ZESZYTY NAUKOWE AKADEMII MARYNARKI WOJENNEJ
SCIENTIFIC JOURNAL OF POLISH NAVAL ACADEMY

2015 (LVI) 1 (200)

DOI: 10.5604/0860889X.1161254

Henryk Jafernik[1], Janusz Ćwiklak[1], Radosław Fellner[2]

SELECTED ASPECTS OF IMPLEMENTING A GNSS SYSTEM IN AVIATION

ABSTRACT

This article presents a risk analysis relating to the implementation of Localizer Performance and Vertical Guidance (LPV) procedures, using a GNSS sensor, for the airports in Warsaw and Katowice. Detailed information is included in a report worked out in the framework of an international project SHERPA. The results of this research were used to determine the probability of risk occurrence, and to set safety targets, as well as to refer them to an ILS system. Following the preliminary safety system assessment (PSSA), safety requirements indispensible for reaching the required safety level were determined. The requirements are presented in respective tables. It should be emphasized that the quantitative requirements were determined using fault tree analysis (FTA).

Key words:
GNSS, flight safety, flight procedures.

INTRODUCTION

Risk analysis is a key aspect in the implementation of navigation techniques, and technology's as well as land based aviation facilities. In this connection it is important to maintain a high reliability level of appliances, and correct identification of hazards, as well as enhance the safety of aviation operations. This work presents an analysis of risk relating to the implementation of Localizer Performance and Vertical Guidance (LPV) procedures for the airports in Warsaw and

[1] Polish Air Force Academy, Aeronautics Faculty, Department of Air Navigation, Dywizjonu 303/35 Str., 08-521 Dęblin, Poland; e-mail: {h.jafernik; j.cwiklak}@wsosp.pl
[2] Silesian University of Technology, Faculty of Transport, Krasińskiego 8 Str., 40-019 Katowice, Poland; e-mail: radoslaw.fellner@polsl.pl

Katowice using a GNSS sensor. It is assumed that these procedure will increase the safety level of operations Warsaw FIR [2].

RELIABILITY IN AVIATION

In aviation reliability is defined as the capability to meet established criteria which allow for carrying out aviation operations and missions in a specific time and conditions [5, 6, 7, 14]. It is connected with the necessity to carry out diagnostic, prophylactic, maintenance activities, and to some extent also forecasting activities in relation to airplanes as well as airport infrastructure and / or navigation systems. Therefore reliability is the capability of carrying missions which excludes existence of occurrences rendering it impossible to fulfill preset functions. In this connection the following are distinguished:

- Capability condition — in the case of full capability to carry out missions; incapability condition — when an operation is impossible to carry out it can be aborted or it may result in an accident or loss.

These conditions are affected by several factors, ranging from crew and maintenance (human factor), weather conditions, technical objects (machines, appliances) to procedures. Combinations of and changes in them can lead to conditions of incapability. Thus we can speak about a risk (possibilities, probabilities) of negative occurrences. It is worth noting that the International Civil Aviation Organization defines safety risk as probability and severity of consequence of risk occurrence, adopting the worst predictable situation as the point of reference [15]. The negative and undesirable occurrences can lead to loss. The probability of a loss occurrence will be referred to as a hazard.

SELECTED ASPECTS OF RISK ANALYSIS

Proper identification of hazards and risk analysis are elements of safety management in aviation, understood to be a set of actions and regulations whose aims are to maintain risk of causing harm at an acceptable level or to reduce a risk of occurrence of loss, failure or error.

Analysis methods are used to correctly identify hazards and assess their effects. They are as follows [13, 14]:

- FMEA (Failure Mode and Effects Analysis) — the analyzed object is divided into its component elements, and potential unreliability causes as well as cause--effect relations between them are determined;
- FTA (Fault Tree Analysis) — at the beginning final critical occurrence (effect) is determined and then the occurrences which may have led to it;
- ETA (Event Tree Analysis) — first determined are the occurrences that may lead to hazard occurrence;
- the risk to safety probability list — presents an assessment of a hazardous occurrence or condition in terms of possibility to occur (tab. 1);
- the risk to safety assessment matrix — it shows the probability of risk to safety occurrence together with severity of the occurrences (tab. 2).

The selection of the appropriate method depends on the available quantitative and qualitative data as well as on the complexity of factors affecting the safety.

Table 1. The risk to safety probability [9]

	Meaning	Value
Frequent	Probably will occur frequently (occurred frequently)	5
Sporadic	Probably will occur sporadically (occurred sporadically)	4
Low	Probably will not occur, but is possible (occurred rarely)	3
Unlikely	Very unlikely to occur (a case of occurrence has not been recorded)	2
Extremally unlikely	Almost unimaginable to ever occur	1

Table 2. The risk to safety assesment matrix [9]

Risk probability	Risk severity				
	Catastrophic A	Hazardous B	Serious C	Small D	Negligent E
Frequent 5	5A	5B	5C	5D	5E
Sporadic 4	4A	4B	4C	4D	4E
Low 3	3A	3B	3C	3D	3E
Unlikely 2	2A	2B	2C	2D	2E
Extremally unlikely 1	1A	1B	1C	1D	1E

SELECTED ASPECTS OF SAFETY CASE IN RELATION TO LANDING APPROACH OPERATIONS USING GNSS SATELLITE SYSTEMS

MPL Katowice and Pyrzowice and MPL Warsaw were the objects of safety analysis. The landings were carried out using certified GNSS receivers which employed satellite signals, mainly EGNOS. The details are included in the document ‘Polish National Scenario Report’ [9, 11] developed within the framework of the international project SHERPA. It should be mentioned that the implementation of SBAS LPV procedures constitutes another research level following the implementation of RNAV GNSS procedures in accordance with the ‘PANSA Navigation Strategy Plan and PANSA Airspace Strategy Plan’ [10, 11]. Hence, due to the methodology requirements, during the research a several stages were adopted:

1. First — hazard identification, connected with the use of SBAS LPV procedures, which are presented in detail by EUROCONTROL in ‘Final Functional Hazard Assessment of LPV approaches in the ECAC Area’. This was used to describe identified hazards (tab. 3).

Table 3. The list of identified hazards [9]

No.	Description of hazrd	Additional information
H3	Fly low while intercepting the final approach path (vertical profile)	Aircraft is in incorrect position approaching FAWP (below minimum procedure)
H4	Attempt to intercept the final approach path from above (vertical profile)	The conditions leading to this hazard are either failure to laterally intercept the final approach track (sequence resulting from H2) or aircraft at too high altitude prior to FAWP. In both cases aircrew fails to intercept the glide slope and, instead of launching a MA, decide to intercept it from above, in violation of the normal procedure
H6	Failure to follow the correct final approach path	Aircraft is in incorrect position at the final approach path
H7	Descending below DA without visual contact	Aircraft decends below DA whithout visual contact (incorrect procedure, incorrect QNH or incorrect DA)
H8	Failure to execute correct Missed Approach	Failure to maintain the correct flight profile while executing the procedure following Missed Approach

2. Second — hazard effect (operational effects) analysis, relating to the use of SBAS LPV procedures, which is also presented in detail by EUROCONTROL in ‘Final Functional Hazard Assessment of LPV approaches in the ECAC Area’ (tab. 4). The existing hazards were considered and then the results of the fault tree analysis were summarized (tab. 5).

Table 4. The hazard effect analysis [9]

No.	Hazard effect	Severity of hazard
C1	Controlled flight into terrain (CFIT)	Accident (effect severity 1)
C2	Landing accident (LA)	Accident (effect severity 1)
C3	Midair collision (MAC)	Accident (effect severity 1)
C4	Missed approach (MA)	Incident (effect severity 4)
C5	Safe landing	No effect

Table 5. Conclusions from FTA [9]

No.	Conclusions	Effects	Frequency
H3	No additional barriers identified in relation to FHA carried out by EUROCONTRL. The analysis did not take into account Safety Nets	CFIT	Warszawa 0.125 Katowice 0.125
H4	No additional barriers identified in relation to FHA carried out by EUROCONTRL. The analysis did not take into account Safety Nets	Landing accident	Warszawa 0.00025 Katowice 0.00025
H6	No additional barriers identified in relation to FHA carried out by EUROCONTRL. The analysis did not take into account Safety Nets	CFIT	Warszawa 0.125 Katowice 0.125
H7	No additional barriers identified in relation to FHA carried out by EUROCONTRL. The analysis did not take into account Safety Nets	CFIT	Warszawa 0.125 Katowice 0.125
		Landing accident	Warszawa 0.125 Katowice 0.125
H8	No additional barriers identified in relation to FHA carried out by EUROCONTRL. The analysis did not take into account Safety Nets	CFIT	Warszawa 0.0025 Katowice 0.0025
		Midair collision	Warszawa 0.00025 Katowice 0.00025

3. Third — safety targets were determined by adopting Target Level of Safety (TLS) and they were divided following the formula:

$$SO_{HX} = C * \frac{TLS_{accident}}{\prod(Q)} \tag{1}$$

where:

SO — safety target for particular hazards (Hx);
Q — probability of accident occurrence caused by a hazard;
C — severity of particular hazards leading to an accident.

TSL was calculated and presented together with reasoning in support of particular hazard effects in 'Final Functional Hazard Assessment of LPV approaches in the ECAC Area' and summarized in table 6 (TLS for LPV related hazard effects). At the same time an equal share of the particular hazard effects in TLS in the analysis was adopted in order to gain an additional buffer where the probability of hazard effect occurrence is lower due to, for example, the flight phase. Hence there appeared proposals relating to safety targets for: CFIT (tab. 7), landing accident (LA) (tab. 8), midair collision (MAC) (tab. 9). Then risk trees were derived determining safety targets: CFIT, LA, MAC. The above risk trees were used to calculate safety targets for the particular hazards (tab. 10).

Table 6. TLS for hazard effects relating to LPV [10]

Type of effect	LPV TLS
CFIT	1×10^{-8}
Landing accident	2×10^{-7}
Midair collision	1×10^{-10}

Table 7. Proposed safety target for CFIT [10]

H3	1.6e-8	20%
H4	N/A. Hazard does not lead to CFIT	
H6	1.6e-8	20%
H7	1.6e-8	20%
H8	1.6e-8	20%
Safety marigin	2e-9	20%

Table 8. Proposed safety targets for landing accident [10]

Hazard	Proposed safety target	Share in LA TLS
H3	Hazard does not lead to LA	–
H4	2.67e-4	33%
H6	Hazard does not lead to LA	–
H7	5.33-7	33%
H8	N/A. Hazard does not lead to LA	–
Safety marigin	5.67e-8	33%

Table 9. Proposed safety targets for midair collisions [10]

Hazard	Proposed safety target	Share in MAC TLS
H3	N/A. Does not lead to MAC	–
H4	N/A. Does not lead to MAC	–
H6	N/A. Does not lead to MAC	–
H7	N/A. Does not lead to MAC	–
H8	2e-7	50%
Safety marigin	5e-11	50%

Table 10. Proposed safety target for particular hazards [10]

No.	Description	Effects	Safety target
H3	Flying low while intercepting the final approach path (vertical profile)	MA, if detected. Safe landing when barriers are not detected or fail to work. GIFT when barriers when barriers are not detected or fail to activate	1.6e-8
H4	Attempting to intercept the final approach path from above (vertical profile)	MA or safe landing procedure when barriers effectively work. CFIT when barriers fail to work	2.66-4
H6	Failure to follow the correct final approach path	MA procedure if detected or when barriers effectively work. CFIT when barriers are not detected or fail to work	1.6e-8
H7	Descending below DA without visual	MA, if detected. Safe landing when barriers effectively work. Landing accident, if deviation is not toward obstacle and the other barriers fail to work. GFIT, if not detected or deviation is towards obstacle	1.6e-8
H8	Failure to execute correct Missed Approach	Negligible effect on safety, if detected and corrected — leads to MA or safe landing. GFIT, when all barriers fail to work, when deviation is toward obstacle. MAC, when all barriers fail to work and deviation is toward another a/c	2e-7

4. Fourth — qualitative and quantitative analysis (FTA) — working out fault trees determining probability of hazard occurrences based on the adopted probabilities of cause occurrences (FTA analysis) in relation to particular hazards. This was part of the preliminary system safety assessment.

It was justifiable to do both the quantitative and the qualitative analysis, due to the occurrence of similarities to the procedure of instrumental landing (ILS), which are certified, accepted, and safe. Based on EUROCONTROL guidelines it was assumed that for hazards H3 and H4 the risk is the same as for ILS, H6. Additional safety requirements were worked out in order to reduce risk (tab. 11).

Table 11. The safety targets in ILS analysis [10]

Hazard	Safety objective	Ocurrence probability achieved	Objective achievement
H3	Risk not higher than in the case of ILS (in accordance with PSSA Eurocontrol, see point 4.1 PSSA LPV)	Risk not higher than in the case of ILS (in accordance with PSSA EUROCONTROL)	Yes
H4	Risk not higher than in the case of ILS (in accordance with PSSA Eurocontrol, see point 4.2 PSSA LPV)	Risk not higher than in the case of ILS (in accordance with PSSA EUROCONTROL)	Yes
H6	1.6e-8	1.84e-6	No
H7	Risk not higher than in the case of ILS (in accordance with PSSA Eurocontrol, see point 4.4 PSSA LPV)	Risk not higher than in the case of ILS (in accordance with PSSA EUROCONTROL)	Yes
H8	2e-7	Risk not higher than in the case of ILS (in accordance with PSSA EUROCONTROL)	Yes

CONCLUSION

Resulting from the preliminary system safety assessment (PSSA) safety requirements, indispensible to reach the required safety level, were determined. The requirements are presented in respective tables. It should be emphasized that the quantitative requirements that were determined by means of FTA. Safety Nets were not considered in the calculations. This was caused by the absence of data relating to the functioning of Safety Nets in the new system.

REFERENCES

[1] *Air Navigation Report 2014*, ICAO Capacity Efficiency, 2014.

[2] Doc. 8168, PANS OPS, ICAO.

[3] Doc. 9613, PBN Manual.

[4] Doc. 9905-RNP, AR Procedure Design Manual, ICAO.

[5] ESARR 1, *Nadzór nad bezpieczeństwem w zarządzaniu ruchem lotniczym [Safety oversight in ATM]*.

[6] ESARR 2, *Raportowanie oraz analiza nieprawidłowości w ruchu lotniczym [Reporting and assementof safety occurences in ATM]*.

[7] ESARR 3, *Wykorzystanie systemu zarządzania bezpieczeństwem przez organy zarządzające ruchem lotniczym [Use of safety management systems by ATM service providers]*.

[8] ESARR 4, *Ocena bezpieczeństwa i redukcja ryzyka w systemie zarządzania ruchem lotniczym [Risk management nad mitigation in ATM]*.

[9] Fellner A., *SHERPA-PANSA-ENIP-D22EP EGNOS, National Implementation Plan*, 21.10.2013, ESSP — GSA, Praha.

[10] Fellner A., *SHERPA-PANSA-NSR-D21EP, Polish National Scenario Report*, 29.10.2013, ESSP — GSA, Praha.

[11] *Global Air Navigation Plan 2013–2020*, ICAO.

[12] *Guidance on hazards identification*, Safety Management System and Safety Culture Working Group (SMS WG), EASA, March 09.

[13] Lewitowicz J., Kustroń K., *Podstawy eksploatacji statków powietrznych — własności i właściwości eksploatacyjne statku powietrznego*, t. II, Warszawa 2003, s. 229–231 [*Fundamentals of operating aircraft — opersating properties and features of aircraft* — available in the Polish language].

[14] *Podręcznik zarządzania bezpieczeństwem, Doc 9859*, Urząd Lotnictwa Cywilnego, Warszawa 2009, s. 82–84 [*Safety Management Manual* — available in the Polish language].

[15] *Prawo lotnicze*, Dz.U. 2012, poz. 933, art. 68, *Obowiązki zarządzającego lotniskiem* [*Aviation Law*, Act of Law as of 20012, No. 933, art. 68, *Responsibilities of airport manager* — available in the Polish language].

[16] *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 [*The European Parliament and of the Council Regulation (EC) 216/2008 on common rules in the field of civil aviation and establishing EASA*].

WYBRANE ASPEKTY LOTNICZEJ IMPLEMENTACJI SYSTEMU GNSS

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 sprawozdaniu opracowanym w ramach międzynarodowego projektu SHERPA. Przeprowadzone badania pozwoliły na wyznaczenie prawdopodobieństw występowania zagrożeń i celów bezpieczeństwa, a także na porównanie ich z systemem ILS. W wyniku wstępnej systemowej oceny bezpieczeństwa (PSSA) określone zostały wymagania niezbędne do osiągnięcia właściwego poziomu bezpieczeństwa. Wymagania przedstawiono w odpowiednich tabelach, wymagania ilościowe zostały zdeterminowane za pomocą drzew FTA.

Słowa kluczowe:
GNSS, bezpieczeństwo lotów, procedury lotów.