Journal of KONBiN 1(29)2014
ISSN 1895-8281

SAFETY CASE AS A NECESSARY ASPECT OF THE AVIATION IMPLEMENTATION OF THE GNSS

SAFETY CASE JAKO NIEZBĘDNY ASPEKT LOTNICZEJ IMPLEMENTACJI SYSTEMU GNSS

Andrzej Fellner, Radosław Fellner, Henryk Jafernik

Politechnika Śląska, Wydział Transportu
e-mail: andrzej.fellner@polsl.pl, rfellner@wp.pl, henrykj21@interia.pl

***Abstract**: The article describes analysis of the risk for the implementation of precise approach procedures (Localizer Performance and Vertical Guidance - LPV) with GNSS sensor at airports in Warsaw and Katowice. There were used some techniques of the identification of threats (including controlled flight into terrain, landing accident, mid-air collision, missed approach, safe landing) and evaluations methods based on: Event Tree Analysis, probability of the risk, safety risk evaluation matrix and Functional Hazard Assesment. Also safety goals were determined. Research led to determine probabilities of appearing of threats, as well as allow compare them with regard to the ILS. As a result of conducting the Preliminary System Safety Assessment (PSSA), there were defined requirements essential to reach the required level of the safety. Research led to determine probabilities of appearing of threats and safety goals, as well as compare them with regard to the ILS requirements.*

***Keywords:** GNSS, safety case, aviation safety, ETA, LPV*

***Streszczenie:** Artykuł przedstawia analizę ryzyka na potrzeby wdrożenia procedur podejścia precyzyjnego (Localizer Performance and Vertical Guidance - LPV) z użyciem sensora GNSS dla lotnisk w Warszawie i Katowicach. Szczegóły zostały zawarte w opracowywanym w ramach międzynarodowego projektu SHERPA. Do analizy wykorzystano techniki identyfikacji zagrożeń (zderzenie z powierzchnią ziemi w locie sterowanym - CFIT, wypadek podczas lądowania - LA, kolizja w powietrzu - MAC, procedura po nieudanym podejściu - MA, bezpieczne lądowanie) i oceny ich następstw oparte o metody analiz: Event Tree Analysis, zestawienie prawdopodobieństwa ryzyka bezpieczeństwa, macierz oceny ryzyka bezpieczeństwa oraz Functional Hazard Assesment. Następnie określono cele bezpieczeństwa. Przeprowadzone badania pozwoliły na wyznaczenie prawdopodobieństw występowania zagrożeń i celów bezpieczeństwa, a także porównanie ich względem wymagań systemu ILS.*

***Słowa kluczowe:** GNSS, safety case, lotnisko, ETA, LPV*

1. Wstęp

Analiza ryzyka jest kluczowym aspektem implementacji technik i technologii nawigacyjnych oraz naziemnych urządzeń lotniczych. Istotne przy tym jest zachowanie wysokiego poziomu niezawodności urządzeń oraz poprawna identyfikacja zagrożeń i podniesienie poziomu bezpieczeństwa operacji lotniczych. W niniejszej pracy przedstawiono analizę ryzyka na potrzeby wdrożenia procedur podejścia precyzyjnego (LPV - Localizer Performance and Vertical Guidance) z użyciem sensora GNSS dla lotnisk w Warszawie i Katowicach. Zakłada się, że procedury podniosą poziom bezpieczeństwa operacji w FIR Warszawa.

2. Niezawodność w lotnictwie

W lotnictwie niezawodność definiuje się jako zdolność do spełniania ustalonych kryteriów, umożliwiających dokonywanie operacji i zadań lotniczych (operacji i misji) w określonym czasie i warunkach [2]. Wiąże się to z koniecznością podejmowania działań diagnostycznych, profilaktycznych, konserwacyjnych, a do pewnego stopnia także prognostycznych, zarówno w odniesieniu do statków powietrznych, jaki i infrastruktury lotniskowej czy systemów nawigacyjnych. Zatem niezawodność to zdolność do realizowania zadań wykluczająca istnienie zdarzeń uniemożliwiających spełnianie wyznaczonych funkcji. Wyróżnia się przy tym:

- stan zdatny - w przypadku pełnej możliwości realizowania wytycznych;
- stan niezdatny - gdy realizacja operacji jest niemożliwa, może zostać wstrzymana lub może skutkować wypadkiem czy też stratami.

Na powyższe stany wpływa szereg czynników począwszy od załogi i obsługi (czynnik ludzki), warunków atmosferycznych, obiektów technicznych (maszyn, urządzeń), na procedurach skończywszy. Kombinacja i zmiany w ich obrębie mogą prowadzić do wystąpienia stanu niezdatności. Można zatem mówić o ryzyku (możliwości, prawdopodobieństwie) zaistnienia negatywnych zdarzeń. Warto odnotować, że Międzynarodowa Organizacja Lotnictwa Cywilnego definiuje ryzyko bezpieczeństwa jako prawdopodobieństwo i dotkliwość konsekwencji wystąpienia zagrożenia, biorąc jako punkt odniesienia najgorszą, dającą się przewidzieć sytuację [4]. Negatywne, niepożądane zdarzenia mogą doprowadzić do strat i wtedy prawdopodobieństwo ich wystąpienia będzie nazywane zagrożeniem.

3. Wybrane aspekty analizy ryzyka

Odpowiednia identyfikacja zagrożeń i analiza ryzyka są elementami systemu zarządzania bezpieczeństwem w lotnictwie, rozumianym jako zespół przedsięwzięć i przepisów mających na celu utrzymanie na akceptowanym poziomie lub zredukowanie ryzyka wyrządzenia szkody, wystąpienia usterki lub pojawienia się błędu. Poprawnej identyfikacji zagrożeń i oceny ich następstw służą szczegółowo zdefiniowane metody analizy, takie m.in. jak [1,3]:

- FMEA (Failure Mode and Effects Analysis) - w której obiekt analizy rozkłada się na części składowe i określa ich potencjalne przyczyny zawodności, oraz ustala związki przyczynowo-skutkowe między nimi;
- FTA (Fault Tree Analysis) - w której początkowo ustala się końcowe zdarzenie krytyczne (skutek), a następnie zdarzenia które mogły do niego doprowadzić;
- ETA (Event Tree Analysis) - w której najpierw określa się zdarzenia które mogą doprowadzić do zaistnienia zagrożenia;
- Zestawienie prawdopodobieństwa ryzyka bezpieczeństwa - przedstawia ocenę ryzyka niebezpiecznego wydarzenia lub okoliczności w terminach możliwości wystąpienia (Tabela 1) [3];
- Macierz oceny ryzyka bezpieczeństwa - zestawiająca prawdopodobieństwo wystąpienia ryzyka bezpieczeństwa z dotkliwością zdarzeń (Tabela 2) [3].

Tabela 1. Tabela klasyfikacji ryzyka bezpieczeństwa.

	Znaczenie	Wartość
Częste	Prawdopodobnie wystąpi często	5
Sporadyczne	Prawdopodobnie wystąpi sporadycznie	4
Niewielkie	Prawdopodobnie nie wystąpi, ale jest to możliwe (występowało rzadko)	3
Nieprawdopodobne	Bardzo małe prawdopodobieństwo, że wystąpi (nie znany jest przypadek by wystąpiło)	2
Skrajnie nieprawdopodobne	Prawie niewyobrażalne, że kiedykolwiek może wystąpić	1

Tabela 2. Macierz oceny ryzyka bezpieczeństwa.

Prawdopodobieństwo ryzyka	Dotkliwość ryzyka				
	Katastrofalna A	Niebezpieczna B	Poważna C	Niewielka D	Nieistotna E
Częste 5	5A	5B	5C	5D	5E
Sporadyczne 4	4A	4B	4C	4D	4E
Niewielkie 3	3A	3B	3C	3D	3E
Nieprawdopodobne 2	2A	2B	2C	2D	2E
Skrajnie nieprawdopodobne 1	1A	1B	1C	1D	1E

Wybór odpowiedniej metody zależy od dostępnych danych ilościowych i jakościowych, jak również od złożoności czynników zagrażających bezpieczeństwu.

4. Wybrane aspekty Safety Case podczas wykonywania podejść do lądowania według systemów satelitarnych GNSS

Analizie bezpieczeństwa poddano MPL Katowice w Pyrzowicach oraz MPL Warszawa, gdzie wykonywano podejścia do lądowania, w oparciu o certyfikowane odbiorniki GNSS, korzystające z sygnałów satelitarnych – szczególnie EGNOS. Szczegóły zostały zawarte w opracowywanym w ramach międzynarodowego projektu SHERPA dokumencie „Polish National Scenario Report".
Zasadne jest podanie, ze wdrożenie procedur SBAS LPV stanowi kolejny poziom badawczy po uruchomieniu procedur RNAV GNSS zgodnie z dokumentem „PANSA Navigation Strategy Plan and PANSA Airspace Strategy Plan". Stąd też, ze względów metodologicznych, podczas prowadzenia badań przyjęto kilka następujących etapów:

1) Pierwszy - identyfikacja zagrożeń, związanych z wykorzystaniem procedur SBAS LPV, które są szczegółowo przedstawione przez EUROCONTROL w „Final Functional Hazard Assessment of LPV approaches in the ECAC Area". Na tej podstawie opracowany został opis zidentyfikowanych zagrożeń (Tabela 3);

Tabela 3. Spis zidentyfikowanych zagrożeń.

Lp.	Opis zagrożenia	Dodatkowe informacje
H3	**Przechwycenie GS "od spodu".** Fly low while intercepting the final approach path (vertical profile)	Statek powietrzny jest w nieprawidłowej pozycji zbliżając się do FAWP (niżej niż minima procedury)
H4	**Przechwycenie GS "z góry".** Attempt to intercept the final approach path from above (vertical profile) Próba przechwycenia drogi podejścia do lądowania z góry (pionowy profil)	Warunki prowadzące do tego zagrożenia, to albo brak bocznego przechwycenia końcowej ścieżki schodzenia (sekwencja będąca wynikiem H2), albo statek powietrzny znajduje się na zbyt dużej wysokości przed FAWP. W obu wypadkach załoga samolotu nie zdoła przechwycić ścieżki schodzenia i, zamiast rozpoczęcia MA, decyduje się na przechwycenie drogi podejścia do lądowania z góry, z naruszeniem normalnej procedury.
H6	**Brak możliwości utrzymania końcowej ścieżki schodzenia.** Failure to follow the correct final approach path	Statek powietrzny znajduje się w nieprawidłowej pozycji na końcowej ścieżce schodzenia
H7	**Zniżanie poniżej DA bez widoczności terenu** Descending below DA without visual	Statek powietrzny zniża się poniżej DA podczas, gdy nie ma kontaktu wzrokowego z terenem (nieprawidłowa procedura, nieprawidłowe QNH lub nieprawidłowe DA.
H8	**Nieprawidłowe wykonanie procedury MA** Failure to execute correct Missed Approach	Niepowodzenie w utrzymywaniu wymaganego profilu lotu podczas wykonywania procedury po nieudanym podejściu;

2) Drugi - analiza następstw zagrożeń (skutki operacyjne), związanych z wykorzystaniem procedur SBAS LPV, również szczegółowo przedstawiona przez EUROCONTROL w „Final Functional Hazard Assessment of LPV approaches in the ECAC Area" (Tabela 4). Rozważono istniejące ograniczenia ryzyka a następnie podsumowano wyniki analizy drzew zdarzeń (Tabela 5);

Tabela 4. Analiza następstw zagrożeń.

Lp.	Następstwa zagrożeń	Waga następstwa zagrożenia
C1	Zderzenie z powierzchnią ziemi w locie sterowanym (CFIT)	Wypadek (waga skutku 1)
C2	Wypadek podczas lądowania (LA)	Wypadek (waga skutku 1)
C3	Kolizja w powietrzu (MAC)	Wypadek (waga skutku 1)
C4	Procedura po nieudanym podejściu (MA)	Incydent (waga skutku 4)
C5	Bezpieczne lądowanie	Bez wpływu

Tabela 5. Wnioski z analizy drzew zdarzeń.

Lp.	Wnioski	Skutki	Częstość
H3	Nie zidentyfikowano dodatkowych barier w stosunku do FHA przeprowadzonego przez EUROCONTROL. W analizie nie uwzględniono Safety Nets.	CFIT	Warszawa 0.125 Katowice 0.125
H4	Nie zidentyfikowano dodatkowych barier w stosunku do FHA przeprowadzonego przez EUROCONTROL. W analizie nie uwzględniono Safety Nets.	Wypadek podczas lądowania	Warszawa 0.00025 Katowice 0.00025
H6	Nie zidentyfikowano dodatkowych barier w stosunku do FHA przeprowadzonego przez EUROCONTROL. W analizie nie uwzględniono Safety Nets.	CFIT	Warszawa 0.125 Katowice 0.125
H7	Nie zidentyfikowano dodatkowych barier w stosunku do FHA przeprowadzonego przez EUROCONTROL. W analizie nie uwzględniono Safety Nets.	CFIT	Warszawa 0.125 Katowice 0.125
		Wypadek podczas lądowania	Warszawa 0.125 Katowice 0.125
H8	Nie zidentyfikowano dodatkowych barier w stosunku do FHA przeprowadzonego przez EUROCONTROL. W analizie nie uwzględniono Safety Nets.	CFIT	Warszawa 0.0025 Katowice 0.0025
		Kolizja w powietrzu	Warszawa 0.00025 Katowice 0.00025

3) Trzeci – określono cele bezpieczeństwa, poprzez przyjęcie TLS (Target Level of Safety) i podzielono je według wzoru:

$$SO_{HX} = C * \frac{TLS_{accident}}{\prod(Q)}$$

gdzie:
SO - cel bezpieczeństwa dla poszczególnych zagrożeń (Hx);
Q - prawdopodobieństwo wystąpienia wypadku spowodowane zagrożeniem;
C - waga poszczególnych zagrożeń prowadzących do wypadku.

TLS został obliczony i przedstawiony wraz z uzasadnieniem dla poszczególnych następstw zagrożeń oraz podsumowany w Tabeli 6 (TLS dla następstw zagrożeń związanych z LPV). Również podczas analizowania przyjęto równy udział poszczególnych następstw zagrożeń w TLS, aby uzyskać dodatkowy bufor dla zagrożeń, gdzie prawdopodobieństwo wystąpienia następstwa jest mniejsze ze względu na np. fazę lotu. Stąd też pojawiły się propozycje celów bezpieczeństwa dla: CFIT (Tabela 7), wypadku podczas lądowania (LA) (Tabela 8), kolizji w powietrzu (MAC) (Tabela 9). Następnie sporządzono drzewa ryzyka określające cele bezpieczeństwa: CFIT, LA, MAC. Na podstawie powyższych drzew obliczono i przyjęto cele bezpieczeństwa dla poszczególnych zagrożeń (Tabela 10).

Tabela 6. TLS dla następstw zagrożeń związanych z LPV.

Rodzaj następstw	LPV TLS
CFIT	1×10^{-8}
Wypadek podczas lądowania	2×10^{-7}
Kolizja w powietrzu	1×10^{-10}

Tabela 7. Propozycje celów bezpieczeństwa dla CFIT.

H3	1.6e-8	20%
H4	Nie dotyczy. Zagrożenie nie prowadzi do CFIT	
H6	1.6e-8	20%
H7	1.6e-8	20%
H8	1.6e-8	20%
Margines bezpieczeństwa	2e-9	20%

Tabela 8. Propozycje celów bezpieczeństwa dla wypadku podczas lądowania.

Zagrożenie	Propozycja celu bezpieczeństwa	Udział w LA TLS
H3	Nie dotyczy. Zagrożenie nie prowadzi do LA	-
H4	2.67e-4	33%
H6	Nie dotyczy. Zagrożenie nie prowadzi do LA	-
H7	5.33-7	33%
H8	Nie dotyczy. Zagrożenie nie prowadzi do LA	-
Margines bezpieczeństwa	5.67e-8	33%

Tabela 9. Propozycje celów bezpieczeństwa dla kolizji w powietrzu.

Zagrożenie	Propozycja celu bezpieczeństwa	Udział w MAC TLS
H3	Nie dotyczy. Zagrożenie nie prowadzi do MAC	-
H4	Nie dotyczy. Zagrożenie nie prowadzi do MAC	-
H6	Nie dotyczy. Zagrożenie nie prowadzi do MAC	-
H7	Nie dotyczy. Zagrożenie nie prowadzi do MAC	-
H8	2e-7	50%
Margines bezpieczeństwa	5e-11	50%

Tabela 10. Cele bezpieczeństwa dla poszczególnych zagrożeń.

Lp.	Opis	Następstwa	Cel bezpieczeństwa
H3	Przechwycenie GS "od spodu"	· Procedura MA jeśli wykryte · Bezpieczne lądowanie w przypadku niewykrycia i zadziałania barier · CFIT w przypadku niewykrycia i niezadziałania barier	1.6e-8
H4	Przechwycenie GS "z góry"	· Procedura MA lub bezpieczne lądowanie w przypadku skutecznego zadziałania barier · CFIT w przypadku niezadziałania barier	2.66-4
H6	Brak możliwości utrzymania końcowej ścieżki schodzenia	· Procedura MA lub bezpieczne lądowanie jeśli wykryte lub w przypadku skutecznego zadziałania barier · CFIT w przypadku niewykrycia i niezadziałania barier	1.6e-8
H7	Zniżanie poniżej DA bez widoczności terenu	· MA jeśli wykryte · Bezpieczne lądowanie w przypadku skutecznego zadziałania barier · Wypadek podczas lądowania jeśli odchylenie nie jest w stronę przeszkody i pozostałe bariery nie zadziałają · CFIT jeśli niewykryte oraz odchylenie jest w stronę przeszkody.	1,6e-8
H8	Nieprawidłowe wykonanie procedury MA	· Bez większego wpływu na bezpieczeństwa jeśli wykryte i skorygowane – prowadzi do MA lub bezpiecznego lądowania. · CFIT w przypadku niezadziałania wszystkich barier, gdy odchylenie jest w stronę przeszkody. · MAC w przypadku niezadziałania wszystkich barier, gdy odchylenie jest w stronę innego a/c.	2e-7

4) Czwarty - analiza jakościowa i ilościowa (FTA) – opracowanie drzew usterek, określających prawdopodobieństwo występowania zagrożeń na podstawie przyjętych prawdopodobieństw występowania przyczyn (analiza FTA) dla poszczególnych zagrożeń. Stanowiło to część wstępnej systemowej oceny bezpieczeństwa.

Zasadne było dokonanie analizy zarówno ilościowej jak i jakościowej, z uwagi na występowanie podobieństwa do funkcjonujących procedur systemu przyrządowego lądowania - ILS, które są certyfikowane, akceptowalnie bezpieczne. W oparciu o wytyczne EUROCONTROL, założono, że dla zagrożeń: H3 i H4 - ryzyko jest takie jak dla ILS, H6 - określono dodatkowe wymagania bezpieczeństwa w celu ograniczenia ryzyka (Tabela 11).

Tabela 11. Analiza celów bezpieczeństwa a system ILS

Zagrożenie	Cel bezpieczeństwa	Osiągnięte prawdopodobieństwo wystąpienia zdarzenia	Osiągnięcie celu
H3	Ryzyko nie większe niż w przypadku ILS (zgodnie z PSSA Eurocontrol patrz. Pkt 4.1 PSSA LPV)	Ryzyko nie większe niż w przypadku ILS (zgodnie z PSSA EUROCONTROL)	Tak
H4	Ryzyko nie większe niż w przypadku ILS (zgodnie z PSSA Eurocontrol patrz. Pkt 4.2 PSSA LPV)	Ryzyko nie większe niż w przypadku ILS (zgodnie z PSSA EUROCONTROL)	Tak
H6	1.6e-8	1.84e-6	Nie
H7	Ryzyko nie większe niż w przypadku ILS (zgodnie z PSSA Eurocontrol patrz pkt. 4.4 PSSA LPV)	Ryzyko nie większe niż w przypadku ILS (zgodnie z PSSA EUROCONTROL)	Tak
H8	2e-7	Ryzyko nie większe niż w przypadku ILS (zgodnie z PSSA EUROCONTROL)	Tak

5. Podsumowanie

W wyniku przeprowadzenia wstępnej systemowej oceny bezpieczeństwa (PSSA), określone zostały wymagania bezpieczeństwa niezbędne do osiągnięcia wymaganego poziomu bezpieczeństwa. Wymagania zostały przedstawione w odpowiednich tabelach. Podkreślić należy, że wymagania ilościowe zostały zdeterminowane przy pomocy drzew FTA. Natomiast podczas przeprowadzania obliczeń nie uwzględniono Safety Nets. Spowodowane to było brakiem danych dotyczących funkcjonowania Safety Nets w nowym systemie.

4. Literatura

[1] EASA: GUIDANCE ON HAZARDS IDENTIFICATION, Safety Management System and Safety Culture Working Group (SMS WG), March 2009.

[2] Lewitowicz J., Kustroń K.: Podstawy eksploatacji statków powietrznych – własności i właściwości eksploatacyjne statku powietrznego, Tom II, Wydawnictwo Instytutu Technicznego Wojsk Lotniczych, Warszawa 2003, s. 229-231.

[3] ICAO: Podręcznik Zarządzania Bezpieczeństwem, Urząd Lotnictwa Cywilnego, Doc 9859, wydanie drugie, Warszawa 2009, s. 82-85.

[4] Art. 68. Ustawy Prawo Lotnicze, Dz.U.z 2012 poz. 933. z późn. zm.

[5] ESARR 1 - Safety Oversight in ATM, second edition, December 2009.

[6] ESARR 2 - Reporting and Assessment of Safety Occurrences in ATM, third edition, December 2009.

[7] ESARR 3 - Use of Safety Management Systems by ATM Service Providers, July 2000.

[8] ESARR 4 - Risk Assessment and Mitigation in ATM, April 2001.

[9] Rozporządzenie Parlamentu Europejskiego i Rady WE Nr 216/2008 w zakresie lotnisk i zarządzania ruchem lotniczym z dnia 20 lutego 2008, WE Nr 1315/2007 dotyczy nadzoru bezpieczeństwa w zarządzaniu ruchem lotniczym oraz WE Nr 691/2010 w sprawie skuteczności działania systemów nawigacyjnych.

Dr hab. inż. nawig. Andrzej Fellner *- profesor nadzwyczajny Politechniki Śląskiej, dyrektor Centrum Kształcenia Kadr Lotnictwa Cywilnego Europy Środkowo-Wschodniej Politechniki Śląskie. Konsultant ds. technologii satelitarnych, autor i współautor ponad 360 artykułów i prac naukowych opublikowanych w kraju i za granicą. Koordynator międzynarodowych projektów naukowo-badawczych z ramienia Polskiej Agencji Żeglugi Powietrznej.*

Dr inż. pil. Henryk Jafernik *- docent Politechniki Śląskiej, adiunkt w Katedrze Nawigacji Lotniczej Wyższej Szkoły Oficerskiej Sił Powietrznych. Współautor trzech podręczników oraz ponad 70 artykułów i prac naukowych opublikowanych w kraju i za granicą. Uczestnik projektów badawczych z dziedziny nawigacji satelitarnej.*

Mgr Radosław Fellner *- pracownik Politechniki Śląskiej. Uczestnik stażu w Parlamencie Europejskim. Autor kilkunastu artykułów oraz prac naukowych z zakresu implementacji technologii satelitarnych w lotnictwie oraz prawa lotniczego Unii Europejskiej.*