ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2006
Seria: TRANSPORT z. 62 Nr kol. 1721

Wojciech CHMURA[1], Marek MALARSKI[2]

ANALIZA ZAGROŻEŃ FUNKCJONALNYCH W RUCHU LOTNICZYM

Streszczenie. Artykuł poświęcony jest zagadnieniu analizy zagrożeń funkcjonalnych (FHA) będącej narzędziem szeroko stosowanych obecnie w lotnictwie cywilnym systemów zarządzania bezpieczeństwem SMS. Celem wdrożenia i stosowania tych systemów jest ciągły monitoring poziomu bezpieczeństwa TLS w instytucji świadczącej usługi żeglugi powietrznej. Opisana w artykule analiza jest punktem wyjściowym do pomiaru poziomu bezpieczeństwa w ruchu lotniczym.

FUNCTIONAL HAZARD ANALYSIS FOR AIR TRAFFIC

Summary. The present article refers to the issue of functional hazard analysis that is generally considered to be the widespread tool of safety management systems. These systems aim at continuous monitoring of a safety level of services provided by an air navigation service provider. The functional hazard analysis is essential for a further measurement of a safety level in air traffic.

1. WPROWADZENIE

Po kilku tragicznych wypadkach lotnictwa cywilnego, które miały miejsce w 1976 nad Zagrzebiem oraz w 1977 na Teneryfie, w których łącznie zginęło ok. 700 osób, światowa opinia publiczna żądała podjęcia przez instytucje zajmujące się bezpieczeństwem ruchu lotniczego zdecydowanych działań zmierzających do poprawy bezpieczeństwa tego ruchu. Społeczność lotnicza przystąpiła więc do długofalowego, lecz niezbędnego procesu mającego na celu odbudowę zaufania opinii publicznej do transportu lotniczego jako najbezpieczniejszego środka transportu. Wszelkie ogólnoświatowe działania w tym zakresie polegały na prewencji, szkoleniu i opracowywaniu programów poprawy bezpieczeństwa. Nie wdając się w szczegóły, wynikiem ewolucji wszelkich działań stał się program zarządzania bezpieczeństwem ruchu lotniczego, który w Europie nosi nazwę *European Air Traffic Safety Management Program* (EATMP). Jego założenia oparte są na [3]. Jednym z wymagań programu EATMP jest ustanowienie, wdrożenie i realizacja tzw. systemu zarządzania bezpieczeństwem SMS (*Safety Management System*) przez instytucje świadczące usługi żeglugi powietrznej. SMS jest procesem stosowanym przez organizacje świadczące usługi związane z szeroko pojętym bezpieczeństwem w celu zapewnienia, że wszelkie aspekty związane z bezpieczeństwem świadczenia tych usług zostały właściwie uwzględnione. Polega

[1] Zakład Inżynierii Transportu Lotniczego, Wydział Transportu, Politechnika Warszawska, ul. Koszykowa 75 00-662 Warszawa, chmura.w@wp.pl
[2] Zakład Inżynierii Transportu Lotniczego, Wydział Transportu, Politechnika Warszawska, ul. Koszykowa 75 00-662 Warszawa, +48 22 660 7339, mma@it.pw.edu.pl

to na określeniu standardów i polityki bezpieczeństwa danej organizacji oraz narzędzi do mierzenia bieżącego poziomu bezpieczeństwa.

Instytucje świadczące usługi żeglugi powietrznej są organizacjami o złożonej strukturze: łączą w sobie technologię i człowieka (ludzi). Ocena bezpieczeństwa jest w takich systemach nie tylko wymagana przez władze lotnicze, ale również bezwzględnie konieczna w celu wyjaśnienia wypadków, incydentów albo niedoskonałości systemu, łącznie z przewidywaniem i zapobieganiem wystąpieniu błędu człowieka. Analizy zaistniałych wypadków wykazały, że przesłanki do ich wystąpienia mogą być przewidywalne i identyfikowane z wyprzedzeniem dzięki odpowiednim narzędziom. Bardzo rzadko zdarza się, aby wypadek był rezultatem pojedynczej przyczyny. Wypadki są zwykle splotem wielu czynników, występujących dzięki niesłychanie rzadkiemu zbiegowi okoliczności w jednym czasie. W przypadku gdy są analizowane oddzielnie, wydają się nie być istotne i nie mieć wielkiego wpływu na zdarzenie. Jednakże w rzeczywistości, w połączeniu z innymi czynnikami, stanowią prostą drogę do wypadku. Dlatego też narzędziom systemu zarządzania bezpieczeństwem przyświeca idea identyfikacji i eliminacji tych czynników, które mogą stanowić zagrożenie dla bezpieczeństwa ruchu lotniczego, zanim dojdzie do tragedii.

2. METODY OCENY BEZPIECZEŃSTWA

Zgodnie z polityką i założeniami EATMP [1] kontrola poziomu bezpieczeństwa w instytucji świadczącej usługi żeglugi powietrznej musi być nieodłącznym elementem każdego z etapów funkcjonowania systemu zarządzania ruchem lotniczym, m. in. dzięki któremu wykonywanie tych usług jest możliwe. Etapami tymi są koncepcja i planowanie systemu, realizacja i testowanie oraz normalna praca operacyjna. Na każdym z tych etapów stosowane są różne narzędzia do określania poziomu bezpieczeństwa. Na pierwszym etapie stosowana jest omawiana w niniejszym artykule analiza zagrożeń funkcjonalnych FHA (*Functional Hazard Analysis*). Na drugim etapie stosuje się wstępną ocenę bezpieczeństwa systemu PSSA (*Preliminary System Safety Assessment*). Na ostatnim etapie stosowane jest narzędzie zwane oceną bezpieczeństwa systemu SSA (*System Safety Assessment*). Artykuł ten poświęcony jest tylko analizie zagrożeń funkcjonalnych, więc pozostałe dwie metody pominięto.

3. ANALIZA ZAGROŻEŃ FUNKCJONALNYCH

Bezpieczeństwo ruchu lotniczego można mierzyć liczbą wypadków w określonym czasie. Jednakże w przypadku systemu, który jest dopiero w fazie projektów, a takiego właśnie dotyczy FHA, nie możemy mówić o jakimkolwiek wypadku, ponieważ system nie pracuje jeszcze operacyjnie. W tej sytuacji FHA proponuje mierzenie poziomu bezpieczeństwa ruchu lotniczego obsługiwanego przez nowo projektowany system w przyszłości za pomocą ryzyka wystąpienia określonego zdarzenia. Wypadki mają miejsce dzięki splotowi określonych czynników powodujących takie zagrożenie. Na skutek pewnego zagrożenia możemy mówić o ryzyku wystąpienia różnych zdarzeń. Aby lepiej to wyjaśnić, posłużmy się przykładem. Kontroler ruchu lotniczego z powodu usterki systemu radarowego nie zapewnia minimalnej separacji pomiędzy dwoma statkami powietrznymi. Fakt ten stanowi zagrożenie (*Hazard*), przy czym usterka jest przyczyną wystąpienia zagrożenia. W wyniku tego zagrożenia możemy mówić, że w zależności od dalszego biegu wydarzeń, o wystąpieniu ryzyka wykonania przez załogi niebezpiecznych manewrów w celu uniknięcia kolizji skutkujących obrażeniami osób na pokładach (ryzyku incydentu lotniczego) lub w skrajnym

przypadku o wystąpieniu ryzyka zderzenia się w powietrzu dwóch maszyn (ryzyku wypadku lotniczego).

Ryzyko ma dwa główne komponenty, które go opisują:
- określoną częstość występowania tego ryzyka (na miesiąc, na rok, na tydzień),
- konsekwencję ryzyka (złamana ręka, trwałe kalectwo, śmierć).

W postaci wzoru ryzyko można zapisać (1)

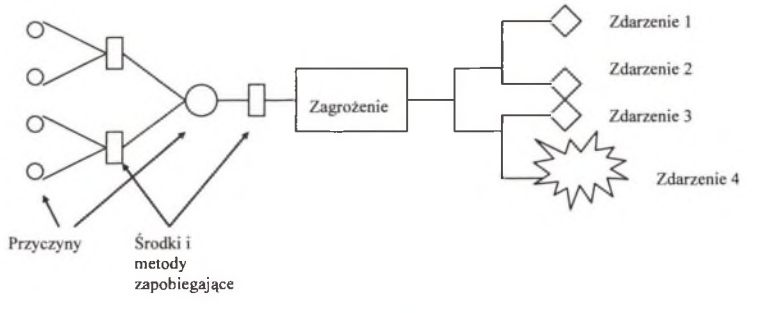
$$\text{ryzyko wystąpienia zdarzenia} = \frac{\text{konsekwencja ryzyka}}{\text{częstość wystąpienia ryzyka}} \quad (1)$$

Analiza zagrożeń funkcjonalnych składa się z trzech procesów:
- identyfikacja zagrożeń,
- analiza ryzyka,
- ocena ryzyka.

Rezultatem całej analizy FHA jest określenie celów, jakie postawi sobie organizacja w zakresie bezpieczeństwa. Innymi słowy, jakie będą liczbowe wartości ryzyka wystąpienia określonego zdarzenia, których system zarządzania ruchem lotniczym, realizując swoje zadania operacyjne, nie będzie mógł przekroczyć (np. wypadek nie będzie się mógł wydarzyć z przyczyn nieprawidłowości funkcjonowania systemu zarządzania ruchem lotniczym częściej niż 1 raz na 15 000 000 godzin lotu).

Identyfikacja zagrożeń

Punktem wyjściowym całej analizy jest identyfikacja zagrożeń ukrytych w systemie. Zagrożenie jest potencjalnym źródłem pogorszenia stanu bezpieczeństwa systemu skutkującym redukcją bieżącego poziomu bezpieczeństwa. Zagrożenie powodowane jest przez usterkę lub błąd ludzki rozumiane jako utrata lub zmniejszenie normalnej sprawności do wykonywania czynności operacyjnych. Usterka ta lub błąd ludzki mogą negatywnie wpływać na bezpieczeństwo świadczonych usług żeglugi powietrznej i przy określonym zbiegu okoliczności mogą spowodować incydent lub wypadek lotniczy. Każde zagrożenie, które może powstać na skutek błędu lub usterki w systemie zarządzania ruchem lotniczym, powinno zostać zidentyfikowane. Następnie każdemu z tych zagrożeń należy przyporządkować zarówno ryzyko wystąpienia określonych zdarzeń (konsekwencje), jak i wszystkie możliwe przyczyny powodujące te zagrożenia. Schemat z rysunku 1 przedstawia połączenie przyczyn zagrożeń z ich konsekwencjami.



Rys. 1. Schemat przyczyn zagrożeń i ich konsekwencji
Fig. 1. The scheme of casual factors and their consequences

Przykład:
Przyczyna 1 – brak zasilania, przyczyna 2 – przerwa w pracy radaru.
Środki i metody zapobiegające: alternatywna linia zasilająca, zwielokrotnienie pokrycia radarowego.
Zagrożenie: utrudniona kontrola ruchu lotniczego, znaczne obciążenie pracą kontrolerów, większe prawdopodobieństwo pomyłki i w rezultacie prawdopodobieństwo niezachowania minimum separacji między statkami powietrznymi.
Zdarzenie 1 – zbliżenie się statków powietrznych do siebie poniżej minimów separacji nie ma wpływu na bezpieczeństwo z racji wciąż dużej odległości minięcia się.
Zdarzenie 2 – zbliżenie się statków powietrznych powoduje konieczność wykonania manewru uniknięcia kolizji skutkującego dyskomfortem pasażerów.
Zdarzenie 3 – uniknięcie kolizji wymaga wykonania gwałtownego manewru przez oba statki powietrzne, co skutkuje poważnymi obrażeniami pasażerów.
Zdarzenie 4 – wypadek, w wyniku którego są ofiary śmiertelne wśród pasażerów.

Jak już wspomniano, po zidentyfikowaniu zagrożeń należy przyporządkować im możliwie jak najwięcej przyczyn oraz rozważyć, jakie można podjąć kroki minimalizujące ich zaistnienie (środki i metody zapobiegające). Ta część konstruowania schematu nazywa się analizą drzewa przyczyn FTA (*Fault Tree Analysis*). Z kolei, przypisanie każdemu zagrożeniu wszystkich przewidywalnych zdarzeń niosących za sobą określone ryzyko nazywa się analizą drzewa zdarzeń ETA (*Event Tree Analysis*).

Analiza ryzyka

Proces ten polega na przypisaniu każdemu zdarzeniu, zidentyfikowanemu dzięki analizie ETA, określonego ryzyka wyrażonego konsekwencjami oraz spodziewaną częstością występowania. Oczywistą regułą jest to, aby zdarzenia o spodziewanym największym ryzyku zdarzały się ekstremalnie rzadko. Europejska Organizacja Bezpieczeństwa Żeglugi Powietrznej Eurocontrol proponuje podział zdarzeń na 5 kategorii, które w zależności od ich konsekwencji zdefiniowano w tablicy 1.

Tablica 1

Podział zdarzeń lotniczych

1	**Wypadek** (kolizja pomiędzy statkami powietrznymi między sobą, z pojazdami, z osobami, z przeszkodami) – zdarzenie to skutkuje ofiarami śmiertelnymi i zniszczeniem samolotu
2	**Poważny incydent** (szczęśliwe uniknięcie wypadku) – niemożność zapewnienia bezpiecznej służby kontroli ruchu lotniczego, nagłe manewry statku powietrznego w celu uniknięcia kolizji (ACAS)
	Główny incydent (kolizja prawdopodobna) – znaczące zaniżenie separacji
	Znaczący incydent (brak ryzyka kolizji) – powoduje zwiększenie obciążenia pracą kontrolera i pilota
	Bez bezpośredniego wpływu na bezpieczeństwo

Źródło: Eurocontrol

Aby w pełni opisać ryzyko danego zdarzenia, niezbędne jest określenie częstości występowania. W tym przypadku Eurocontrol proponuje schemat opisany w tablicy 2.

Tablica 2

Częstość zdarzeń lotniczych

A	**Ekstremalnie rzadkie/ekstremalnie nieprawdopodobne** – praktycznie nieprawdopodobne, aby wydarzyło się w czasie „życia systemu"
B	**Bardzo rzadkie/nieprawdopodobne** - praktycznie nieprawdopodobne, aby wydarzyło się w czasie „życia systemu", jednak może zaistnieć w wyjątkowych sytuacjach
C	**Rzadkie/prawdopodobne** - może zdarzyć się sporadycznie, rzadko
D	**Częste/prawdopodobne** - może wydarzyć się kilka razy w czasie „życia systemu"

Źródło: Eurocontrol

Zazwyczaj mają miejsce albo zdarzenia o kodzie 1A albo 5D. W celu kontynuowania analizy FHA i przejścia do jej ostatniego procesu – oceny bezpieczeństwa niezbędna jest znajomość wartości liczbowych ukrytych pod enigmatycznymi słowami „ekstremalnie rzadko", „bardzo rzadko" itd. Wspomniane wartości powinny zostać określone przez władzę lotniczą danego kraju. Jak dotychczas, na poziomie europejskim obowiązuje jedynie wartość liczbowa dla kategorii 1 „wypadki" określona na podstawie danych historycznych i wynosi $1{,}55*10^{-8}$ wypadku z przyczyn usterki systemu zarządzania ruchem lotniczym/1 lot. Przyjmując następujące założenia:

1 miesiąc = 1000 h = 10^3 h

1 rok=,10 miesięcy

1 rok = 10000 h =10^4 h

10^{-4} zdarzenia na godzinę oznacza, że wydarzy się ono z matematycznego punktu widzenia nie częściej niż 1 raz na rok

10^{-5} zdarzenia na godzinę oznacza, że wydarzy się ono 1 raz na dziesięć lat

10^{-8} zdarzenia na godzinę oznacza, że wydarzy się ono 1 raz na 10 tys. lat),

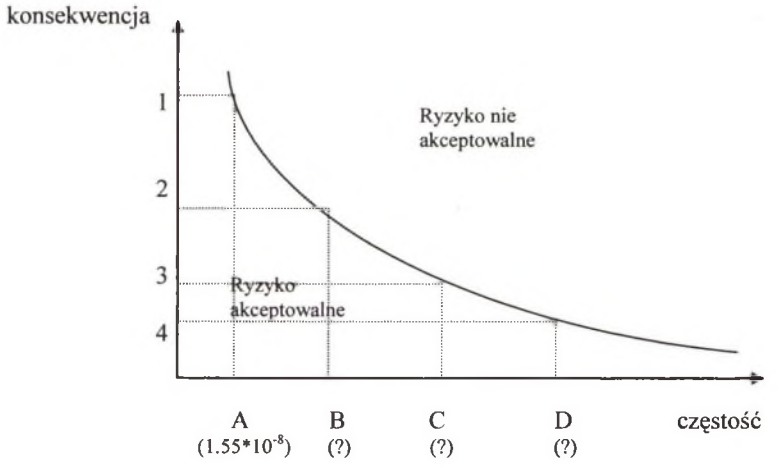
można określić co, w rozumieniu terminu „ekstremalnie rzadkie", oznacza wartość $1{,}55*10^{-8}$. Takie jest wymaganie odnośnie do bezpieczeństwa stawiane obecnym systemom zarządzania ruchem lotniczym. Mają one zapewniać takie bezpieczeństwo ruchu lotniczego, aby do wypadków lotniczych (nie innych zdarzeń) z ich winy nie dochodziło statystycznie częściej niż 1 raz na 10 tysięcy lat.

Problemem są wartości liczbowe dotyczące pozostałych 4 kategorii zdarzeń, które nie są obliczone i opublikowane. Wiadomo, że najbardziej zależy na tym, aby nie dochodziło do wypadków, w rezultacie których giną ludzie, dlatego w pierwszej kolejności opublikowano nieprzekraczalną wartość dla 1 kategorii - „wypadków". Należy liczyć się z tym, że i pozostałe zdarzenia doczekają się swoich nieprzekraczalnych częstości występowania.

Ocena ryzyka

W związku z tym, że błędy i usterki są nieodłącznym elementem planowania, pracy operacyjnej i utrzymania systemu zarządzania ruchem lotniczym, niemożliwe jest ich całkowite wyeliminowanie. Dlatego też ryzyko z nimi związane należy minimalizować do akceptowalnego poziomu. Akceptowalny poziom ryzyka jest to liczba niebezpiecznych zdarzeń danej kategorii, które miały miejsce w określonym czasie, wyrażona wartością liczbową niższą niż graniczna, obliczona i opublikowana dla tego zdarzenia. Taka graniczna wartość nazywana jest nieprzekraczalnym poziomem bezpieczeństwa TLS (*Target Level of Safety*). Akceptowalny poziom ryzyka inaczej nazywany jest bieżącym poziomem bezpieczeństwa CLS (*Current Level of Safety*). System jest bezpieczny, gdy ryzyko jest akceptowalne, czyli gdy CLS<TLS dla zdarzenia danej kategorii. Ponadto, przy określaniu akceptowalnej wartości liczbowej należy kierować się zasadą ALARA – tak nisko jak to tylko możliwe, ale ROZSĄDNIE. Należy mieć tu na uwadze, że nie chodzi o to, aby kosztem milionów złotych zainwestowanych w oprogramowanie lub sprzęt doprowadzić do tego, że częstość występowania zjawiska zmniejszy się np. z jednego na 95 lat do 1 na 100 lat.

Ogólna zasada, która jest stosowana do określenia akceptowalnego ryzyka, jest następująca: im poważniejsze są konsekwencje, tym mniejsza częstość występowania ryzyka. Schemat 2 przedstawia w formie logicznej akceptowalność ryzyka.



Rys. 2. Schemat akceptowalności ryzyka
Fig. 2. The scheme of risk acceptability

Schemat przedstawia podział obszaru ryzyka na dwie części:
- ryzyko nie akceptowalne: ryzyko jest tak duże, że nie może zostać przyjęte; należy albo usunąć przyczynę powodującą to ryzyko, albo tak je zredukować, aby stało się akceptowalne,
- ryzyko akceptowalne: ryzyko jest tak małe lub zostało tak zminimalizowane, że jest pomijalne lub akceptowalne.

Krzywa przedstawiona na wykresie obrazuje wspomniany już TLS. Skonstruowanie schematu 2 wymaga obliczeń na podstawie rzeczywistych danych o zdarzeniach w ruchu lotniczym oraz wiedzy eksperckiej, szczególnie w fazie określania, czy ryzyko jest akceptowalne czy też nie.

4. PODSUMOWANIE

W artykule przedstawiony został tzw. schemat klasyfikacji ryzyka (*Risk Classification Scheme*), składający się z trzech elementów:
- kategorii konsekwencji (A, B, C, D),
- kategorii częstości (1, 2, 3, 4),
- kryterium akceptowalności ryzyka (TLS/CLS).

Stanowi on punkt wyjścia do stałego monitorowania bezpieczeństwa świadczonych usług żeglugi powietrznej. Warto dodać, że jakakolwiek zmiana w systemie, np. zakup i instalacja nowego oprogramowania/urządzenia, ale również zmiana klasyfikacji przestrzeni powietrznej wymagają przeprowadzenia analizy wpływu tych zmian na bezpieczeństwo ruchu lotniczego. Tego wymaga system zarządzania bezpieczeństwem SMS. Jest to możliwe dzięki takim narzędziom, jak FHA, PSSA i SSA.

Literatura

1. Introduction to EATM System Safety Assessment Methodology and Functional Hazard Assessment. SAF-SAM1-FHA, Luxemburg 2005.
2. Malarski M., Kozłowski M.: Metody badania przyczyn i skutków zagrożenia bezpieczeństwa ruchu lotniskowego. XXXIII Zimowa Szkoła Niezawodności, Szczyrk 2005, s. 317-326.
3. Podręcznik Zapobiegania Wypadkom Lotniczym. Doc. 9422-AN/923, Luksemburg 2005.
4. Chmura W.: Problem nieprzekraczalnych poziomów bezpieczeństwa w ruchu lotniczym, I Międzynarodowa Konferencja Naukowo-Techniczna „Systemy Logistyczne - teoria i praktyka". Warszawa 2005, s. 123-128.
5. Chmura W., Malarski M.: Nieprzekraczalne poziomy bezpieczeństwa w ruchu lotniczym, XXXIV Zimowa Szkoła Niezawodności, Szczyrk 2006, s. 85-93.
6. Malarski M.: Bezpieczeństwo eksploatacji układu człowiek - złożone systemy transportowe. Zeszyty Naukowe AM Szczecin nr 11(83), Szczecin 2006, s. 195-202.