TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 14
Number 3
September 2020

DOI: 10.12716/1001.14.03.14

Safety Case Activities in SHERPA Project

A. Fellner
Silesian University of Technology, Katowice, Poland

ABSTRACT: This paper has been issued in the framework of the SHERPA project under the Grant Agreement No 287246 with the GSA (European GNSS Agency). This document contains the main technical activities conducted by PANSA in the frame of project's WP2000. The objectives of WP2000 are: To work towards the implementation of a LPV procedure at each of the scenarios; To develop EGNOS National Implementation Plans, To develop and EGNOS Regional Implementation Plan, To summarise EGNOS expected benefits in a single airport. Specifically, the objectives of this document are technical activities conducted towards the implementation of a LPV procedure in scenario: procedure design, safety assessment, business case, EGNOS service provision requirements. The first step shall be to describe the operational environment at the scenario including the level of ATS provided, CNS equipment, the airport ground equipment, airspace and any procedures in place. The purpose of the operational description is to define the CONOPS specific to the airport. The Final FHA of LPV approaches is based on the Operational Model of LPV approaches in the ECAC Area, which clearly defined nominal operations prior to analyse degraded cases. For each operational action (performed by either system, human operator or jointly in the successive phases of flight), relevant failure modes were identified. Each failure mode was then analysed in turn in terms of examples of causes (to check its validity), operational consequences and mitigations, hazards, rough risk comparison against ILS operations, and when pertinent, recommendations in terms of risk reducing measures to be considered. Safety Case Activities drawn up as part of the SHERPA project was accepted by GSA, EUROCONTROL. At present an algorithm of acting while designing and executing procedures constitutes final approaches according to GNSS.

1 INTRODUCTION

The first step shall be to describe the operational environment at the scenario including the level of ATS provided, CNS equipment, the airport ground equipment, airspace and any procedures in place. The purpose of the operational description is to define the CONOPS specific to the airport. The objective is therefore to provide detailed information on the operational environment and compare it to.

2 LIST OF HAZARDS

The Final FHA of LPV approaches is based on the Operational Model of LPV approaches in the ECAC Area, which clearly defined nominal operations prior to analyse degraded cases. For each operational action (performed by either system, human operator or jointly in the successive phases of flight), relevant failure modes were identified. Each failure mode was then analysed in turn in terms of examples of causes (to check its validity), operational consequences and mitigations, hazards, rough risk comparison against

ILS operations, and when pertinent, recommendations in terms of risk reducing measures to be considered. A more detailed view on the hazards identification method is provided in the next section, where the Final FHA table is described. In deviation to the SAM FHA guidance, a brainstorming FHA session bringing together the adequate operational and technical experts was not possible given the constraints of the project and the experts' availability. Consequently, the work was organized as follows:

1 In a first iteration FHA tables were filled in by a safety expert, with support (questions/answers) from two technical experts;
2 Then several FHA working sessions were organized:
   - Three half-day working sessions were held with 3 technical experts from an airframer, among which one has a solid operational background as well; and
   - One half-day working session was held with ANSP relevant specialists: 4 APP, ATCO, one En-route ATCO and one technical expert.

During those working sessions, the operational model was first submitted to experts for validation, and then the FHA as initiated by the safety expert was submitted for discussion and further development. As the FHA table was projected on screen, conclusions of the discussions were recorded on-line on reaching agreement. Note that, as a mature operational concept is not yet available for the LPV operations, a major amount of effort (including the FHA working sessions) was spent to complete, refine and validate the operational model. The Final FHA table was submitted for review to a sub-set of RAFG participants and other relevant operational and technical experts. Main results of a Final FHA intermediary version and open issues were submitted to the validation of the operational and technical experts at the occasion of the Safety Assessment workshop mainly dedicated to the PSSA.

3 EVENT TREE ANALYSIS

The next step, which is the second part of the FHA, is to analyse the hazards with the help of event tree analysis. This methodology can be broken down into several steps:

1 Identify the hazard consequences and classify them according to severity of effects.

Table 1. Summary of consequences of hazards.

ID	Consequence	Severity of effect
C1	Controlled Flight Into Terrain (CFIT)	Catastrophic (Severity 1)
C2	Landing accident	Catastrophic (Severity 1)
C3	Mid-air collision	Catastrophic (Severity 1)
C4	Missed approach	Minor (Severity 4)
C5	Safe landing	No effect

2 Identify mitigations and their effect. The probability of any hazard leading to a catastrophic event (accident) is affected by mitigations. Mitigations are potential barriers which can prevent hazard leading to an accident. It is proposed to fill the following table:

Table 2. List of mitigations

ID	Mitigation	Description	Max probability of failure
M1	Deviation is not towards obstacle	Aircraft can wrongly fly at a lower altitude than the approach procedure minima or can deviate from the approach path or MA procedure path. Thus the aircraft is in a risk of CFIT. The mitigation of this risk is that there is no obstacle in that area and the approach/ manoeuvre/MA can be finished safely. In the generic safety case, EUROCONTROL proposed value 0.5. The value for Warszawa and Katowice was set to 0.5, but further reduction possible. Warszawa is not located in a mountainous area. In addition, the approach path is relatively obstacle free (this was included in the NPA GNSS approach safety assessment).	Warszawa 0.5 Katowice 0.5
M2	Deviation is not towards another aircraft	Aircraft can wrongly deviate from the approach path or MA procedure path. Thus the aircraft is in a risk of mid air collision. The mitigation of this risk is that there is not any traffic in the vicinity of the aircraft on approach, hence the deviation is not towards another, aircraft. In the generic case EUROCONTROL used value 0.05. The values for Warszawa due to crossing RWY is being reviewed and Katowice -specific value is consistent with this. Probability of deviation towards another aircraft depends on multiple parameters (e.g. airport & runways configuration, departure routes structure, etc). Although it could be fairly assumed that the probability of having two aircraft in the same airspace with conflicting trajectories is much lower than the probability to converge to obstacles, the proposed value for flying towards an aircraft is Q = 0.05.	Warszawa 0.05 Katowice 0.05
M3	Missed Approach (MA) timely initiated and correctly executed	The aircraft may deviate from the final approach path (vertically or laterally), air crew may detect some FAS errors or can fail to establish visual contact with the RWY above DA, and thus will initiate MA to avoid CFIT or landing accident. EURCONTROL used probability value of 0.5 in the generic safety case.	Warszawa 0.5 Katowice 0.5

M4	Approach is stabilising	Air crew can fail to laterally intercept the final approach path or aircraft can be too high before FAWP. In such situation, air crew can decide to intercept the final approach path from above, in violation of the normal procedure. On deciding to capture the glide slope from above, the flight crew have some confidence on succeeding. However, this manoeuvre involves certain risk that the crew will not be able to stabilise the aircraft path. The mitigation is that crew is able to stabilise the aircraft (intercept the final approach path, decelerate to extend flaps and landing gear) on time and land safely. EUROCONTROL’s probability of failure of this mitigation is 0.1. The value for Warszawa and Katowice is consistent with it.	Warszawa 0.1 Katowice 0.1
M5	Aircraft is in right position for landing	Crew may decide to descend below DA without visual. This involves a risk of CFIT. However,if aircraft manages to descend safely to an altitude where visual contact is established, it can be in right position for landing. EUROCONTROL’s probability of failure for this mitigation is 0.5. The value for Warszawa and Katowice is consistent with it. Value for this mitigation reflects the degree of information available by this time. According to EUROCONTROL, when further information is collected,this figure might evolve.	Warszawa 0.5 Katowice 0.5
M6	Recovery with visual cues	Proximity to terrain, obstacle or another aircraft can be recovered by the flight crew via visual cues by launching a MA or avoidance manoeuvre. The effectiveness of this mitigation depends on the number of factors, such as weather, day/night, airport lighting, surrounding vicinity lighting, etc. For this reason the probability of failure has to be rather conservative and is consistent with EUROCONTROL’S assumption in the generic safety case. Difference in airport lighting in favour for Warszawa so value could be further decreased.	Warszawa 0.5 Katowice 0.5
M7	Recovery with visual cues – specific to missed approach (H8)	Proximity to terrain, obstacle or another aircraft can be recovered by the flight crew via visual cues by launching a MA or avoidance manoeuvre and is assumed to be 0.5 for M8 when the aircraft is on final approach path. Note that M7 mitigation during MA is considered five times more efficient than on final approach path. On final approach, guidance is very accurate and has a high integrity. One can assume that the crew will trust this and therefore will less monitor the final path itself. During missed approach, the crew is aware of the route to fly, and of the fact that precision is lower than on final approach. Also, as the route is not converging towards a known point, the crew will be more involved in the navigation process than it was during final approach. Therefore, fail of recovery via on-board detection of incorrect MA path execution is assumed 0.1 and is consistent with EUROCONTROL’S probability of failure.	Warszawa 0.1 Katowice 0.1
M8	Recovery via aircrew detection onboard	Recovery via aircrew detection onboard mitigates risk resulting from deviating from the correct final approach path or MA path. Some deviations are noticeable (e.g. magnetic heading differs from what is expected, too high or too low vertical speed, abnormal engine thrust settings, sudden deviation due to some discontinuity), other cannot be determined, especially deviations at the end of the FAS are the most dangerous. Aircrew might detect discrepancies with respect to chart by monitoring the distance to threshold (displayed to pilots) which allows them to roughly estimate if current height is right (about 300 ft resolution) compared to altitudes on the charts. With regard to these various means a rough probability of 0.5 for recovery via aircrew detection was defined. This is in line with EUROCONTROL’s probability of failure.	Warszawa 0.5 Katowice 0.5
M9	Recovery via ATC radar detection	The ATCO detection that an aircraft flies low while intercepting the final approach path strongly depends on the size of the vertical deviation and the distance to runway. A 1000 ft Mode C deviation at 8 Nm away from the runway should attract his attention. Based on that, the adopted probability for detection and recovery is 0.5	Warszawa 0.5 Katowice 0.5
M10	External conditions (runway dry or long, luck…)	Even when the aircraft is not in perfect landing conditions above the runway threshold, this should not necessarily lead to a landing accident: Probability that External conditions (runway dry or long, luck…) favour collision is 0.01. In both cases the value was consistent with EUROCONTROL’s probability of failure.	Warszawa 0.01 Katowice 0.01

3 Analyse the hazard consequences with the use of event trees. Analyse the hazard consequences with the use of event trees, in order to allow assessing the risk associated to those hazards. Once the analysis is done, it is proposed to States to provide the final conclusion for each of the hazards by means of the following table:

Table 3. Summary of event trees analysis

ID	General conclusion	Consequence	Frequency
H3	No additional barriers as to EUROCONTROL FHA identified. The safety nets were not included in this calculation.	CFIT (catastrophic)	Warszawa 0.125 Katowice 0.125
H4	No additional barriers as to EUROCONTROL FHA identified. The safety nets were not included in this calculation.	Landing accident (catastrophic)	Warszawa 0.00025 Katowice 0.00025
H6	No additional barriers as to EUROCONTROL FHA identified. The safety nets were not included in this calculation.	CFIT (catastrophic)	Warszawa 0.125 Katowice 0.125
H7	No additional barriers as to EUROCONTROL FHA identified. The safety nets were not included in this calculation.	CFIT (catastrophic)	Warszawa 0.125 Katowice 0.125
		Landing accident (catastrophic)	Warszawa 0.125 Katowice 0.125
H8	No additional barriers as to EUROCONTROL FHA identified. The safety nets were not included in this calculation.	CFIT (catastrophic)	Warszawa 0.0025 Katowice 0.0025
		Midair collision (catastrophic)	Warszawa 0.00025 Katowice 0.00025

4 Establish the TLS - identify relevant categories of accidents and find target level of safety for each of these accidents. It is proposed to fill the following table:

Table 4. Summary of LPV TLSs

Accident type	LPV TLS
Controlled Flight Into Terrain (CFIT)	1×10^{-8}
Landing accident	1×10^{-10}
Mid-air collision	2×10^{-7}

5 Allocate safety objectives - allocate TLS from step 1 for each type of accident to individual hazards by using risk tree analysis. Risk trees for individual accident categories shall be prepared. Allocation has to be done apportioning the TLS among the branches that compose each risk tree. Then, the Safety Objectives will determine the allocation of Safety Requirements to system elements in the fault tree analysis. Using the probabilities coming from the previous section:

$$SO_{HX} = C \cdot \frac{TLS_{accident}}{\Pi(Q)} \qquad (1)$$

where:
Q are the event probabilities in sequences initiated by Hazard X that end up in the applicable accident;
C is the allocation chosen for each branch of the trees.
The candidate Safety Objectives for each accident shall be presented in the next table (a new table must be generated for each accident):

Table 5. Candidate safety objectives for CFIT

Hazard	Candidate Safety Objective	Contribution of the branch to CFIT TLS
H3	1.6e-8	20%
H4	Not applicable - Hazard does not lead to CFIT	
H6	1.6e-8	20%
H7	1.6e-8	20%
H8	1.6e-8	20%
Safety margin	2e-9	20%

Table 6. Candidate safety objectives for landing accident

Hazard	Candidate Safety Objective	Contribution of the branch to the landing accident TLS
H3	Not applicable - Hazard does not lead to LA	-
H4	2.67e-4	33%
H6	Not applicable - Hazard does not lead to LA	-
H7	5.33-7	33%
H8	Not applicable - Hazard does not lead to LA	-
Safety margin	5.67e-8	33%

Table 7. Candidate safety objectives for MAC

Hazard	Candidate Safety Objective	Contribution of the branch to the MAC TLS
H3	Not applicable - Hazard does not lead to MAC	-
H4	Not applicable - Hazard does not lead to MAC	-
H6	Not applicable - Hazard does not lead to MAC	-
H7	Not applicable - Hazard does not lead to MAC	-
H8	2e-7	50%
Safety margin	5e-11	50%

6 Derive final Safety Objectives: when one hazard has more than one ultimate consequence (i.e. contributes to more than one type of accident), the most constraining objective has to be kept. Please fill the following table:

Table 8. Final safety objectives

ID	Title	Consequences	SO in environment
H3	Fly low while intercepting the final approach path	Missed approach if detected. Safe landing if undetected and barriers work. CFIT if undetected and barriers fail	1.6e-8
H4	Attempt to intercept the final approach path from above	Missed approach or safe landing if barriers work. CFIT if barriers fail	2.66-4
H6	Failure to follow the correct final approach path	Missed approach or safe landing if detected and/or barriers work. CFIT if undetected and barriers fail	1.6e-8
H7	Descending below DA without visual	Missed approach if detected. Safe landing if barriers work. Landing accident if deviation is not towards obstacle but other barriers fail. CFIT if undetected and in case deviation is towards obstacle	4e-9
H8	Failure to execute correct missed approach	No major impact on safety if detected and corrected-ultimate result would be missed approach or safe landing. CFIT if all barriers fail and deviation is towards obstacle. MAC if all barriers fail and deviation is towards aircraft	2e-7

4 FAULT TREE ANALYSIS

The Fault tree analysis consists in apportioning the Safety Objectives of each hazard into Safety Requirements to elements of the system. In other words, one fault tree analysis has to be done for each of the hazards identified in Table. The fault tree analysis contains all the causes that can potentially incur to the hazard. States are aimed to develop the fault trees and perform the associated qualitative and quantitative analyses.

The probability of occurrence of each of the causes must be combined as specified by the developed fault tree (sequence of AND and OR functions) to obtain the final probability of occurrence for each hazard.

Obviously, probability of occurrence shall be lower than the applicable Safety Objective. In case that the Safety Objective is not met, it is necessary to define additional:

- Safety Requirements (SR), which define additional functions to those already mentioned in the nominal case; or
- Integrity Requirements (IRs), which define the level of performance of certain elements and functions.

To summarise the final results of the fault tree analysis, it is proposed to States to fill in the following table:

Table 9. Summary of all hazards' achieved probability of occurrence

Hazard ID	Safety Objective	Achieved probability of occurrence	Objective met
H3	1.6e-8	Idem (according to Eurocontrol PSSA)	Yes
H4	2.66-4	Idem (according to Eurocontrol PSSA)	Yes
H6	1.6e-8	1.84e-6	No
H7	4e-9	Idem (according to Eurocontrol PSSA)	Yes
H8	2e-7	Idem (according to Eurocontrol PSSA)	Yes

5 CONSEQUENCES ANALYSIS

Consequences analysis involves identifying the sequences of events initiated by an OH, defined by the success/failure of a series of barriers or other relevant events and ending up in unacceptable end consequences (accidents like CFIT, MAC and landing accident) that are usually used in the NAV domain. TLS-DNV clarifies what events are covered by these accident categories:

- **Mid-air collision** is where two aircraft come into contact with each other while both are airborne. This includes any in-flight collision between an aircraft and another flying vehicle, whether commercial, military or general aviation, including microlights, hang-gliders, gliders and balloons. It excludes collisions caused by hostile attack (i.e. terrorism, hijack, sabotage or military attack) but includes collisions caused in all other ways. This is consistent with the CAST/ICAO common terminology for mid-air collision;
- **Controlled flight into terrain (CFIT)** is an in-flight collision with terrain, water or another obstacle without prior loss of control. This excludes intentional flight into terrain/buildings due to hostile attack. It also excludes cases where the aircraft lands short or to one side of the runway (covered under landing accidents). It includes cases where the CFIT follows or is caused by an in-flight disruption such as a fire or engine failure, provided that flight control is maintained. This is consistent with the CAST/ICAO occurrence category "controlled flight into or toward terrain";
- **Landing accidents** include all types of accidents during the landing phase of flight (see below), other than collision. This includes abnormal runway contacts (e.g. hard landings, gear-up landings), loss of control on the runway (e.g. due to wind-shear or surface contamination), runway incursions (e.g. by animals, vehicles or people, but not aircraft), runway excursions (e.g. veer-off, overrun), off-runway touchdown (e.g. undershoot, overshoot and offside touchdown). It includes external causes (e.g. snow/ice/rain and wind-shear), technical causes (e.g. gear failure) and human causes (e.g. flight crew misjudgements). It includes cases where the landing accident follows or is caused by an in-flight disruption such as a fire or engine failure, provided that sufficient control is maintained to attempt a normal or emergency landing. It includes cases where the landing accident is followed by collision with another aircraft outside the runway. There is no specific CAST/ICAO equivalent for this term.

The consequences analysis is performed using the Event Trees, but only the event sequences relevant for the safety assessment (which determine the Safety Objectives) are shown in the subsequent tables. The full Event Trees, providing a graphical representation of all the sequences of events developing subsequently to an operational hazard (OH) occurrence and their final outcomes, are provided in Annex IV. Rough probability values will be assumed for the events/barriers occurrence, based on field feedback experience, expert judgement and other qualitative considerations that will be duly justified. In a first version of the FHA, efficiency of the ground and airborne safety nets equipage were considered as potential barriers to prevent accidents. In the final version of the FHA they do not more influence the safety objectives determination process. Meanwhile their impact on the consequences analysis is provided for information in annex V.

REFERENCES

APV SBAS Approach - Concept of Operations, CONOPS, 2009;

Operational and Functional model of LPV approaches in the ECAC area, OFM-LPV 2.0 2007;

Draft Guidance Material for the Implementation of RNP APCH Operations PBN TF6 WP06 Rev 1 05/01/2012

SHERPA Grant Agreement Grant number 287246

EASA - AMC 20-26 : Airworthiness Approval and Operational Criteria for RNP AR Operations;

EASA - AMC 20-27: Airworthiness Approval and Operational Criteria for RNP APPROACH (RNP APCH) Operations Including APV BARO VNAV Operations;

EASA - Helicopters Deploy GNSS in Europe (HEDGE) project documentation,

EATMP Navigation Strategy for ECAC;

EGNOS Introduction in European Eastern Region MIELEC project documentation,

EUR Document 001/RNAV/5 Guidance Material Relating to the Implemen-tation of European Air Traffic Management Programme;

FAA - AC 20-105: Approval Guidance for RNP Operations and Barometric Vertical Navigation in the U.S. National Airspace System;

FAA - AC 20-129: Airworthiness Approval for Vertical Navigation (VNAV) Systems for Use in the U.S. National Airspace System (NAS) and Alaska;

FAA - TSO C146A: Stand-Alone Airborne Navigation Equipment Using the Global Positioning System Augmented by the Wide Area Augmentation System (WAAS);

FAA: TSO C145A: Airborne Navigation Sensors Using the Global Positioning System (GPS) Augmented by the Wide Area Augmentation System (WAAS);

Fellner A. SHERPA-PANSA-NMA-D11EP Issue: 01-00 EGNOS Poland Marked Analysis, 2012

Fellner A. SHERPA- PANSA-NSR-D21EP,2014

ICAO Annex 10,

ICAO Doc 8168 – PANS-OPS,

ICAO Doc 9613 – PBN Manual,

ICAO Doc 9905 – RNP AR Procedure Design Manual

ICAO Doc. 7754 European Region Air Navigation Plan;

ICAO European Region Transition Plan to CNS/ATM;

ICAO Global Air Navigation Plan for CNS/ATM Systems. Doc 9750;