ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ **Nr 279**
Mechanika z. 83 (2/11) **2011**

Edward BABIASZ
Instytut Lotnictwa w Warszawie

PRZEWODNIK ZAPEWNIENIA BEZPIECZEŃSTWA W KONSTRUKCJACH POKŁADOWYCH URZĄDZEŃ ELEKTRONICZNYCH – DOKUMENT RTCA DO-254/ED-80 EUROCAE

Praca stanowi krótkie omówienie istotnego dokumentu RTCA DO-254/ED-80: Przewodnik zapewnienia bezpieczeństwa w konstrukcjach pokładowych urządzeń elektronicznych. Wytyczne zawarte w tym dokumencie mają służyć producentom statków powietrznych i dostawcom wyposażenia elektronicznego systemów pokładowych. Opisano w nich procedury poszczególnych etapów cyklu projektowania wyposażenia. Określono cele i działania w ramach każdej procedury. Podobnie jak w dokumencie DO-178B/ED-12B dotyczącym oprogramowania, przyjęto pięć kategorii wyposażenia ze względu na wymagane bezpieczeństwo konstrukcji. Wytyczne mają zastosowanie dla każdego przyjętego poziomu bezpieczeństwa konstrukcji.

Wstęp

Rozwój i zastosowanie złożonych systemów elektronicznych w lotnictwie wywołało nowe problemy związane z bezpieczeństwem i certyfikacją. W odpowiedzi na nie powołano stosowne, współpracujące komisje SC-180 RTCA i WG-46 EUROCAE. Ten wspólny komitet został zobowiązany do opracowania jasnych i zwartych wytycznych dla konstrukcji pokładowego wyposażenia elektronicznego, tak by bezpiecznie realizowane były zamierzone funkcje. W wyniku tych prac powstał dokument DO-254/ED-80 [1, 2]. Jest to jeden z ważniejszych dokumentów RTCA. Mimo że został on wydany w 2000 r., chyba nie zakorzenił się jeszcze w świadomości krajowej braci awionicznej. Przywoływany jest już jednak w najnowszych wydaniach norm przedmiotowych (TSO, ETSO).

Wytyczne zawarte w niniejszym dokumencie mają służyć producentom statków powietrznych i dostawcom wyposażenia elektronicznego systemów pokładowych. Opisano w nich procedury poszczególnych etapów cyklu projektowania wyposażenia. Określono cele i działania w ramach każdej procedury. Podobnie jak w dokumencie DO-178B/ED-12B dotyczącym oprogramowania, przyjęto pięć kategorii wyposażenia ze względu na wymagane bezpieczeństwo

konstrukcji. Wytyczne mają zastosowanie dla każdego przyjętego poziomu bezpieczeństwa konstrukcji.

Zastosowanie znacznie bardziej skomplikowanych urządzeń elektronicznych, wypełniających coraz więcej funkcji krytycznych dla bezpieczeństwa statku powietrznego, stanowi nowe wyzwanie dla bezpieczeństwa lotu i certyfikacji. Aby przeciwdziałać temu świadomemu wzrostowi ryzyka, niezbędne staje się zapewnienie, że potencjalne błędy konstrukcji urządzeń są możliwe do zlokalizowania w bardziej ścisły i weryfikowalny sposób, zarówno w procesie projektowania, jak i certyfikacji.

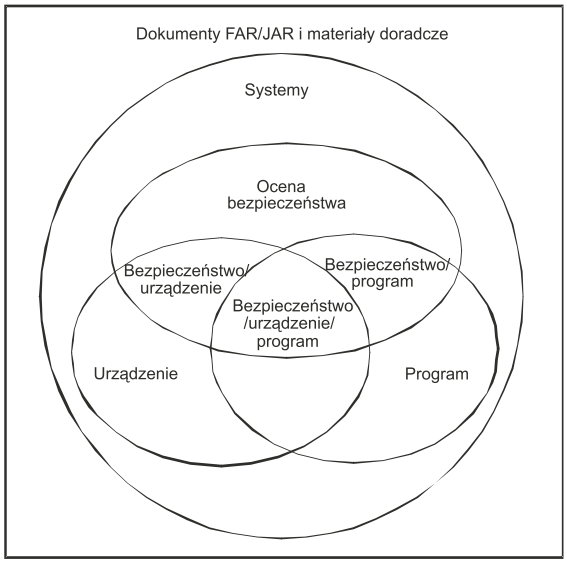
Realizowane są trzy procesy oceny bezpieczeństwa systemu: ocena ryzyka funkcjonalnego (FHA), wstępna ocena bezpieczeństwa systemu (PSSA) i ocena bezpieczeństwa systemu (SSA). Procesy te wykorzystywane są do określenia wskaźników i parametrów bezpieczeństwa systemu stosownie do etapu procesu zapewnienia bezpieczeństwa oraz do ustalenia, czy funkcje systemu osiągnęły zadane parametry bezpieczeństwa. Przyjęte skróty pochodzą od angielskich nazw dokumentów i procesów.

1. Aspekty systemowe zapewnienia bezpieczeństwa konstrukcji

Zapewnienie bezpieczeństwa konstrukcji na poziomie systemu zaczyna się od przyporządkowania funkcji systemu do urządzenia i przyporządkowania im odpowiednich poziomów zapewnienia bezpieczeństwa konstrukcji. Poszczególna funkcja systemu może być związana z jednostkowym urządzeniem, oprogramowaniem lub kombinacją urządzenia i oprogramowania. Wymagania bezpieczeństwa związane z daną funkcją widziane z perspektywy systemu, oprogramowania czy urządzenia definiują wybrany poziom niezawodności i zapewnienia bezpieczeństwa konieczny do spełnienia tych wymagań (rys. 1.).

Przyjęto pięć poziomów zapewnienia bezpieczeństwa rozwoju systemu – od A do E, odpowiadających pięciu klasom sytuacji awaryjnych wynikających z uszkodzeń: katastroficznej, wysoce ryzykownej, niebezpiecznej, umiarkowanie niebezpiecznej i bez konsekwencji.

Na etapie wstępnym poziom zapewnienia bezpieczeństwa konstrukcji dla każdej funkcji urządzenia określany jest w procesie oceny bezpieczeństwa systemu (SSA) z wykorzystaniem oceny ryzyka funkcjonalnego (FHA) do identyfikacji potencjalnych zagrożeń. Następnie proces wstępnej oceny bezpieczeństwa systemu (PSSA) przypisuje wymagania bezpieczeństwa i powiązane sytuacje awaryjne do funkcji realizowanych w urządzeniu. W procesie projektowania mogą występować iteracyjne sprzężenia między procesami zapewnienia bezpieczeństwa, rozwoju systemu i urządzenia. Umożliwia to uzyskanie pewności, że zaprojektowane i wykonane urządzenie spełni zarówno wymagania bezpieczeństwa systemu, jak i te dotyczące funkcji i właściwości przypisanych do urządzenia (rys. 2.).



Rys. 1. Zależności między procesem projektowania systemów wyposażenia pokładowego a procesami oceny bezpieczeństwa, projektowania urządzenia i rozwoju oprogramowania

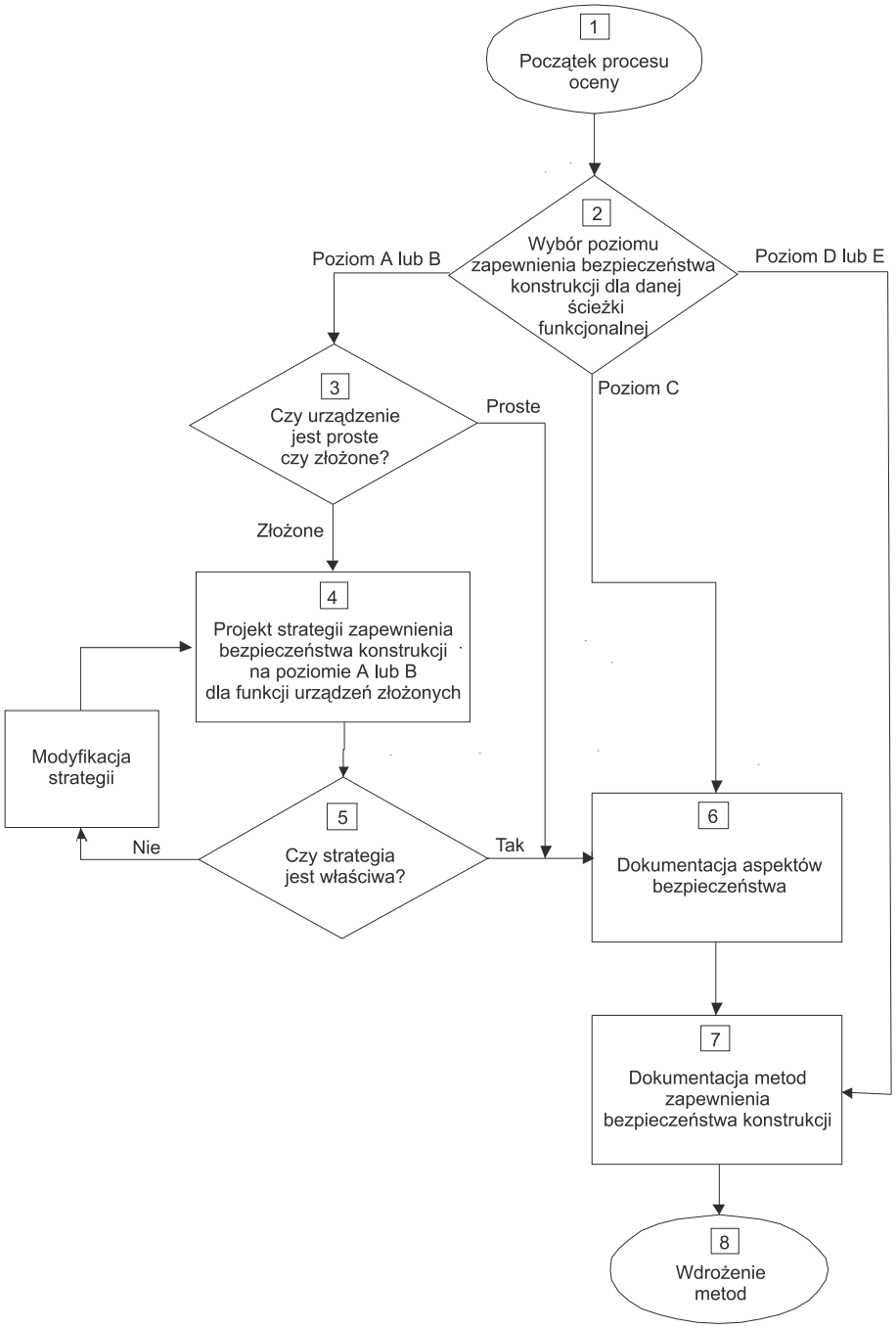
2. Proces projektowania urządzenia

W procesie projektowania urządzenia można wyróżnić następujące etapy:

1. Etap planowania określający i wzajemnie koordynujący działania w projektowaniu urządzenia i procesów wspomagających.
2. Etap konstruowania urządzenia generujący dane projektowe i kończący się wytworzeniem urządzenia. Na tym etapie następuje sformułowanie wymagań, prace koncepcyjne, konstruowanie, wykonanie urządzenia i przekazanie go do produkcji.
3. Procesy wspomagające wypracowujące dane z przebiegu procesu projektowania, które potwierdzają prawidłowość i właściwe kierowanie procesem projektowania urządzenia i materiałami uzyskiwanymi na wyjściu, z włączeniem planowania, konstruowania, oceny bezpieczeństwa i procesów wspomagających. Procesy te są realizowane współbieżnie z etapami planowania i konstruowania. Do procesów tych należą: walidacja, weryfikacja, zarządzanie konfiguracją, zapewnienie bezpieczeństwa i uzyskanie certyfikacji.

3. Proces planowania

Celem etapu planowania urządzenia jest zdefiniowanie środków stosowanych do przetwarzania wymagań funkcjonalnych i zdatności do lotu w konkretnym urządzeniu przy akceptowalnej ilości dowodów zapewnienia, że urządzenie będzie bezpiecznie realizować założone funkcje.



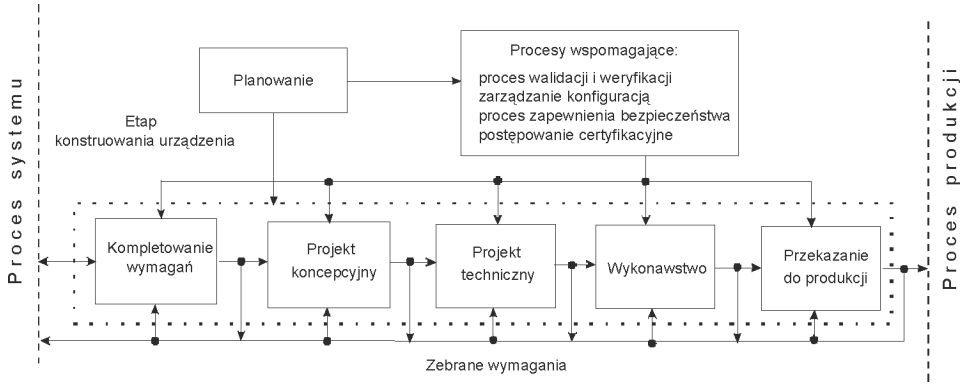
Rys. 2. Proces podejmowania decyzji przy wyborze strategii zapewnienia bezpieczeństwa konstrukcji urządzenia

Zadania na etapie planowania konstrukcji polegają na:

- zdefiniowaniu procesu projektowania urządzenia (opis działań, punkty decyzyjne, wejścia, wyjścia, podział odpowiedzialności),
- wyborze przydatnych norm,
- wyborze lub określeniu warunków środowiskowych dla konstrukcji,
- wyborze środków wykazania zgodności z wymaganymi parametrami bezpieczeństwa konstrukcji, z uwzględnieniem przyjętych strategii proponowanych organowi certyfikującemu,
- przyjęciu środków służących do uzyskania koordynacji między procesami projektowania urządzenia a procesami pomocniczymi, ze szczególnym uwzględnieniem działań związanych z systemami, oprogramowaniem i certyfikacją statku powietrznego,
- zdefiniowaniu działań dla każdego etapu procesu projektowania urządzenia i związanego z nim procesu pomocniczego,
- wyborze środowiska projektowego, a w tym narzędzi, procedur, oprogramowania i oprzyrządowania, jakie będą wykorzystane do opracowania, weryfikacji i kontroli urządzenia i danych z przebiegu projektowania,
- przyjęciu zasad dokonywania zmian ustalonych planów, jeżeli okażą się one konieczne i jeżeli wpływają na certyfikację.

4. Proces konstruowania urządzenia

Proces konstruowania urządzenia polega na wytworzeniu konkretnego urządzenia, które będzie spełniać wymagania systemu przypisane do urządzenia. W pracy opisano pięć podstawowych faz: skompletowanie wymagań, projekt koncepcyjny, projekt techniczny, wykonanie prototypów i przekazanie do produkcji (rys. 3., tab. 1.).



Rys. 3. Przebieg procesu projektowania urządzenia

Każdy proces i każde oddziaływanie między procesami może mieć charakter iteracyjny. Dla każdej iteracji rezultat zmian na każdy z procesów powinien być oceniany przez wpływ na wyniki poprzedniej iteracji i w powiązaniu z nią.

Do dobrej praktyki inżynierskiej należy dokumentowanie zdarzeń i obserwacji z procesu konstruowania w formie notatek, zapisów z przeglądu konstrukcji, książki problemów przez cały proces projektowania. Obecna praktyka inżynierska dostarcza wiele różnych środków – graficznych, matematycznych, opartych na bazach danych lub tekście, służących do przedstawiania, zapisu, prezentacji konstrukcji i opisu wymagań.

Tabela 1. Typowy proces projektowania elementów ASIC/PLD

Typowy proces projektowania ASIC/PLD	**Proces**
Udział na wyższym poziomie planowania	Planowanie
Decyzje dotyczące architektury ASIC/PLD	Ocena bezpieczeństwa
Kompletowanie wymagań ASIC/PLD	Kompletowanie wymagań
Projektowanie wstępne ASIC/PLD z włączeniem projektowania behawioralnego uwzględniającego potrzeby i wymagania użytkowników	Projekt koncepcyjny
Projekt techniczny ASIC/PLD zawierający pliki złożeniowe, masek i zabezpieczeń	Projekt techniczny
Wykonanie ASIC/PLD, z włączeniem wykonania na zewnątrz, oraz badań i programowania elementów programowalnych	Wykonawstwo
Przekazanie do produkcji ASIC/PLD	Przekazanie do produkcji
Walidacja i weryfikacja ASIC/PLD z włączeniem analiz czasowych, symulacji zachowań, symulacji poziomów bramek	Proces walidacji i weryfikacji
Zarządzanie konfiguracją ASIC/PLD z włączeniem bazy danych narzędzi i części	Proces zarządzania konfiguracją

5. Proces walidacji i weryfikacji

Proces walidacji w swym zamierzeniu ma udowodnić, za pomocą obiektywnych i subiektywnych metod, że sformułowane wymagania są poprawne i kompletne w odniesieniu do wymagań systemu przypisanych do urządzenia. Walidacja może być prowadzona przed, jak i po wykonaniu urządzenia; walidacja zazwyczaj jest prowadzona w trakcie całego cyklu projektowania.

Proces weryfikacji daje gwarancję, że wykonane urządzenie spełnia wymagania. Weryfikacja składa się z przeglądów, analiz i badań wykonanych zgodnie z planem weryfikacji. W ramach tego procesu należy dokonać oceny uzyskanych rezultatów.

Proces weryfikacji może być realizowany na dowolnym etapie konstruowania, zgodnie z planem weryfikacji. W przypadku wymagań bezpieczeństwa stosowanie procesu weryfikacji na różnych etapach konstruowania jest korzystne ze

względu na wzrost prawdopodobieństwa (w wysokim stopniu), że nastąpi wyeliminowanie błędów konstrukcyjnych. Dla niektórych poziomów zapewnienia bezpieczeństwa konstrukcji wymagane jest, aby oczekiwane rezultaty procesu weryfikacji były sprawdzone przez czynnik niezależny.

Procesy weryfikacji oprogramowania, integracji między oprogramowaniem a urządzeniem oraz integracji systemów nie zostały opisane (sferę tę obejmuje dokument DO-178B). Jednakże weryfikacja wymagań dla urządzenia w trakcie tych procesów jest uprawomocnioną metodą weryfikacji urządzenia.

6. Proces zarządzania konfiguracją

Proces zarządzania konfiguracją służy zapewnieniu możliwości powtarzalnego odtwarzania urządzenia w danym, szczególnym wariancie wykonania, odtwarzania informacji w miarę potrzeby i modyfikowania danego wariantu wykonania w sposób kontrolowany. W artykule opisano spodziewane wyniki procesu zarządzania konfiguracją i działania, które wspierają dążenia do tych rezultatów.

Wytyczne dotyczące działań w procesie zarządzania konfiguracją

1. Warianty wykonania urządzenia powinny być jednoznacznie zidentyfikowane, udokumentowane i nadzorowane. Może to dotyczyć (ale nie tylko) urządzenia, zapisu konstrukcji urządzenia, narzędzi i innych danych wykorzystywanych do uzyskania certyfikatu oraz wzorców bazowych, wyjściowych.

2. Należy ustalić wzorce bazowe, wyjściowe.

3. Problemy należy jednoznacznie zidentyfikować, prześledzić i opisać.

4. Należy utrzymywać nadzór nad zmianami odtworzenia ścieżki przebiegu zmian. Wymagane jest zachowanie danych z przebiegu projektowania wyszczególnionych w planach i zapewnienie możliwości ich odszukania.

5. Należy zapewnić nadzór nad archiwizowaniem, zasadami odszukiwania i udostępniania materiałów dotyczących konfiguracji.

Zdefiniowano dwie kategorie związane z zarządzaniem konfiguracją danych: kategoria nadzoru urządzenia 1 (HC1) i kategoria nadzoru urządzenia 2 (HC2). Stworzenie dwóch kategorii pozwala na mniej sztywny nadzór nad konfiguracją dla pewnych rodzajów danych. Kategoria HC1 wymaga przeprowadzenia wszystkich działań zarządzania konfiguracją, kategoria HC2 jest mniej restrykcyjna.

7. Proces zapewnienia bezpieczeństwa

Proces zapewnienia bezpieczeństwa ma zagwarantować osiągnięcie założonych rezultatów procesu projektowania, zrealizowanie działań nakreślonych

w planach i uzasadnienie odstępstw. Opisano spodziewane wyniki procesu zapewnienia bezpieczeństwa oraz działania, które służą ich osiągnięciu.

Nie sugeruje się specyficznych, konkretnych rozwiązań organizacyjnych. Aby dokonać obiektywnej oceny procesów, działania procesu zapewnienia bezpieczeństwa należy realizować przy zagwarantowaniu niezależności.

Działania procesu zapewnienia bezpieczeństwa

1. Należy zapewnić dostępność planów związanych z urządzeniem, zgodnie z postanowieniami rozdziału dotyczącego procesu planowania w niniejszym dokumencie i uzgodnieniami zawartymi w planie sprzętowych aspektów certyfikacji (PHAC).

2. Należy zapewnić przeprowadzanie przeglądów zgodnie z zatwierdzonymi planami i śledzenie do skutku wykonania działań z nich wynikających.

3. Należy zapewnić wykrywanie, rejestrację, dochodzenie przyczyn, aprobowanie, wytyczanie nowych kierunków i rozwiązywanie niezgodności z planami i normami dotyczącymi urządzenia.

4. Należy zapewnić spełnianie kryteriów przechodzenia do kolejnego etapu projektu zgodnie z zatwierdzonymi planami.

5. W celu zapewnienia, że urządzenie wykonano zgodnie z danymi konstrukcyjnymi należy dokonać odpowiedniego sprawdzenia (np. przez kontrolę pierwszej sztuki).

6. Należy prowadzić zapisy z działań procesu zapewnienia bezpieczeństwa, z włączeniem dowodów potwierdzających zakończenie działań konstrukcyjnych.

7. Prowadzący projekt powinien zapewnić (tam, gdzie jest to stosowne), aby procesy przeprowadzane przez podwykonawców były spójne z planami dotyczącymi urządzenia.

8. Proces ubiegania się o certyfikację

W procesie ubiegania się o certyfikację istotne jest ustanowienie łączności i uzyskanie wzajemnego zrozumienia między ubiegającym się o certyfikat (aplikantem) a organem certyfikującym. Proces ubiegania się o certyfikację powinien być realizowany tak, jak to opisano w procesie planowania i planie sprzętowych aspektów certyfikacji (PHAC), stanowiącym podstawowy dokument planowania procesu certyfikacyjnego. Ubiegający się certyfikat proponuje sposoby wykazania zgodności urządzenia, które należy podać w planie PHAC.

Wytyczne dotyczące sposobów wykazania zgodności

1. Plan PHAC, plan weryfikacji urządzenia i inne wymagane dokumenty należy przedłożyć organowi certyfikującemu do przeglądu, gdy wpływ zmian na przebieg programu jest minimalny.

2. Należy wyjaśnić zastrzeżenia sformułowane przez organ certyfikujący dotyczące planowania na rzecz sprzętowych aspektów certyfikacji (PHAC).

3. Należy uzyskać potwierdzenie organu certyfikującego na dokumencie PHAC.

4. Należy kontynuować współpracę z organem certyfikującym na etapie konstruowania i certyfikacji zgodnie z zapisami w planach, oraz wyjaśniać niezwłocznie zgłaszane przez organ uwagi.

9. Dane z przebiegu procesu projektowania

W niniejszym punkcie opisano dokumenty i materiały stanowiące rezultat procesu projektowania wraz z wytycznymi dotyczącymi zawartości tych dokumentów.

Dane z przebiegu projektowania powinna charakteryzować:

- **jednoznaczność** – informacje/dane są zapisane w sposób, który pozwala tylko na jedną interpretację,
- **kompletność** – informacje/dane zawierają niezbędne i stosowne wymagania oraz materiał opisowy – opisane rysunki, zdefiniowaną przyjętą terminologię i jednostki miar,
- **weryfikowalność** – informacje/dane mogą być sprawdzone pod kątem poprawności przez sprawdzających lub za pośrednictwem narzędzi,
- **spójność** – informacje/dane nie zawierają żadnych sprzeczności,
- **modyfikowalność** – informacje/dane posiadają określoną strukturę, zmiany mogą być dokonywane kompletnie, spójnie i poprawnie z zachowaniem struktury,
- **odtwarzalność** – możliwe jest określenie genezy, przebiegu powstawania informacji/danych.

Materiały wytwarzane i wykorzystywane w procesie projektowania

1. Plan/założenia sprzętowych aspektów certyfikacji (PHAC). W PHAC określa się procesy, procedury, metody i normy, których stosowanie ma na celu osiągnięcie zamierzonych rezultatów i zatwierdzenie systemu zawierającego dane urządzenia przez organ certyfikujący. Plan PHAC po zatwierdzeniu stanowi porozumienie między ubiegającym się o certyfikację a organem certyfikującym, dotyczące prowadzonych procesów i działań, i wynikających z tego dokumentów dowodowych wytworzonych dla spełnienia sprzętowych aspektów certyfikacji. PHAC może być częścią innego planu, takiego jak plan certyfikacji systemu pokładowego.

2. Plan/założenia projektowe urządzenia. W założeniach projektowych urządzenia opisywane są procedury, metody i normy, jakie zostaną zastosowane,

oraz procesy i działania, niezbędne do wykonania projektu urządzenia. Założenia te mogą być włączone w plan PHAC i mogą przywoływać przyjęte ogólne zasady projektowania i zastosowane unormowania.

3. Plan walidacji urządzenia. W planie walidacji opisywane są procedury, metody i normy przewidziane do zastosowania oraz procesy i działania, które należy przeprowadzić w celu walidacji pozyskanych wymagań dla urządzenia, tak aby osiągnąć zamierzone rezultaty walidacji zgodnie z niniejszym dokumentem. Plan ten może być włączony w plan PHAC i może przywoływać przewidziane do zastosowania normy dotyczące walidacji.

4. Plan weryfikacji urządzenia. W planie weryfikacji opisywane są procedury, metody i normy stosowane w procesach i działaniach prowadzonych na rzecz weryfikacji urządzenia, aby uzyskać założone rezultaty weryfikacji, zgodnie z niniejszym dokumentem. Niniejszy plan może być włączony w plan PHAC i może przywoływać przewidziane do zastosowania ogólne zasady i normy weryfikacji.

5. Plan zarządzania konfiguracją urządzenia. W planie zarządzania konfiguracją urządzenia opisywane są ogólne zasady, procedury, normy i metody służące spełnieniu założonych rezultatów zarządzania konfiguracją zgodnie z niniejszym dokumentem.

6. Plan procesu zapewnienia bezpieczeństwa urządzenia. W planie procesu zapewnienia bezpieczeństwa urządzenia opisywane są procedury, metody i normy przewidziane do zastosowania oraz procesy i działania prowadzące do uzyskania założonych rezultatów procesu zapewnienia bezpieczeństwa, zgodnie z niniejszym dokumentem.

7. Normy i poradniki dotyczące projektu urządzenia. Normy przedmiotowe, poradniki i wytyczne dotyczące projektowanego urządzenia mogą określać zasady, procedury, metody i kryteria dla procesów projektowania urządzenia, walidacji, weryfikacji, zapewnienia bezpieczeństwa i nadzoru. Są one wykorzystywane do oceny zdatności i jakości produktów powstałych w trakcie projektowania urządzenia. Zgodność z normami może nie być wymagana, ale jeżeli zostaną one przywołane w projekcie, stają się częścią podstawy certyfikacji i założeń projektu.

8. Dane projektowe. Danymi projektowymi urządzenia są wykazy, dokumenty i rysunki, które definiują przedmiotowe urządzenie.

8.1. Wymagania dotyczące urządzenia. Wymagania te są szczegółowym zestawieniem wymagań funkcjonalnych, właściwości, wymagań bezpieczeństwa, jakościowych, podatności obsługowej i niezawodności opracowywanego urządzenia.

8.2. Dokumentacja konstrukcyjna urządzenia. Definiuje ona projektowane urządzenie i obejmuje rysunki, dokumenty i zestawienia wykorzystywane do wytwarzania danego urządzenia. Rodzaj danych, rysunki i dokumenty wytworzone dla danego urządzenia będą w dużej mierze zależeć od rozmiarów,

złożoności i liczby podzespołów urządzenia. Na dane zawarte w dokumentacji konstrukcyjnej składają się dane projektów koncepcyjnego i technicznego.

9. Dane z walidacji i weryfikacji. Dane te stanowią dokumentację kompletności i poprawności rezultatów projektu urządzenia i samego urządzenia. Jest to zabezpieczenie zgodnego z wymaganiami opracowania urządzenia, poprawności wytwarzania i osiągnięcia zamierzonych rezultatów projektu. Dane zawierają procedury i wyniki przeglądów, analiz i badań urządzenia.

10. Kryteria akceptacji dla badań urządzenia. Dane te zawierają kryteria i ocenę danych, na ile wykonane badania i związane z nimi wyniki są w stanie zapewnić, że urządzenie zostało wytworzone lub udoskonalone poprawnie.

11. Zgłoszenia problemów. Jest to środek identyfikacji i rejestracji rozwiązań problemów konstrukcyjnych, niezgodności procesów z założeniami i normami oraz braków w danych z przebiegu procesu projektowania.

12. Zapisy z zarządzanie konfiguracją urządzenia. Wyniki działań podjętych w ramach procesu zarządzania konfiguracją są rejestrowane w zapisach z zarządzania konfiguracją. Mogą one zawierać wykazy identyfikacyjne konfiguracji, wzorce lub rejestracje elektroniczne, zapisy dotyczące historii zmian, streszczenia zgłoszeń problemów, dane identyfikacyjne narzędzi, zapisy archiwalne i zapisy dotyczące zezwoleń na publikację.

13. Zapisy z procesu zapewnienia bezpieczeństwa urządzenia. Wyniki działań procesu zapewnienia są rejestrowane w zapisach z procesu zapewnienia bezpieczeństwa. Mogą one zawierać raporty z przeglądów lub auditów, notatki ze spotkań, zapisy odstępstw w procesie autoryzacji lub zapisy z przeglądów zgodności.

14. Podsumowanie realizacji urządzenia. Podsumowanie realizacji urządzenia jest podstawowym dokumentem wykazania zgodności z planem PHAC i zademonstrowania organowi certyfikującemu, że dla danego urządzenia zostały osiągnięte założone rezultaty niniejszego dokumentu. Może być one połączone z podsumowaniem realizacji systemu.

10. Czynniki dodatkowe

W procesie projektowania należy również uwzględnić czynniki dodatkowe.

1. Wykorzystanie opracowanego wcześniej urządzenia. Jest to omówienie zagadnień związanych z wykorzystaniem opracowanego wcześniej, gotowego urządzenia. Wytyczne dotyczą oceny modyfikacji urządzenia, instalacji, środowiska pracy lub środowiska projektowego oraz modernizacji wzorców konstrukcyjnych.

2. Zastosowanie elementów handlowych (COTS). Elementy handlowe (COTS) są powszechnie używane w konstrukcjach urządzeń. Dane projektowe elementów COTS są zazwyczaj niedostępne. Proces certyfikacji nie jest specjal-

nie nakierowany na poszczególne elementy, moduły lub podzespoły, o ile nie zachodzi przypadek realizacji przez nie specyficznych funkcji statku powietrznego podlegających certyfikacji.

3. Doświadczenia z eksploatacji wyrobu. Doświadczenie z eksploatacji może być wykorzystane do dowodzenia bezpieczeństwa konstrukcji dla opracowanych wcześniej urządzeń i elementów handlowych COTS. Doświadczenie z eksploatacji to dane zebrane z dowolnych wcześniejszych i obecnych zastosowań elementu. Dane z zastosowań poza pokładem statków powietrznych nie są wykluczone.

4. Ocena i kwalifikacja narzędzi. Celem oceny i kwalifikacji jest zapewnienie, że narzędzie jest zdolne do realizacji poszczególnych działań projektowych i weryfikacyjnych na wymaganym poziomie ufności. Jest uporządkowaną, prowadzoną od góry w dół, analizą iteracyjną. Identyfikuje ona poszczególne części konstrukcji, które realizują daną funkcję; analizowane są więc zespoły, podzespoły i elementy związane z każdą ścieżką oraz powiązane z nimi stany uszkodzeń i inne objawy dla ustalenia zgodności przyjętej architektury urządzenia i jego wykonanie z wymaganiami bezpieczeństwa. FFPA identyfikuje także te zespoły, komponenty i elementy konstrukcji, które realizują funkcje poziomu A i B.

W dokumencie opisano również przykładowe metody zapewnienia bezpieczeństwa konstrukcji, takie jak wykorzystanie właściwości architektury, doświadczeń z eksploatacji, wyrafinowanych metod analitycznych (analiza elementarna, analiza wpływu szczególnych czynników na bezpieczeństwo – *Safety-Specific Verification Analysis*, metody formalne). Załącznik C zawiera słownik terminologii, a załącznik D – słownik skrótów.

11. Podsumowanie

DO-254 jest bardzo istotnym, obok DO-160 i DO-178, dokumentem o charakterze ogólnym. Nie jest on wprawdzie normą, ale staje się nią przez przywołanie w innych dokumentach normalizacyjnych. W dokumencie zawarto wiele stwierdzeń o charakterze wydawałoby się oczywistym, ale systematyzuje on cały proces projektowania urządzenia, aż do przekazania go do produkcji. Dokument doczekał się już wielu programów komputerowych ułatwiających zastosowanie wymaganych procedur. W kraju jest mało rozpowszechniony.

RTCA, podobnie jak inne dokumenty, jest dostępna za opłatą, za pośrednictwem strony internetowej RTCA. Cena dokumentu wynosi 125 $ dla krajów spoza Ameryki Północnej.

Literatura

[1] DO-254: Design Assurance Guidance for Airborne Electronic Hardware, RTCA, April 19, 2000.
[2] DO-254: Przewodnik zapewnienia bezpieczeństwa w konstrukcjach pokładowych urządzeń elektronicznych, tłum. Edward Babiasz, grudzień 2009, www.rtca.org.

DESIGN ASSURANCE GUIDANCE FOR AIRBORNE ELECTRONIC HARDWARE RTCA DO-254/ED-80 – EUROCAE

A b s t r a c t

Document DO-254 defines guidance intended to be used by manufacturers and suppliers of airborne electronic hardware items. The hardware design life processes are identified. These text shortly describe objectives and activities for each process.

Złożono w Oficynie Wydawniczej w sierpniu 2011 r.