym.

Deklaracja bezpieczeństwa oprogramowania

Zawartość deklaracji bezpieczeństwa oprogramowania

Zaleca się sporządzanie Deklaracji bezpieczeństwa oprogramowania, która w sposób formalny potwierdzi przeprowadzenie pozytywnej oceny bezpieczeństwa oprogramowania, zgodnie z wymogami określonymi w rozporządzeniu nr 482/2008.

Zaleca się wpisywanie w Deklaracji bezpieczeństwa oprogramowania co najmniej następujących danych:

1) nazwy oprogramowania;
2) rodzaju i typu oprogramowania;
3) nazwy i typu systemu, w którym oprogramowanie będzie wykorzystywane;
4) opisu systemu;
5) nazwy i adresu producenta oprogramowania lub jego autoryzowanego przedstawiciela we Wspólnocie (z podaniem znaku towarowego i pełnego adresu, oraz w przypadku autoryzowanego przedstawiciela, z podaniem znaku towarowego producenta);
6) nazwy podmiotu, który dokonał oceny bezpieczeństwa oprogramowania.

Zaleca się zamieszczanie czytelnego podpisu osoby odpowiedzialnej za ocenę bezpieczeństwa oprogramowania na Deklaracji bezpieczeństwa oprogramowania.

Dokumenty związane z deklaracją bezpieczeństwa oprogramowania

Zaleca się dołączenie do Deklaracji bezpieczeństwa oprogramowania:

1) protokołu przekazania do eksploatacji;
2) kopii analizy bezpieczeństwa systemu;
3) raportów z testów funkcjonalnych i technicznych*;
4) specyfikacji oprogramowania*;
5) specyfikacji funkcjonalno-technicznej systemu*;
6) ocen oprogramowania typu COTS, w szczególności przeprowadzonych według stosownych tabel określonych w pkt. 5 do niniejszych zasad.

Tabele: Tab. 1 Formy dowodów

AEL	Dowody wynikające z testów	Dowody wynikające z doświadczenia służb	Dowody analityczne
5	Kryteria testu Specyfikacja testu Wyniki testu Oświadczenie – wybór najlepszych praktyk/ norm / narzędzi Oświadczenie – wszystkie badania spełniają kryteria / uzasadnienie niedotrzymania kryteriów Oświadczenie – weryfikacja i zatwierdzenie narzędzi i procedur	Oświadczenie – zakres zgromadzonej przez służby dokumentacji wspiera określone twierdzenia Oświadczenie – oprogramowanie odpowiada twierdzeniom służb Oświadczenie – środowisko operacyjne odpowiada twierdzeniom służb Oświadczenie – zakres zgromadzonej przez służby dokumentacji jest kompletny i poprawny	Oświadczenia – wybór najlepszych praktyk / standardów / technik / narzędzi/ notacji Oświadczenie – analiza prezentuje, że kryteria są spełnione dla wszystkich atrybutów /uzasadnienie niespełnienia kryteriów Oświadczenie – weryfikacja i zatwierdzanie poprawności narzędzi
4	Raport – weryfikacja wykorzystania standardów/ wytycznych / narzędzi Raport – analiza błędów narzędzi i procedur Opracowanie i uzasadnienie specjalnego projektu testów	Zgromadzona przez służby dokumentacja Procedura DRACAS (*Data Reporting Analysis and Corrective Action System*) Raport – analiza błędów narzędzi i procedur	Wyniki analizy Raport – weryfikacja wykorzystania wytycznych/ standardów/ zapisów/ technik/ narzędzi/ notacji Opracowane i uzasadnione procesu określającego rozwój projektu Zasady dotyczące pracowników oraz ich kompetencje (wraz z uzasadnieniem) Raport – analiza błędów narzędzi

* Dokument w wersji elektronicznej.

3	Raport – weryfikacja kryteriów testowych Sprawozdanie – ocena wyników badań Sprawozdanie – adekwatność danych testowych (w tym uzasadnienie pokrycia) Raport – weryfikacja wykorzystania specjalnego projektu badania procesów Raport – weryfikacja i zatwierdzanie narzędzi i procedur	Raport – analiza zakresu twierdzeń służb Raport – analiza podobieństwa oprogramowania / uzasadnienie różnic Raport – analiza podobieństwa środowiska operacyjnego / uzasadnienie różnic Raport – weryfikacja użycia DRACAS oraz narzędzi wspierających	Raport – weryfikacja kryteriów Raport – ocena wyników Raport – ocena procesu rozwoju (wszystkie możliwe środki zostały podjęte w celu zapewnienia, że produkt jest wolny od błędów) Raport – adekwatność kryteriów (w tym uzasadnienie pokrycia) Raport – weryfikacja wykorzystania konkretnych procesów w rozwoju projektu Raport – weryfikacja i zatwierdzanie narzędzi Raport – weryfikacja kompetencji personelu
2	Ocena testów przez niezależny departament	Ocena przeprowadzonej analizy, zweryfikowana oraz uzasadniona przez niezależny departament	Ocena przeprowadzona przez niezależny departament
1	Ocena testów przez niezależną organizację	Ocena przeprowadzonej analizy, zweryfikowana oraz uzasadniona przez niezależną organizację	Ocena przeprowadzona przez niezależną organizację

UWAGI!

1. Powyższe dowody się kumulują. Oznacza to, że wszystkie dowody dla wyższego AEL powinny być zawarte w dowodach niższego AEL.
2. W przypadku badań statystycznych lub w dziedzinie doświadczenia argumenty należy potwierdzić na poziomie ufności równym 95%.
3. Dla AEL 3 do 5, wszelkie różnice między środowiskiem operacyjnym a testowym są identyfikowane, a ich wpływ na ocenę wyników badań musi zostać ujęty w raporcie.
4. Dla AEL 1 i 2, badania wykonywane są dla identycznej jak docelowa konfiguracji operacyjnej systemu.

Tab. 2 Źródła dowodów

AEL	**Akceptowalne źródła dowodów** *(należy wybrać tylko jedną kolumnę dla danego wiersza)*			
Wymagania funkcjonalne; Wymagania czasowe; Odporność na nietypowe warunki operacyjne				
5	TESTOWANIE	DOŚWIADCZENIE SŁUŻB, Testowanie		ANALIZA, Testowanie
4	TESTOWANIE	DOŚWIADCZENIE SŁUŻB, Testowanie		ANALIZA, Testowanie
3	ANALIZA, Testowanie		ANALIZA, Testowanie, Doświadczenie służb	
2	ANALIZA, Testowanie		ANALIZA, Testowanie, Doświadczenie służb	
1	ANALIZA, Testowanie			
Niezawodność				
5	TESTOWANIE	DOŚWIADCZENIE SŁUŻB, Testowanie	ANALIZA, Testowanie	ANALIZA, Doświadczenie służb, Testowanie
4	TESTOWANIE	DOŚWIADCZENIE SŁUŻB, Testowanie	ANALIZA, Testowanie	ANALIZA, Doświadczenie służb, Testowanie
3	DOŚWIADCZENIE SŁUŻB, Testowanie	ANALIZA, Testowanie	ANALIZA, Testowanie, Doświadczenie służb	
2	ANALIZA, Testowanie		ANALIZA, Testowanie, Doświadczenie służb	
1	ANALIZA, Testowanie, Doświadczenie służb			

Dokładność; Wykorzystanie zasobów docelowej platformy sprzętowej				
5	TESTOWANIE	DOŚWIADCZENIE SŁUŻB, Analiza, Testowanie	ANALIZA, Testowanie	ANALIZA, Doświadczenie służb, Testowanie
4	TESTOWANIE, Analiza	ANALIZA, Doświadczenie służb, Testowanie		ANALIZA, Testowanie
3	ANALIZA, Testowanie		ANALIZA, Doświadczenie służb, Testowanie	
2	ANALIZA, Testowanie			
1	ANALIZA, Testowanie			
Tolerancja na przeciążenia				
5	TESTOWANIE	DOŚWIADCZENIE SŁUŻB, Analiza, Testowanie	ANALIZA, Testowanie	ANALIZA, Doświadczenie służb, Testowanie
4	TESTOWANIE, Analiza	ANALIZA, Doświadczenie służb, Testowanie		ANALIZA, Testowanie
3	TESTOWANIE, Analiza	ANALIZA, Doświadczenie służb, Testowanie		ANALIZA, Testowanie
2	ANALIZA, Testowanie (deterministyczny projekt przeciążenia)		TESTOWANIE, Analiza (niedeterministyczny projekt przeciążenia)	
1	ANALIZA, Testowanie (deterministyczny projekt przeciążenia)		TESTOWANIE, Analiza (niedeterministyczny projekt przeciążenia)	

Tab. 3 Zakres testów i analiz

Atrybuty zachowań oprogramowania	Testy	Doświadczenie służb	Analizy
Wymagania funkcjonalne	Testy funkcjonalne	Analiza znanych wad produktu	Formalny dowód poprawnego działania
Wymagania czasowe	Testy czasu reakcji Testy maksymalnej wydajności	Analiza znanych wad produktu	Analiza najgorszego przypadku czasowego Modelowanie wydajności
Odporność na nietypowe warunki operacyjne	Wprowadzanie błędnych danych (wewnętrzne i i/o) Testy uszkodzenia zasilania i wyposażenia	Dowody w postaci raportów z incydentów na skuteczność środków podnoszących odporność na uszkodzenia	Dowody na poparcie, że wewnętrzne i zewnętrzne nieprawidłowości zostaną wykryte oraz, że odpowiednie akcje zostaną podjęte
Niezawodność	Testy niezawodności (użycie oczekiwanego profilu operacyjnego) Dowody z testów wysokiego pokrycia	Pomiaru zakresu niezawodności (na podstawie zbliżonego profilu operacyjnego) Szacunki oparte na znanych wadach i czasie pracy operacyjnej już działających zbliżonych aplikacji	Dowody potwierdzające niskie prawdopodobieństwo wystąpienia wad (wynikające z analizy procesów i produktu) np. analiza statyczna, analiza zgodności, miara złożoności, jakość narzędzi wsparcia Gęstość błędów w podobnych projektach.
Dokładność	Błędy pomiarów dla znanych przypadków testowych	Analiza znanych wad produktu	Analiza numeryczna Analiza stabilności algorytmu
Wykorzystanie zasobów docelowej platformy sprzętowej	Testy przypadków największego obciążenia (dyski, pamięć operacyjna, wejścia/wyjścia, kanały komunikacji, procesor)	Dane uzyskane z monitorowania wykorzystania zasobów przez inne zbliżone aplikacje	Model dokumentacji ze statycznego przydzielenia zasobów startowych. Analiza przypadku najgorszego wykorzystania zasobów
Tolerancja na przeciążenia	Testy nadmiernego obciążenia	Analiza znanych wad produktu	Dowody, że system w warunkach przeciążenia będzie stopniowo ulegał degradacji

Tab. 4 Oceny dla COTS $1x10^{-4}$

Zintegrowane punkty oceny oprogramowania COTS 1 x 10^{-4}					
Wyszczególnienie	**Ilość punktów wg kryteriów**			**Dowody**	**Liczba uzyskanych punktów**
Testowanie				Wykonany test = przyznanie punktów; maksymalnie: 90	
Factory Acceptance Test	20			1. Skrypt testu; 2. Wyniki testu; 3. Test Traceability matrix. Wszystkie wymagania związane z funkcjami bezpieczeństwa muszą być przetestowane (SAT lub FAT). Test musi obejmować skrajne warunki, w jakich system ma działać.	
Site Acceptance Test	20				
ANSP Soak Test i obserwacje późniejsze w czasie:	*1 tydzień*	*2 tygodnie*	*1 miesiąc*		
Uruchomienie systemu na określony czas (bez resetowania), podczas którego są wprowadzane dane wejściowe odpowiadające zakresowi normalnej pracy. Test przeprowadzany po teście funkcjonalnym.	50	60	70	1. Skrypt testu; 2 .Wyniki testu	
Korzystanie z systemu (praca testowa) w czasie:	*1 tydzień*	*2 tygodnie*	*1 miesiąc*		
Korzystanie z systemu i brak nieprawidłowości w jego działaniu.	20	30	40	Dowód, że system był używany i żadne nieprawidłowości nie zostały wykryte.	
Test wykonywany przez dostawcę w czasie:	*1 miesiąc*	*2 miesiące*	*6 miesięcy*		
Test przeprowadzany po teście funkcjonalnym.	50	55	60	1. Skrypt testu; 2. Wyniki testu	
ŁĄCZNIE					
Doświadczenie służb	Tylko jeden z poniższych elementów może być wykorzystany;				
Takie samo oprogramowanie na takiej samej platformie	*1 rok*	*5 lat*	*10 lat*		
	10	40	80	1. Oświadczenie o budowie wyposażenia (dowody od dostawcy na to, że 100% kodu aplikacji pozostało niezmienione oraz platforma sprzętowa jest taka sama) 2. Oświadczenie o zaobserwowanych awariach (wszelkie błędy powodujące niespełnienie wymagań bezpieczeństwa skutkują nie przyznaniem punktów); 3. Lokalizacja spełnia warunki podobnego środowiska pracy.	
Oprogramowanie o zbliżonej wersji na takiej samej platformie	*1 rok*	*5 lat*	*10 lat*		
	10	30	65	1. Oświadczenie o budowie wyposażenia (dowody od dostawcy na to, że 95% kodu aplikacji pozostało niezmienione); 2. Oświadczenie o zaobserwowanych awariach (wszelkie błędy powodujące niespełnienie wymagań bezpieczeństwa skutkują nie przyznaniem punktów); 3. Lokalizacja spełnia warunki podobnego środowiska pracy.	
Takie samo oprogramowanie na zbliżonej platformie (system operacyjny i/lub hardware)	*1 rok*	*5 lat*	*10 lat*		
	4	16	32	1. Oświadczenie o budowie wyposażenia (dowody od dostawcy na to, że 100% kodu aplikacji pozostało niezmienione - wyłączając system operacyjny i sterowniki); 2. Oswiadczenie o zaobserwowanych awariach (wszelkie błędy powodujące niespełnienie wymagań bezpieczeństwa skutkują nie przyznaniem punktów); 3. Lokalizacja spełnia warunki podobnego środowiska pracy.	
Takie samo oprogramowanie na innej platformie (system operacyjny i/lub hardware)	*1 rok*	*5 lat*	*10 lat*		
	2	8	16	1. Oświadczenie o budowie wyposażenia (dowody od dostawcy na to, że 95% kodu aplikacji pozostało niezmienione); 2. Oświadczenie o zaobserwowanych awariach (wszelkie błędy powodujące niespełnienie wymagań bezpieczeństwa skutkują nie przyznaniem punktów); 3. Lokalizacja spełnia warunki podobnego środowiska pracy.	
Podobne oprogramowanie od tego samego dostawcy	*1 rok*	*5 lat*	*10 lat*		
	0	0	5	Dowody na odpowiednio niską częstotliwość błędów związanych z ponownie użytym kodem aplikacji. Minimum 5% ponownie użytego kodu.	
ŁĄCZNIE					
Doświadczenie dostawcy oraz ekspertyzy	Maksymalnie można uzyskać 20 punktów				
Dostawca ma doświadczenie w rozwoju i wprowadzaniu tego typu oprogramowania na rynku ATM	*5 lat*	*10 lat*	*15 lat*		
	5	10	15	Dowodów dostawcy na sukcesy w danym sektorze rynku.	
Personel dostawcy wykazał się specjalistyczną wiedzą	Niskie zaufanie	Średnie zaufanie	Wysokie zaufanie		
	10	15	20	Dowody w postaci CV kluczowych osób zaangażowanych w projekt	
Dostawca projekt/rozwój	Maksymalnie można uzyskać 30 punktów				
Dostawca może przedstawić pomyślnie przeprowadzenie odpowiednich procesów w cyklu życia oprogramowania	Poniżej zalecanego poziomu	Na zalecanym poziomie	Powyżej zalecanego poziomu		
Procesy zgodne z EC 61508, ED 109 lub inną normą. Normy te zalecają poziomy rygorystyczności procesów cyklu życia oprogramowania.	10	25	30	1. Certyfikat zgodności produktu **LUB** 2. Niezależny audyt zgodności **LUB** 3. Niezależny audyt zasadności procedur dostawcy	
Wiedza na temat wewnętrznych cech konstrukcyjnych (funkcji), które zostały wprowadzone w celu ograniczenia możliwości niepożądanego działania systemu	Niektóre funkcje	Wszystkie funkcje			
Funkcje systemowe, takie jak ograniczenie zakresu danych wejściowych lub usuwanie niepotrzebnych elementów systemu operacyjnego w celu zapewnienia znacznie większej pewność, że system będzie działać prawidłowo.	5	10		Dowody potwierdzające skuteczność funkcji. UWAGA: Jeżeli rozwiązania systemowe zostały potwierdzone na poziomie oprogramowania, to dowody muszą prezentować ich powiązania z wymaganiami funkcjonalnymi.	
ŁĄCZNIE					
R A Z E M					

Tab. 5 Oceny dla COTS $1x10^{-5}$

Zintegrowane punkty oceny oprogramowania COTS 1×10^{-5}					
Wyszczególnienie	**Ilość punktów wg kryteriów**			**Dowody**	**Liczba uzyskanych punktów**
Testowanie				Wykonany test = przyznanie punktów; maksymalnie: 75	
Factory Acceptance Test	10			1.Skrypt testu; 2.Wyniki testu; 3.Test Traceability matrix. Wszystkie wymagania związane z funkcjami bezpieczeństwa muszą być przetestowane (SAT lub FAT). Test musi obejmować skrajne warunki, w jakich system ma działać.	
Site Acceptance Test	10				
ANSP Soak Test i obserwacje późniejsze w czasie:	*1 tydzień*	*2 tygodnie*	*1 miesiąc*		
Uruchomienie systemu na określony czas (bez resetowania), podczas którego są wprowadzane dane wejściowe odpowiadające zakresowi normalnej pracy. Test przeprowadzany po teście funkcjonalnym.	30	35	40	1.Skrypt testu; 2.Wyniki testu	
Korzystanie z systemu (praca testowa) w czasie:	*1 tydzień*	*2 tygodnie*	*1 miesiąc*		
Korzystanie z systemu i brak nieprawidłowości w jego działaniu.	10	15	20	Dowód, że system był używany i żadne nieprawidłowości nie zostały wykryte.	
Test wykonywany przez dostawcę w czasie:	*1 miesiąc*	*2 miesiące*	*6 miesięcy*		
Test przeprowadzany po teście funkcjonalnym.	30	35	40	1.Skrypt testu; 2.Wyniki testu	
ŁĄCZNIE					
Doświadczenie służb	Tylko jeden z poniższych elementów może być wykorzystany;				
Takie samo oprogramowanie na takiej samej platformie	*1 rok*	*5 lat*	*10 lat*		
	10	40	80	1. Oświadczenie o budowie wyposażenia (dowody od dostawcy na to, że 100% kodu aplikacji pozostało niezmienione oraz platforma sprzętowa jest taka sama) 2. Oświadczenie o zaobserwowanych awariach (wszelkie błędy powodujące niespełnienie wymagań bezpieczeństwa skutkują nie przyznaniem punktów); 3. Lokalizacja spełnia warunki podobnego środowiska pracy.	
Oprogramowanie o zbliżonej wersji na takiej samej platformie	*1 rok*	*5 lat*	*10 lat*		
	10	30	65	1. Oświadczenie o budowie wyposażenia (dowody od dostawcy na to, że 95% kodu aplikacji pozostało niezmienione); 2. Oświadczenie o zaobserwowanych awariach (wszelkie błędy powodujące niespełnienie wymagań bezpieczeństwa skutkują nie przyznaniem punktów); 3. Lokalizacja spełnia warunki podobnego środowiska pracy.	
Takie samo oprogramowanie na zbliżonej platformie (system operacyjny i/lub hardware)	*1 rok*	*5 lat*	*10 lat*		
	4	16	32	1. Oświadczenie o budowie wyposażenia (dowody od dostawcy na to, że 100% kodu aplikacji pozostało niezmienione - wyłączając system operacyjny i sterowniki); 2. Oświadczenie o zaobserwowanych awariach (wszelkie błędy powodujące niespełnienie wymagań bezpieczeństwa skutkują nie przyznaniem punktów); 3. Lokalizacja spełnia warunki podobnego środowiska pracy.	
Takie samo oprogramowanie na innej platformie (system operacyjny i/lub hardware)	*1 rok*	*5 lat*	*10 lat*		
	2	8	16	1. Oświadczenie o budowie wyposażenia (dowody od dostawcy na to, że 95% kodu aplikacji pozostało niezmienione); 2. Oświadczenie o zaobserwowanych awariach (Wszelkie błędy powodujące niespełnienie wymagań bezpieczeństwa skutkują nie przyznaniem punktów); 3. Lokalizacja spełnia warunki podobnego środowiska pracy.	
Podobne oprogramowanie od tego samego dostawcy	*1 rok*	*5 lat*	*10 lat*		
	0	0	5	Dowody na odpowiednio niską częstotliwość błędów związanych z ponownie użytym kodem aplikacji. Minimum 5% ponownie użytego kodu.	
ŁĄCZNIE					
Doświadczenie dostawcy oraz ekspertyzy	Maksymalnie można uzyskać 20 punktów				
Dostawca ma doświadczenie w rozwoju i wprowadzaniu tego typu oprogramowania na rynku ATM	*5 lat*	*10 lat*	*15 lat*		
	5	10	15	Dowodów dostawcy na sukcesy w danym sektorze rynku.	
Personel dostawcy wykazał się specjalistyczną wiedzą	Niskie zaufanie	Średnie zaufanie	Wysokie zaufanie		
	10	15	20	Dowody w postaci CV kluczowych osób zaangażowanych w projekt	
Dostawca projekt/rozwój	Maksymalnie można uzyskać 30 punktów				
Dostawca może przedstawić pomyślnie przeprowadzenie odpowiednich procesów rozwojowych w rozwoju oprogramowania	Poniżej zalecanego poziomu	Na zalecanym poziomie	Powyżej zalecanego poziomu		
Procesy zgodne z EC 61508, ED 109 lub inną normą. Normy te zalecają poziomy rygorystyczności procesów cyklu życia oprogramowania.	10	25	30	1. Certyfikat zgodności produktu **LUB** 2. Niezależny audyt zgodności **LUB** 3. Niezależny audyt zasadności procedur dostawcy	
Wiedza na temat wewnętrznych cech konstrukcyjnych (funkcji), które zostały wprowadzone w celu ograniczenia możliwości niepożądanego działania systemu	Niektóre funkcje	Wszystkie funkcje			
Funkcje systemowe, takie jak ograniczenie zakresu danych wejściowych lub usuwanie niepotrzebnych elementów systemu operacyjnego w celu zapewnienia znacznie większej pewność, że system będzie działać prawidłowo.	5	10		Dowody potwierdzające skuteczność funkcji. UWAGA: Jeżeli rozwiązania systemowe zostały potwierdzone na poziomie oprogramowania, to dowody muszą prezentować ich powiązania z wymaganiami funkcjonalnymi **oraz wymaganiami bezpieczeństwa systemu.**	
ŁĄCZNIE					
R A Z E M					