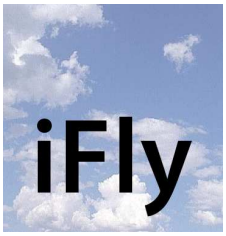

Project no. TREN/07/FP6AE/S07.71574/037180 IFLY

iFly

Safety, Complexity and Responsibility based design and validation of highly automated Air Traffic Management

Specific Targeted Research Projects (STREP)

Thematic Priority 1.3.1.4.g Aeronautics and Space

iFly Deliverable D9.2: ED78a/DO-264 based Operational Hazard Assessment and Allocation of Safety Objectives and Requirements of Airborne Self-Separation Procedure

Honeywell

Version: 1.4

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

DOCUMENT CONTROL SHEET

Title of document:	***iFly Deliverable D9.2: Operational Hazard Assessment (OHA) and Allocation of Safety Objectives and Requirements (ASOR) of Airborne Self-Separation Procedure (SSEP)***
Authors of document:	Eva Gelnarová, Jaroslav Jonák
Deliverable number:	*D9.2*
Project acronym:	*IFly*
Project title:	*Safety, Complexity and Responsibility based design and validation of highly automated Air Traffic Management*
Project no.:	*TREN/07/FP6AE/S07.71574/037180 IFLY*
Instrument:	*Specific Targeted Research Projects (STREP)*
Thematic Priority:	*1.3.1.4.g Aeronautics and Space*

DOCUMENT CHANGE LOG

Version #	Issue Date	Sections affected	Relevant information
Draft 0.1	25 April 2010	All	
1.0	21 May 2010	1,2,4,Appendixes 4,8,9 and 10/All	
1.1	2 July 2010	1,4,Appendix 4	Reaction to NLR feedback
1.2	21 July 2010	1,4,6, Appendices 4,7,8,9	Reaction to NLR feedback
1.3	20 August 2010	Editorial changes	Reaction to NLR feedback
1.4	25 February 2011	All	Reaction to EC feedback

Version 1.1		Organisation	Signature/Date
Authors	Eva Gelnarová	HNWL	
	Jaroslav Jonák	HNWL	
Internal reviewers	Petr Císek	HNWL	
	Silvie Luisa Brázdilová	HNWL	
	Henk Blom	NLR	
	Claudia Keinrath	HNWL	
External reviewers	Uwe Voelckers	EC ext. reviewer	

Contents

1. Introduction

The iFly project picks up the challenge of studying the feasibility of airborne self separation in high density airspace. Instrumental to this feasibility study, iFly aims to develop an advanced airborne self separation design together with a vision how well-equipped aircraft can be integrated within SESAR. iFly does not intend to develop a fully defined airborne self separation design, but aims to investigate the boundaries of an advanced airborne self separation concept of operations.

The iFly Work Package WP9, which builds on the iFly:D1.3 report started with WP9.1 which provided the description of the operational environment and the air traffic services required by the A3 concept. In line with this, the outcome of WP9.1 was an *Operational Services and Environment Description (OSED)* document of the A3 ConOps, which served as an base for Operational Safety Assessment (OSA) that has been performed within WP9.2, resp. Operational Safety Assessment (OPA) that has been performed within WP9.3 running in parallel to WP9.2.

During OSA process, the main operation hazards are to be identified together with localization of their basic causes and operational effects. The implemented safety requirements, risk mitigation means which would reduce the operational effect of operational hazard, should be formulated.

Operational Safety Assessment (OSA) of Airborne Self-Separation Procedure (SSEP) document delivered as a result of WP9.2 was developed in accordance with the guidelines provided by EUROCAE ED-78A/RTCA DO-264. However process is usually implemented in later stage of procedure development.

1.1 The Scope of Operational Safety Assessment

OSA developed within WP 9.2 builds on A3 ConOps which concentrates on the airborne self separation for en-route operations in a net centric environment where only appropriately equipped aircraft fly. The responsibility for airborne self-separation lies entirely on so called autonomous aircraft (combination of airborne system and the flight crew) without ground support from air traffic controllers.

OSA strictly follows the A3 self-separation concept described within iFly:D1.3 and iFly:D9.1 – OSED for SSEP. Only aircraft state and intent information are broadcast via ADS-B. There is no space left for aircraft/aircraft or aircraft/ground explicit communication, which would include mutual information exchange on dialog basis. Similarly, no explicit conflict detection or resolution coordination among involved aircraft is expected. Some space for voice communication is left solely for emergency situations.

Inherent to the innovative nature of the iFly project, its research activities are aligned with E-OCVM phase V1, i.e., setting the **scope** of Airborne Self Separation under very high traffic demands. Since ED78a/DO-264 are aimed for prime application in a much later E-OCVM phase, not all ED78a/DO-264 steps can be performed at the right level of detail in this phase (for example detailed tasks and functions

allocation is not yet possible). In this context, this OSA presents the initial concept, the logic and causality structure of identified operational hazards, but there is not a solid foundation to provide the quantitative requirements analysis (e.g., allocation of safety objectives) at this research phase.

The attention has been limited towards pairwise conflicts, as described in iFly: D9.1 scenarios. Scenarios covering multi-aircraft conflicts are not considered. This limitation in analysis might have significant impact on the results obtained; this however is left for study outside WP9.

1.2 Document Organization

After a short introduction (*Chapter 1*), the problematic of airborne self-separation is recapitulated based on OSED results (*Chapter 2*). The assumptions on operational environments and other assumptions used throughout this document are also introduced.

Chapter 3 brings a short Operational Safety Assessment (OSA) methodology description together with detailed discussion on steps which have been omitted (OSA provided in current document lacks the numerical probability assessment).

First of all, the operational hazards are identified in *Chapter 4.* The operational hazards are the results of autonomous aircraft states analysis. Further the relationship of these operational hazards with hazards from WP2 and WP7 is discussed. This introductory part is followed by the Operational Hazard Assessment (OHA) section, where External Mitigation Means (EMMs) are formulated. Finally the Allocation of Safety Objectives and Requirements (ASOR) section contains a list of Basic Causes (BC) with Safety Requirements and Internal mitigation Means (IMMs).

Chapter 5 is devoted to a detailed analysis of all identified operational hazards. Event trees accompanied with barriers and fault trees are components of a comprehensive operational hazard analysis.

The core part of the document formed by Chapters 4 and 5 is followed by a number of Appendixes:
Appendix 1 contains proposals of Safety Requirements, which could be beneficial to mitigate the operational hazard severity, but currently they do not appear in a SSEP concept of operation (iFly: D1.3).
Appendix 2 summarizes all Operational, Performance and Functional Requirements, which have appeared in OSED (iFly: D9.1).
Appendix 3 is a supplement to Chapter 2. Although the OSA methodology is well described elsewhere, most important definitions are formulated together with their SSEP OSA specifications in Appendix 3.
Appendix 4 provides a mapping of hazards indentified during MFF brainstorming session and iFLY WP2 session on operational hazards and mitigation means identified during OSA process. Results of this appendix built a bridge between iFly WP7.1 and iFLY WP 9.2. This appendix is a supplement to a subsection of Chapter 4.
Appendix 5 is devoted to emergency and non-normal procedures, originally described in iFly: D1.3.
Appendix 6 is a Hazard Classification Matrix.

Appendixes 7 makes an interconnection between WP9.2 and WP 2.4. The levels of automation proposed in iFly: D2.4 served as a base for flight crew role identification. *Appendix 7* presents as well how the main Automation related problems indentified in iFly: D2.4 were treated by OSA mitigation means.

The document itself is closed up with a List of Abbreviations (*Appendix 8*) and a List of References (*Appendix 9*).

2. Airborne Self-Separation

The following chapter is devoted to a short summary of Operational Services and Environment Description of Airborne Self-Separation Procedure as developed in iFly: D9.1.
As there were presented more environments and service levels for SSEP, we specify the characteristics directly assumed within OSA process further.

2.1 SSEP Operation Overview

After World War II, the Air Traffic Management system has utilized a concept, where the responsibility for aircraft separation lies solely on air traffic controllers. Aircraft fly along predefined flight paths and each aircraft is monitored by a controller, who has an overview of the situation in his sector and beyond and guides aircraft towards their destinations via a sequence of waypoints.

The motivating idea for airborne self separation is the possibility to overcome the performance limitations of the current system by taking advantage of using distributed control principles and new airborne technologies. In particular, data links will enable aircraft to monitor their surroundings and develop a "big picture" about the traffic and other hazards themselves. It is expected that the information about the surrounding environment will be sufficiently accurate and reliable, so – with substantial support from advanced on-board equipment – the flight crew will be able to assess the situation, plan the trajectory and avoid conflicts with aircraft or other hazards.

A typical airborne self separation flight may have the following progression: An aircraft takes off from the airport and climbs through the departure TMA, where the traffic flow is controlled by the Air Navigation Service Provider (ANSP) who is responsible for aircraft separation. For each flight there is an agreed and shared flight trajectory (so-called Reference Business Trajectory (RBT)) up to the destination allowing to balance the capacity/demand en-route and at the destination TMA and airport. For this purpose there is a flow constraint associated to the flight at the entering fix of the destination TMA in the form of a 3D point with a Constrained Time of Arrival (CTA) restriction.

When leaving the departure TMA, the responsibility for separation is shifted from the ANSP to the flight crew. The following en-route part of the flight (located within so-called Self Separation Airspace (SSA)) is performed according to SSEP operations. During this phase of flight, the flight crew can modify the SSA-part of the RBT without negotiation with any ANSP (but taking into account the relevant traffic), provided that defined Autonomous Flight Rules (AFR) are satisfied and that the CTA at the destination TMA will be achieved. Nevertheless, if there is a need to modify the CTA constraints, such change must be negotiated with the ANSP at the destination TMA. The aircraft need not to follow any predefined airway structure.

Within SSA the information exchange among aircraft will primarily be assured through data link, voice communication (for instance, among imminent aircraft) will be limited and used mainly in emergency situations. The aircraft has to continuously broadcast information about its state and if possible intent, to allow other participants to predict its planned trajectory. The goal of the self separation operations described in the OSED is to prevent Loss of Separation (LoS), collision avoidance (preventing a collision in the case of LoS) being handled in the same way as within the ATC-managed airspace.

In case of a conflict, the involved aircraft will not broadcast any additional information and there is no requirement for any additional individual data exchange. The coordination of actions among conflicting aircraft is enabled by the set of rules included in AFR, which are binding for all participants. Based on these rules there are two types of Conflict Resolution (CR) processes:

- For urgent conflicts (time to predicted LoS shorter than a predefined threshold) all conflicting aircraft must maneuver and the applied maneuvers shall be coordinated through so-called **implicit coordination**. The latter is based on the use of compatible algorithms that generate complementary maneuvers for conflicting aircraft.

- Conflicts with the time for maneuvering greater than the predefined threshold are solved using the **Priority rules principle**. This means that there are predefined rules which assign a priority number to each aircraft and the conflict is actively solved only by aircraft with a lower priority. The aircraft with higher priority simply continues to fly its original trajectory. The priority of aircraft evolves during the flight and is primary determined by the aircraft maneuverability, mission statement and the remaining time to CTA (when an aircraft has to meet a time constraint, it has higher priority).

To ensure separation and onboard trajectory management tasks, the flight crew takes advantage of the onboard equipment, which is monitoring the surroundings and helps the flight crew to detect and resolve conflicts. When a conflict is detected, the onboard equipment proposes a solution, which is assessed by the flight crew. When the solution is approved by the flight crew, the flown trajectory is updated and the aircraft broadcasts its new state and intent information. Note, that **any processes directly influencing (beyond a threshold which should be defined) the flown trajectory may be executed only when approved by the flight crew.**

When the aircraft approaches the destination TMA, the responsibility for separation is shifted back from the flight crew to the ANSP and the self-separation part of the flight is terminated.

The scope of the A3 ConOps , OSED and OSA is not to describe the whole self separation flight but to focus only on its part within SSA. Therefore the transitions procedures and operations in the departure and terminal TMA are omitted.

2.2 Operational Environment and Other Assumptions

The following environmental conditions were assumed through the OSA process of SSEP procedure. Assumptions presented in Tables 2-1 and 2-2 origin in OSED (iFly: D9.1). OSED identified operational, performance and functional requirements may be found in Appendix 2.
Table 2-3 contains additional assumptions and restrictions that have been respected during SSEP OSA development.

Table 2-1: Assumptions - Environmental conditions and communication.

Assumption	Description	Location of assumption in OSED (iFly:D9.1)
ASSUMP-1 - EC	Only ASAS equipped aircraft – so called ”autonomous aircraft” flying under AFR	Page 9
ASSUMP-2- EC	En-route phase of the flight in so called SSA, the transition procedures (SSA towards MA and vice versa) are not discussed in the iFly framework.	Page 9
ASSUMP-3 - EC	User preferred routing and no flight levels binding	Page 9
ASSUMP-4 - EC	Airspace boundaries are dynamically allocated.	Page 9
ASSUMP-5 - COM	All aircraft broadcast its state together with intent via ADS-B	ADS-B Initial Performance Assumptions Page 10
ASSUMP-6 - COM	Information provided to/by a ground supporting system (SWIM)	SWIM General and SSA-Based Assumptions Page 10
ASSUMP-7 - COM	HF voice left mainly for emergency procedures.	Page 9
ASSUMP-8 - COM	No explicit communication Only implicit coordination for short term conflict	IfLY: D1.3 Chapter 8.6

Table 2-2: Initial assumptions / performance estimates

Assumption	Description	Location of assumption in OSED
ASSUMP-1-INI	Quality of broadcast information corresponds to the standard value of RNP required during the en-route phase of flight.	Navigation FB, page 28
ASSUMP-2-INI	Broadcast state information has got a form of State Vector, Mode Status and Air Referenced Velocity Report (DO-260A)	Navigation FB, page 28
ASSUMP-3-INI	MLAT=10min, SLAT=3 minutes	Surveillance FB, page 30

ASSUMP-4-INI	Air-Air datalink range is 90NM (120 NM desired)	Surveillance FB, page 30
ASSUMP-5-INI	When a new conflict appears during CR process, the CR should not be interrupted except well defined conditions. "Restart conditions" to be defined in Safety requirement chapter (see Appendix 1: Safety requirements – new proposals.)	Events handling FB, page 30
ASSUMP-6-INI	Mid-term conflict resolution algorithm is always able to find a solution	Trajectory modification FB, page 31
ASSUMP-7-INI	CPP (mid-term) should take no longer than maximally predefined time (first estimation 2 min)	Trajectory modification FB, page 31
ASSUMP-8-INI	Short-term conflict resolution algorithm is always able to find a solution	Tactical maneuver FB, page 31
ASSUMP-9-INI	CPP (short term) should take no longer than maximally predefined time (first estimation 30sec)	Tactical maneuver FB, page 31

Table 2-3: OSA specific assumptions.

Assumptions – others OSA specific	Description
ASSUMP-1-OTH	Priority number determination as stated in iFlyD1.3 used only in case of pairwise conflict
ASSUMP-2-OTH	ACAS is not considered as a part of SSEP and is not a synonym to *Emergency procedure;* SSEP does not modify ACAS procedures
ASSUMP-3-OTH	**Only pairwise conflicts – simplified scenarios, no multi-aircraft conflicts will be discussed within SSEP OSA.**
ASSUMP-4-OTH	Security issues are outside the scope of this document. The intentional violation of AFR or mischievous acting by flight crew is not considered.
ASSUMP-5-OTH	Technical realization of flight and connected (technology implementation) problems are not investigated. It is supposed that the feasibility of flight is guaranteed.

3. Operational Safety Assessment Methodology – Brief Description

Since the OSA methodology has already been well described elsewhere, it is not a point to duplicate the effort. The fundamental source is a document EUROCAE ED-78A/RTCA DO-264. More detailed OSA manual together with application on selected air traffic management operations maight be found in documments RTCA-DO303(NRA),RTCA SC-214/EUROCAE WG-78 (4DTRAD-OSA), FAA DTFAWA-09-A-00001(ATSA-SURF IA),RTCA DO-312 (ATSA-ITP) and RTCA DO-319 (ATSA-AIRB).

The ED-78A/DO-264, together with last two ones, has served as a template for OSA of SSEP in iFly project. Due to the fact that SSEP procedure works with many processes and supporting automation tools not yet certificated – even not theoretically well described, we have omitted the quantitative analysis and ad hoc definition of any probabilities of failures. E.g. Safety Objectives for operational hazards have not been determined.

The schema of a bow tie model is drawn at Figure 3-1. The following list of OSA steps as defined in literature indicates which steps have been followed and which ones have been omitted due to reason stated above.

Operational Hazards Assessment (OHA) stage:
OHA: Operational hazard identification – Operational Hazards (OH) have been identified based on the application description in iFly:D9.1.
OHA: Operational hazard assessment and severity class allocation – the Environment Conditions (EC) from operational environment, External Mitigation Means (EMM) from operational requirements, Severity Class (SC) allocated to Operational Effect (OE). Hazard Classification Matrix adopted from ED-78A/DO-264. Event trees (ET) have been used to formalize the process.
OHA: Probability of effect determination – probabilities of effects, effectiveness of identified EC and EMM have not been determined.
OHA: Assign safety objectives – quantitative Safety Objectives not calculated; list of Safety Requirements (SR) provided.

Allocation of Safety Objectives and Requirements (ASOR):
ASOR: Fault tree development – Fault Tree (FT) for each of operational hazard has been constructed, operational hazard decomposed into a combination of failures: Basic Causes (BC). Internal Mitigation Means (IMM) identified, but not used to assess probabilities of FT elements.
ASOR: Safety objectives allocation – Safety Objectives not allocated, not apportioned to different Basic Causes. A list of Safety Requirements developed, but not to capture the expected performance of IMM.

ASOR: Safety requirements derivation - Safety Requirements established; qualitative, not quantitative (functional-system related BCs), assumptions (human-procedures related BCs).

Definitions of important terms might be found in RTCA DO-312 (page 128-129) or RTCA DO-319 (page 144). There is a set of definitions in Appendix 3, which have got slightly shifted meaning in our SSEP OSA in comparison with RTCA DO-312, e.g. discrepancy between IMM and EMM and location of Detection Means (DM).

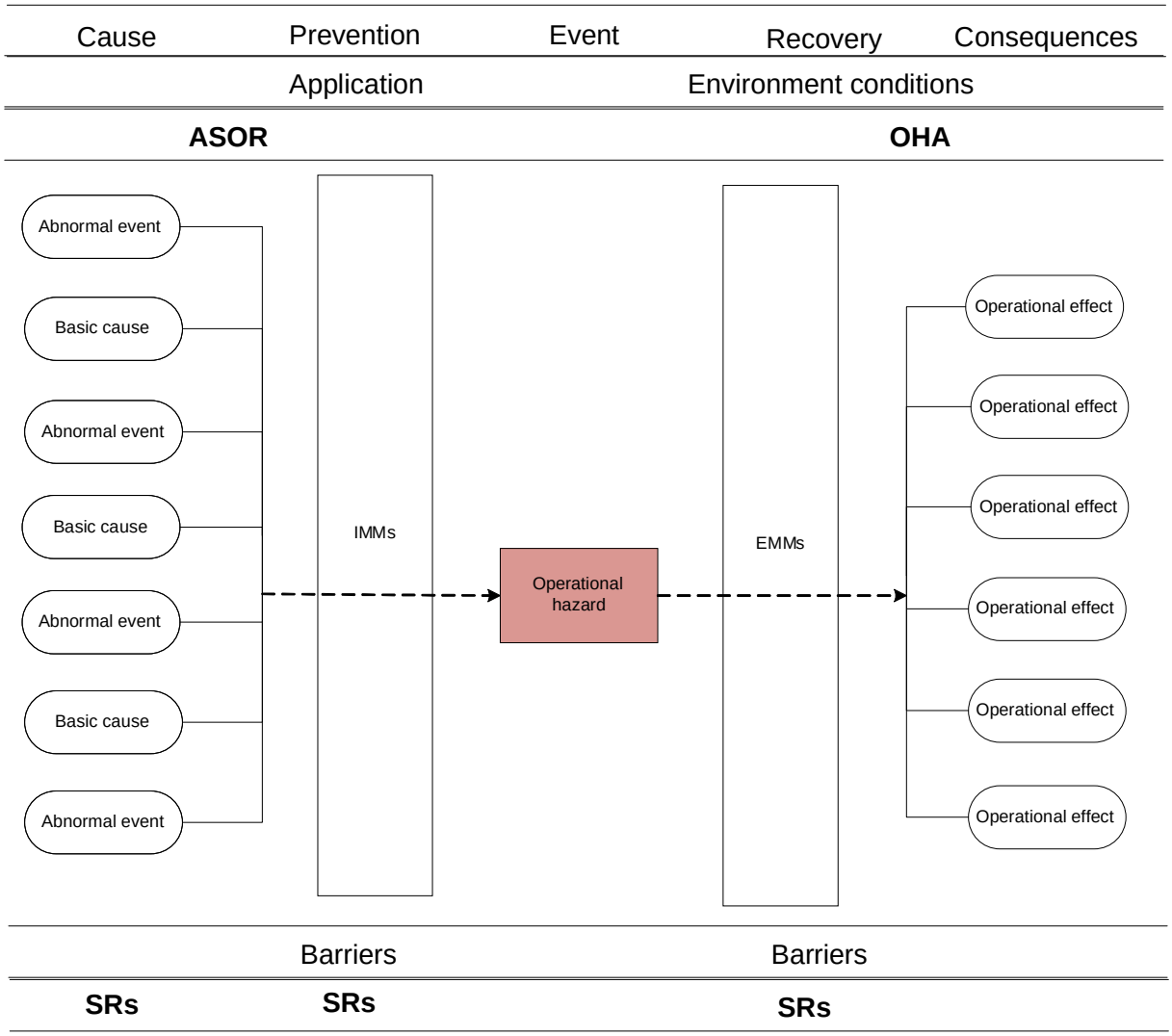

Figure 3-1: Bow tie model used through this document, adopted from RTCA DO-319.

4. SSEP Main OSA Results Summary

Document iFly: D9.1 (Operational Services and Environment Description) has presented typical behavior and processes onboard autonomous aircraft which take place during airborne self-separation operations. A flight crew supported by automation conducts the flight of own a/c without any involvement of ground in the separation management tasks. To maintain a fluent flight the following is required

- To broadcast aircraft state, intent and maintain planned trajectory (Navigation FB)
- To scan the surrounding situation for potential problems/conflicts (Surveillance FB)
- To deal with the situation where a planned trajectory is not conflict free anymore (other FBs).

One should be reminded that a conflict itself is not sensed as an operational hazard during self separation operations but a natural phenomenon. The separation task is to eliminate the unwanted conflict, but the existence of a conflict is not a foreign element in SSEP.

OSA delivered in iFly:D9.2 moves along the OSED from iFly:D9.1, both of them have been developed based on the methodology of ED78a. However, as already discussed earlier, this methodology was not developed for applications in the level of maturity corresponding to the V1 phase of E-OCVM. In this early phase an advanced concept keeps open several options at detailed design level, and therefore does not yet allow a detailed allocation of low level tasks which typically is accomplished when ED78a/DO-264 is applied in later design phase.

4.1 Operational Hazards

One of the main steps in the OSA process is to set up an appropriate level of hazard abstraction in order to distinguish the main operational hazards from their causes. The results may, to some extent, vary according the perspective of the analysis and the limitations described above must be taken into account in this context.

The approach adopted in this preliminary OSA is to focus on the interaction of own self separating aircraft with surrounding traffic. In other words, the analyzed hazards are based on the situations that directly affect near aircraft through an unexpected behavior of own aircraft. The onboard procedures are simplified to a straightforward use of ASAS as a decision support tool. In particular, it is considered that the automation manages the information about surrounding traffic through data links, and provides this information to the flight crew, performs conflict detection and alerts flight crew about detected threats, and finally presents possible conflict resolution maneuvers to the flight crew. The primary role of the flight crew in this simplified model is to react on the provided alerts, to decide about the solution, and to initiate the execution of the selected solution. Beyond this primary role the flight crew plays an essential role in different (both external and internal) mitigation means based on its situation awareness

and experience. The implementation aspects of the tasks (e.g., which information should be shown on CDTI in the different contexts, form of alerts, etc.) are considered out of scope of this preliminary analysis and are postponed for subsequent research.

The scope of this OSA is further limited to the hazards specific for self separation operations. In particular, the hazards related to the general technical problems (not ASAS related), general weather issues, etc. are omitted from the analysis. The analysis itself is performed on the example scenarios provided in Appendix A of D1.3.

Obviously, there is a considerable gap in such approach, particularly in relation to the safety assessment of onboard procedures and human-automation interaction. It is expected that the missing elements should be filled by a subsequent research and after a refinement of the definition of SSEP operations. In addition, WP 9.2 is not the only one work package in iFly dealing with the potential sources of failures and SSEP hazards identification and the results of other WPs (in particular, WP2 and WP7) complement the analysis provided in this document. Some details related to the comparison of D9.2 with the outcomes of WP2 and WP7.1 are provided in Appendices 4 (WP7.1) and 7 (WP2).

4.2 Operational Hazards Identification

The analysis presented in this section is based on the SSEP process flow described in iFly:D9.1. For reference, the typical "conflict life-cycle" is shown in Figure 4-2 (also iFly: D9.1, page 16) and Figure 4-3 (also iFly: D9.1, page 22) presents SSEP-stages diagram. Potential hazards are bound with the moments, when the expected stage or step is not initialized or initialized in a wrong way and thus the optimal flow of actions is corrupted.

To understand the regular flow of SSEP and deviations caused by operational hazards let us describe the states which an autonomous aircraft may experience and the transitions between them. The following paragraphs explain the meaning of Figure 4-1. The circles represent particular states of own autonomous a/c and there are distinguished with their colors regular states (green color) from operational hazards (white ones) and emergency state (red one). Arrows (both solid and dashed) represent possible transitions between these states. Solid arrows indicate natural 'aircraft status' evolution. Dashed arrows indicate the 'aircraft status' evolution as soon as hazard is detected. **We consider the scenario, when the own aircraft may be only in one state at a moment, but actually there might be a concurrency of operational hazards related to several detected /undetected conflicts.** All states are listed systematically later in following subchapter. Already mentioned Figure 4-2 may be understood as a subset of this broader picture (when aircraft experience only the regular, green states).

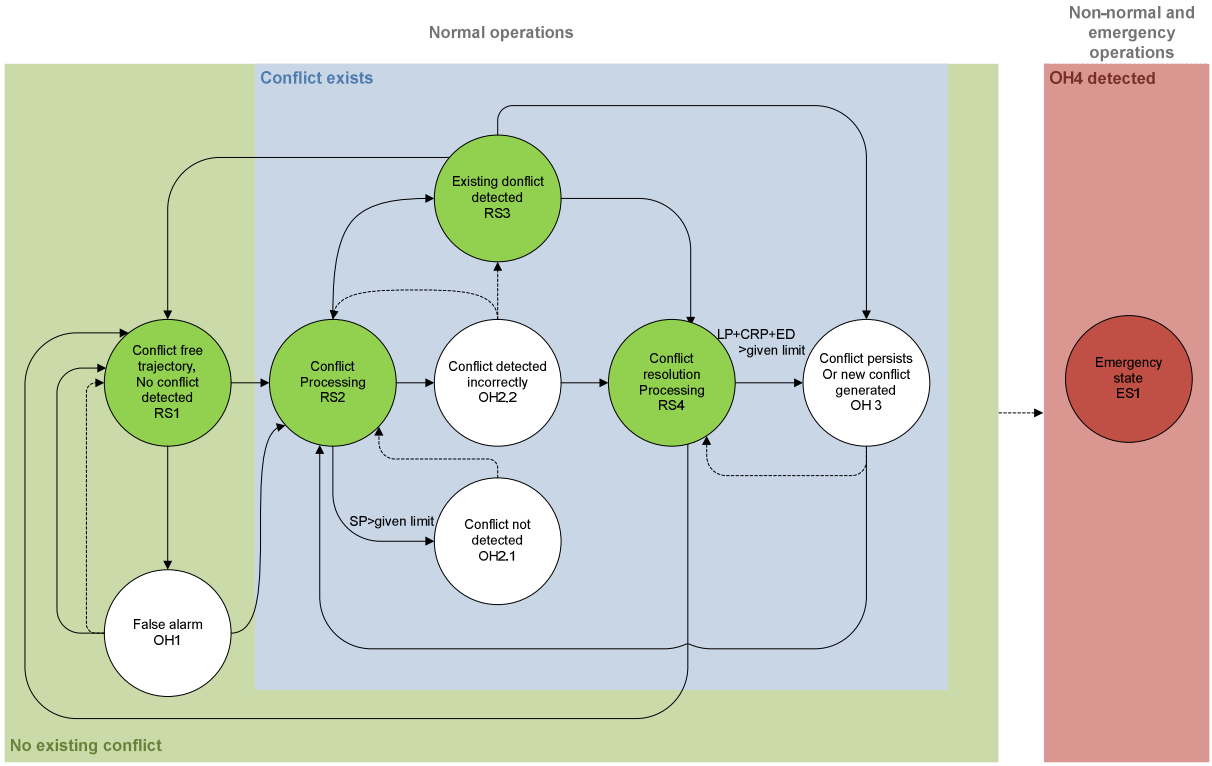

Figure 4-1: Own aircraft states. Solid arrows indicate natural 'aircraft status' evolution. Dashed arrows indicate the 'aircraft status' evolution as soon as hazard is detected. Green area marks the conflict-free environment. The blue area marks environment where the own aircraft faces at least one conflict. While staying in states inside this blue "conflict area", the aircraft may deal with several consequent conflicts - not only one conflict.

The starting point is the situation when there is no conflict and an autonomous aircraft is flying its conflict free trajectory - it is a green Regular State (RS) numbered as 1.
First operational hazard is related to a still conflict-free environment when own aircraft indicates non-existing conflict. This situation may be called "False alarm" and it is a first example of conflict detection failure. Once this operational hazard is detected, the own aircraft terminate all conflict resolution actions and an own aircraft continues to fly its planned conflict-free trajectory. When this operational hazard remains undetected, the own aircraft takes all actions to solve the "conflict" which may result into an unnecessary maneuvering and under some circumstances generate a true conflict.

If an own aircraft intent is not conflict-free any more, even if the own aircraft has got all available information and the conflict is already detectable by means available onboard, there might be a time period (labeled as Surveillance Performance, SP in Conflict-life cycle) when the conflict has not been

detected yet but this time delay is still acceptable. This not hazardous state is labeled as "Conflict Processing" regular state 2.
Anyway, too long silence concerning the true conflict is definitely an Operational Hazard ("Conflict not detected", OH 2.1) which may result in a worst case into a mid-air collision. Once there is suspicion of not detected conflict, the aircraft moves into Regular State 2 again.

Let us suppose the true conflict which is detected within time limit of SP. This conflict may be detected correctly – it is located in space and time with required precision and more over, the conflicting aircraft is determined correctly. This situation is described with Regular State 3.
Other possibility is that the autonomous aircraft is correctly aware of a conflict but its localization in time and space or identification of conflicting aircraft is incorrect. This is another Operational Hazard, OH2.2 "Conflict detected incorrectly".

Both, RS3 or OH2.2, may initialize conflict resolution process. Similarly as in conflict detection case (RS2), there might be a time period, when conflict is detected, the on-board conflict resolution processing is in run, but the conflict resolution has not been provided yet. Again, there is a time limit for this conflict resolution processing, LP+CRP+ED (see Figure 4-2). Until this time limit is not exceeded or conflict resolution is not provided, the aircraft stays in Regular State 4, RS4.

When the time limit for conflict resolution processing is exceeded or if any conflict resolution is issued, the aircraft may move to any of following states:
Once any conflict resolution is provided and accepted by the flight crew, the conflict resolution processing is finished. The proposed conflict resolution may be "correct" or may be "wrong". By the term "correct" we mean that the proposed intent solves the actual conflict and does not induce any new conflict. So the result is any conflict free trajectory. In case of correct conflict resolution, aircraft leaves state RS4 in favor of another regular state, RS1.
The "wrong" conflict resolution is a conflict resolution which does not solve the current conflict or induce another conflict (OH3). Since conflict resolution process is finished and nobody is aware, the aircraft moves to the state Conflict processing, RS2 in case of new induced conflict. The last possibility is that conflict resolution is not issued at all and conflict persists (still OH3).
Theoretically the aircraft may jump directly from RS3 into OH3, and completely omit RS4, when onboard conflict resolution process is not initialized.

The not solved current conflict, despite the fact that any conflict resolution has been released may be a sign of ASAS failure, which falls under another Operational Hazard (OH4).

Any of Operational Hazards OH1, OH2.1, OH2.2 or OH3 may be a sign of serious aircraft equipment failure when aircraft is not able to perform airborne self-separation (OH4), so post-hoc ASAS and ADS-B equipment tests should be accomplished. The detected OH4, depending on the degree of malfunction, leads to an emergency situation represented by Emergency State 1, ES1. The non-normal and

emergency procedures should be defined to be followed when emergency situation appear. It is expected that the aircraft will continue to flight in this emergency mode till it reaches TMA or MA and the aircraft will not return to any of regular states (RS1-RS4).
The undetected OH4 is not explained by any separate hazard state, because it runs on the background and may be parallel to any of regular states (RS1-RS4) or hazard states (OH1, OH2.1,OH2.2,OH3).

4.3 Own Aircraft States

- Regular states - normal operations
  - Regular State 1 (RS1): Conflict free trajectory and no conflict detected
  - Regular State 2 (RS2): Conflict exists, conflict resolution process has not detected this conflict, but the time delay (SP) is still within given limits.
  - Regular State 3 (RS3): Conflict exists and its position is correctly and in time determined
  - Regular State 4 (RS4): Conflict has been detected, conflict resolution process has been initiated, and the time delay (LP+CRP+ED) is still within given limits.
- Hazard states – operational hazards
  - False Alarm (OH1): There is no true conflict, but any conflict is indicated.
  - Conflict detection problems
    - Conflict not detected (OH2.1): The existing conflict not detected
    - Conflict detected not correctly (OH2.2): There is a true conflict, any conflict is detected but its location or target aircraft is not determined correctly.
  - Conflict resolution problems
    - Conflict persists or new conflict generated (OH3): There is existing detected conflict, but the conflict resolution of current conflict is not provided within given time or the new RBT is not conflict free – new conflict is generated.
- Emergency and non-normal states
  - Emergency State (ES1): Emergency procedures initiated due to degradation of airborne self-separation ability.
    Emergency state is initialized in case of Airborne self-separation failure(OH4) – operational hazard appears and is detected (otherwise OH4 may be a cause of any of OH1, OH2.1, OH2.2 or OH3) e.g. when there is
    - ASAS failure - Loss of airborne self-separation ability
    - Information insufficiency
      - Broadcast failure (0/1) – other aircraft
      - Receiver failure (0/1) – own aircraft

As a result, there have been identified five operational hazards which endanger the smooth flow of SSEP procedure and bring the possibility of aircraft harm or humans onboard in peril. All operational hazards are described from perspective of an own aircraft.

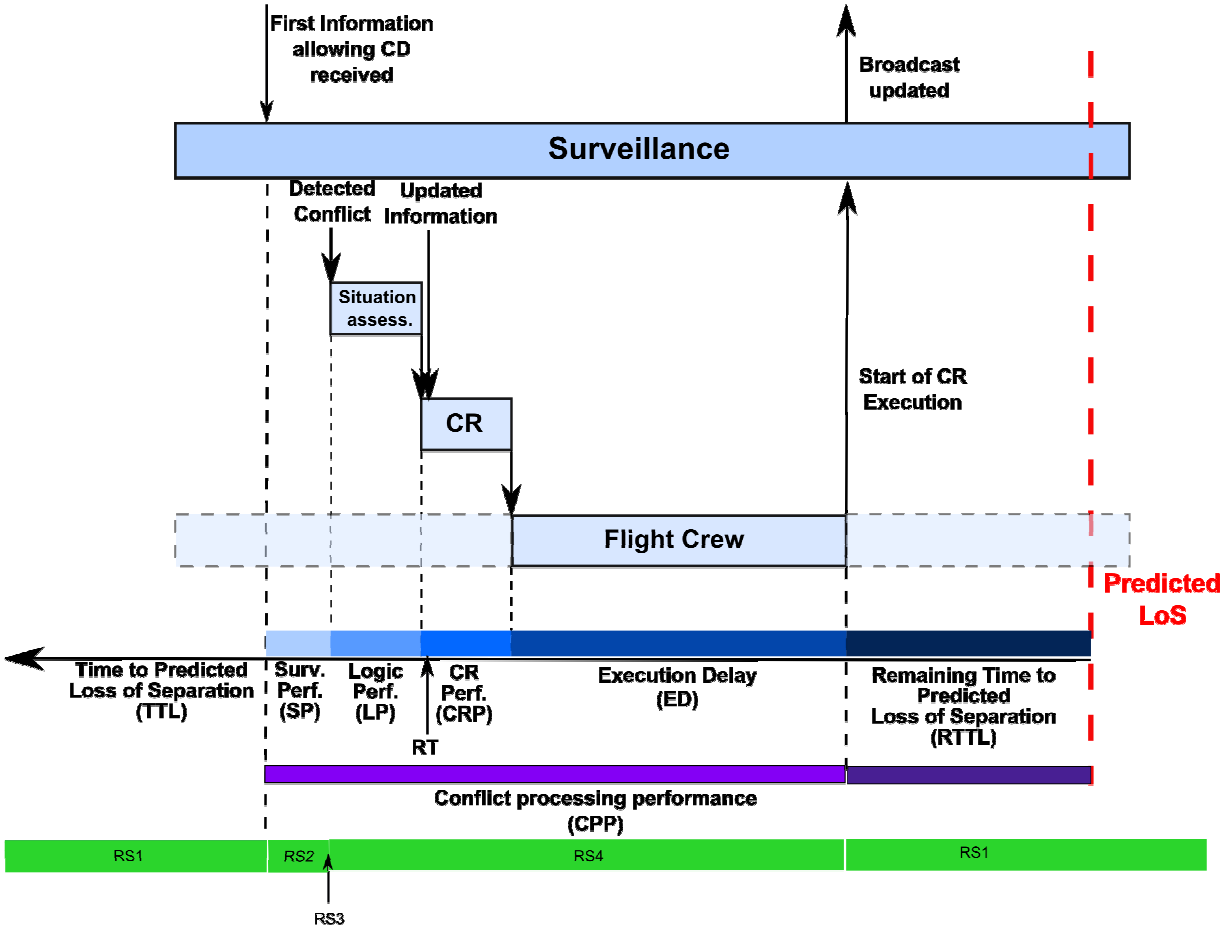

Figure 4-2: Conflict life cycle and regular states.

Interconnection between SSEP stages and identified operational hazards locations is available at Figure 4-3. Non-correct situation assessment OHs are located on borders of *Regular flight stage* and *Initiation stage*. These are

Conflict false alarm (OH1) – non-existing conflict was detected by own aircraft. As a consequence the own aircraft starts to solve this conflict according to standard guidelines.

Conflict not detected (OH2.1) – existing conflict is not detected by own aircraft. The own aircraft does not initiate conflict resolution process.

Conflict detected incorrectly (OH2.2) – existing conflict is detected, but its location or target aircraft is not determined correctly. Conflict resolution process is initiated, but the input information for conflict resolution process are corrupted.

Conflict resolution OH is located within one of following stages: *Initiation stage, Enhanced monitoring stage, New trajectory generation stage or Tactical maneuvering stage*. Corresponding parameters of conflict lifecycle are *Logic Performance (LP), Conflict Resolution Performance (CRP) and Execution Delay (ED).*

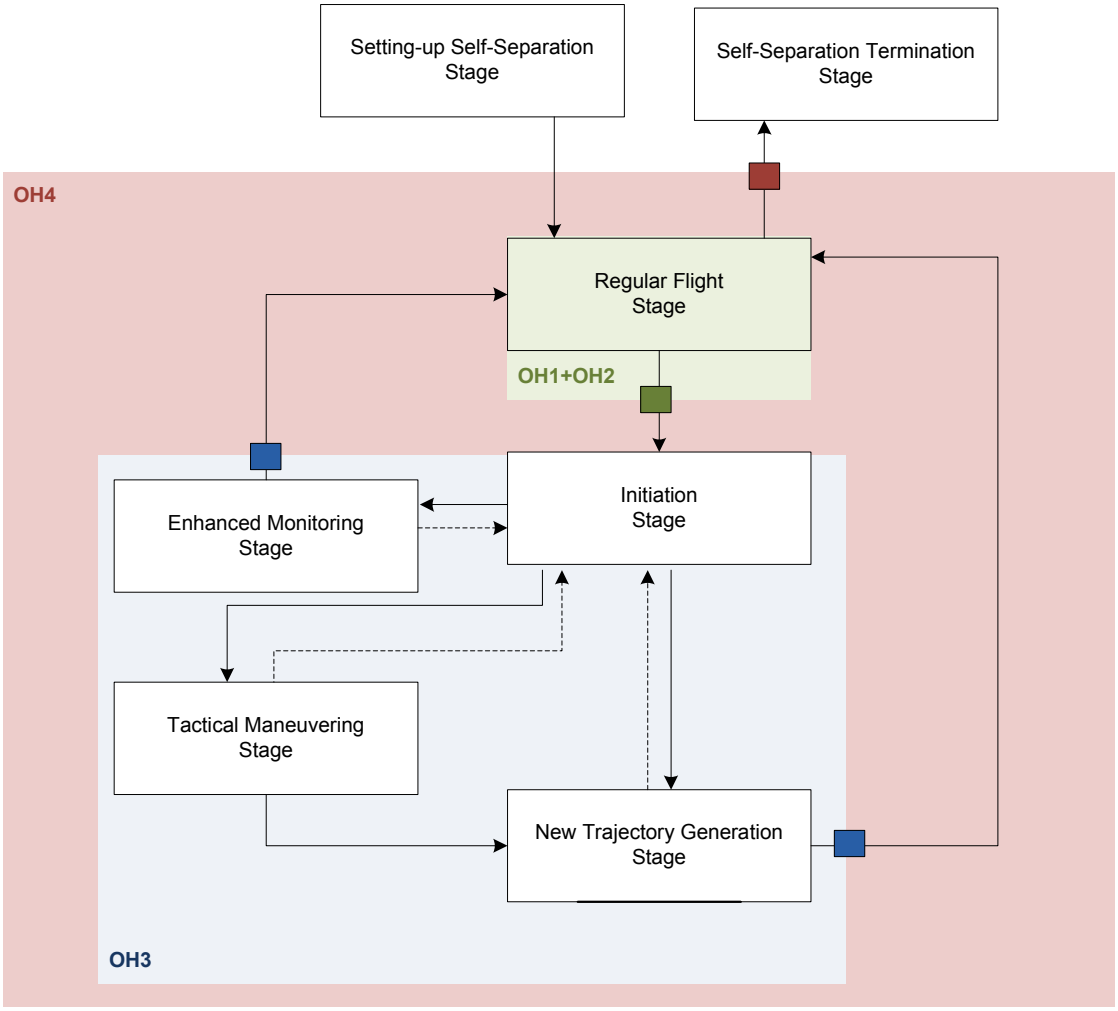

Figure 4-3: Interconnection between SSEP stages and identified operational hazards. The SSEP stages diagram is taken from iFly: D9.1 (OSED). The big shadowed boxes demarcate the stages affected by the operational hazards. The small squared marks on borders of hazard areas show the transitions influenced by the operational hazard existence.

Conflict persists or new conflict generated (OH3) – own aircraft has detected a conflict, but the conflict resolution is not provided or executed. This operational hazard also covers the situation when any resolution is provided and executed, but the provided conflict resolution is "wrong" – that means FC confirms a conflicting trajectory. This means that current conflict has not been solved or a new conflict is induced.

ASAS and supporting equipment related hazard *affects the whole conflict detection and resolution process, all stages:*

Airborne self-separation failure (OH4) – aircraft is not capable to perform airborne self-separation. There are problems with conflict detection and proposed conflict resolutions may be "wrong", e.g. may not follow AFR. The ASAS failure is not a temporal issue and chance to heal up spontaneously is negligible. Transmission of own aircraft state and intent might (but need not) be also dysfunctional. Flight crew has no possibility to repair the failure. Failure of ADS-B receiver falls also under this operational hazard. This operational hazard also covers the situation when resolution is provided and executed, but the broadcast intent information does not reflect this trajectory change.

In case this operational hazard is detected and flight crew is aware of automation failure, the defined emergency procedures are initiated. If the airborne self-separation failure remains undetected (despite detection means) then it may result into any of SSEP operation related hazards OH1-OH3.

Note:
The question arises: when Operational Hazard begins to exist? From ATM perspective, it is the moment when aircraft takes actions which is noted by other participants– e.g. aircraft maneuvers to solve non-existing "conflict" or at given time horizon aircraft do not provide solution of true conflict. From perspective of onboard processes, beginning of OH is, e.g. first activation of conflict resolution process (OH1) or the silence when action is needed (the true conflict is not detected – OH2.1). The authors give the preference to the second definition.

4.4 Operational Hazards Assessment (OHA)

4.4.1 Environment Conditions (EC)

The evolution of an existing OH and final OH effect is dependent on the efficiency of external mitigation means/barriers but also on observed environment conditions. Some of them do not remain the same as at the moment of hazard occurrence, but evolve and change in time.

Environment Conditions (ECs) determine the steps of conflict resolution process taken by own and other aircraft. The ECs may vary during the conflict resolution process unlike the external mitigation means which are expected to remain constant and the same as at the moment when OH appeared. The list of identified ECs is available in Table 4-2.

Environment factors:

- **Remaining Time To predicted Loss of separation** (RTTL) – indicate the required actions according to requested type of conflict solution. When the operational effects of operational hazards will be assessed, we will work with RTTL specification in a form of
    - Mid-term conflict (EC-1)
    - Short-term conflict (EC-2)

- **Environment complexity** – number of aircraft/conflict involved into conflict cluster. Let us note that the *presented scenarios describe only simplified situations with two aircraft –own aircraft and other aircraft - which are involved into a mutual conflict at a moment. But this does not mean that the considered airspace is simple. The airspace is considered to be populated with number of aircraft, which may be potentially involved.*

  The densely populated airspace may be a cause *of information sharing blackout*, when ADS-B messages are not delivered due to interference (discussed further as BC-16).
    - Based on assumptions ASSUMP-6-INI and ASSUMP-8-INI we expect the SSEP operation to be used in airspace of any traffic density (EC-3). The true limits of environment complexity should be investigated further in connection with the development of conflict resolution algorithms.

- **Assumed communication channels –** For purposes of SSEP OSA we suppose the environment with the largest information exchange.
    - All aircraft broadcast their state together with intent via ADS-B. This information are provided also to/by a ground supporting system SWIM (EC-4). This range of services has been named as *Service level 3* in iFly: D9.1.

Table 4-2: Environmental conditions

Environmental Conditions	Description	Location in OSED iFly: D9.1 or OSA (in brackets)	OH Ref
EC-1	Mid-term conflict, TTL>STT, priority rules respected	Page 14	OH1-OH4
EC-2	Short-term conflict, TTL<STT, implicit coordination	Page 14	OH1-OH4
EC-3	The SSEP application can be used in airspace of any traffic density.	(ASSUMP-6-INI) (ASSUMP-8-INI)	OH1-OH4
EC-4	Communication – Service Level 3	Page 10 (ASSUMP-5-COM) (ASSUMP-6-COM)	OH1-OH3 (OH4?)

4.4.2 Identified Operational Effects

Each operational hazard evolves in dependence on environmental conditions and other factors until resulting operational effect appears. List of identified operational effects is in Table 4-3. The worst possible operational effects for each of identified operational hazard are recapitulated in Table 4-4.

During OHA process, the severity class is assigned to each of operational effects. The summary of severity classes with description of characteristics in relation to SSEP procedure may be found in Appendix 6 and Table 4-3. Three points of views may be taken into account:

- The minimal resulting remaining time to loss of separation (RTTL). (Appendix 6)
- The degree of failure of airborne self-separation ability (Appendix 6).
- The flight crew workload together with ASAS occupancy and loss of separation (see Table 4-3 below).

Table 4-3: List of all operational effects

Operational effect	Description	Severity Class	OH Ref
OE-1	No increase in FC workload	5	OH1-OH4
OE-2	Slight increase in FC workload	4	OH1-OH4
OE-3	Significant increase in FC workload, significant reduction in safety margins	3	OH2-OH4
OE-4	Large reduction of safety margins	2	OH2-OH4
OE-5	Loss of separation	1	OH2-OH4

Table 4-4: The worst possible operational effect.

Operational hazard	The worst operational effect	Severity Class
OH-1	Slight increase in FC workload	4
OH-2.1	Loss of separation	1
OH-2.2	Loss of separation	1
OH-3	Loss of separation	1
OH-4	Loss of separation	1

4.4.3 External Mitigation Means (EMM)

The resulting consequences of an operational hazard may be extremely severe thus the identification of means available to detect the operational hazard or mitigate the effect is very important. Based on analysis presented in Appendix 7 (Role of Flight Crew) the Flight Crew (FC) plays a main role as a mitigation mean when an hazard already exists. The overall summary of external mitigation means are presented in Table 4-5.

Note: It is supposed that all EMMs and Detection Means (DM) operate simultaneously and there is not predefined order of DMs or EMMs.

Table 4-5: List of External Mitigation Means

EMM	Description	OH
EMM 1.	**Flight crew in the loop – the flight crew shall monitor and analyze situation**	
EMM 1.1	**Visual control** - Flight crew shall look out of the window and checks visually the closest aircraft neighborhood. Flight crew shall make connection between situation displayed on CDTI and the situation as it is seen out of the window. Flight crew shall make connection between seen situation and ASAS alerts, e.g. Flight crew shall visually recognize conflicting aircraft announced by ASAS.	OH1, OH2.1, OH2.2, OH3
EMM 1.2	**Flight crew shall monitor the airspace configuration on CDTI** to gain an over-view of traffic along its trajectory. Flight crew shall compare its knowledge concerning surroundings with alerts provided by ASAS, e.g. when ASAS announce a conflict detection, flight crew shall identify the conflicting aircraft and a point of expected loss of separation on CDTI. On the other hand FC may recognize a conflict on CDTI when no ASAS alert is released.	OH1, OH2.1, OH2.2, OH3

EMM	Description	OH
EMM 1.3	**Flight crew of own aircraft shall analyze the other aircraft actions,** understand motivations of maneuvers conducted by other aircraft. If possible, flight crew shall foresee the other aircraft steps.	OH1, OH2.1, OH2.2
EMM 1.4	**Flight crew shall "shadow" the automation processes of own aircraft**. Flight crew shall be aware of problems solved onboard, e.g. shall be informed what steps of "conflict life-cycle" are actually solved by ASAS. Flight crew shall monitor the time spent by ASAS on separate tasks. Flight crew shall critically assess proposed ASAS resolutions, e.g. conflict detection and conflict resolutions. Flight crew shall be able to notice any ASAS malfunctions and have suitable tools for such detection.	OH3
EMM 2	**Information integration & information cross-check**	
EMM 2.1	**Additional informational sources** As outlined at Figure 4-4, the correct aircraft actions and flow of SSEP rely on input information and their onboard processing. The high quality of input information is essential. So autonomous aircraft shall verify the traffic information from several sources such as a) received ADS-B reports vs. list of aircraft provided by SWIM (push mode) b) analyze additional information (other aircraft information upon request – SWIM pull mode) c) intent - based detected conflict vs. state-based detected conflict.	OH1, OH2.1, OH2.2
EMM 3	**Surroundings configuration, demands on conflict resolution algorithms**	
EMM 3.1	**Own and other aircraft share OH**, flight crews of both aircraft have the same Situation Awareness. This external mitigation mean is functional and meaningful only in case of OH1. Both aircraft share the same detected conflict (no matter that non-existing) and provide all conflict resolution steps to avoid the point of conflict.	OH1
EMM 3.2	**OH solved by own or other a/c, when maneuvering because of other reasons.**	OH1, OH 2.1, OH2.2, OH3
EMM 3.3	**OH solved by aircraft with lower priority**	OH1, OH 2.1, OH2.2, OH3, OH4
EMM 3.4	**Demands on short-term conflict resolution algorithm** – SR-N-4.1	OH1, OH 2.1, OH2.2, OH3, OH4
EMM 4	**Emergency procedures**	

EMM	Description	OH
EMM 4.1	**Emergency resolution** When an own aircraft realizes that it is not able to perform airborne self-separation any more, the emergency status shall be announced to other aircraft via a) ADS-B message (in case of functional transmitter) – the changed priority number is released b) Voice communication (in case of ADS-B transmitter failure) c) Report shall be provided into SWIM	OH 4
EMM 4.2	**Other stakeholders active participation** a) Other aircraft are aware of own aircraft emergency status. In case of a mid-term conflict, the other aircraft has lower priority and solve the conflict, in case of short-term conflict other aircraft should ensure conflict resolution SR-N-4.1. b) SWIM periodically update the emergency aircraft position or create RAA around emergency aircraft	OH 4

4.5 Allocation of Safety Objectives and Requirements (ASOR)

The operational hazard is caused by a simultaneous influence of basic causes, abnormal events and possibly environmental conditions. The operational hazard appears in case of internal mitigation means failure. The ASAS failure may be one of causes of OH1-OH3.

The basic causes might be divided into two classes according to natural way of services failure.

- Service/functionality does not provide full range of services or the quality of resulting product is of a lower quality with respect to required outcome *("degradation mode").*
- Service/functionality complete failure ("*0/1 mode*"). This failure mode is indicated when there is not sense in speaking of functional degradation – the machine is working or not, there is no halfway house.

The required binding limits of performance which indicate the failure of functionality should be defined via Safety Requirements (Table 4-7).

For correct completion of SSEP operation the ASAS functionalities have to be functional and more over the input information quality must be within given limits.

- The operational hazard may appear due to **poor Information quality**, when there is state or intent information missing or is corrupted.
    - **Other aircraft state and intent**
    - **Own aircraft state and intent**

    are essential.

- **ASAS failure** may also cause an operational hazard. ASAS failure is a an overall terminology for both – the automation failure and the flight crew failure (e.g. flight crew does not perform the tasks as required).

Schema of locations which shall provide correct outputs to avoid an operational hazard is drawn at Figure 4-4. The color symbolism: *red* for ASAS unit; *blue* for own aircraft state and *green* for other aircraft state and intent will be used also through the detailed ASOR part of Chapter 5 inside the fault trees of each operational hazard.

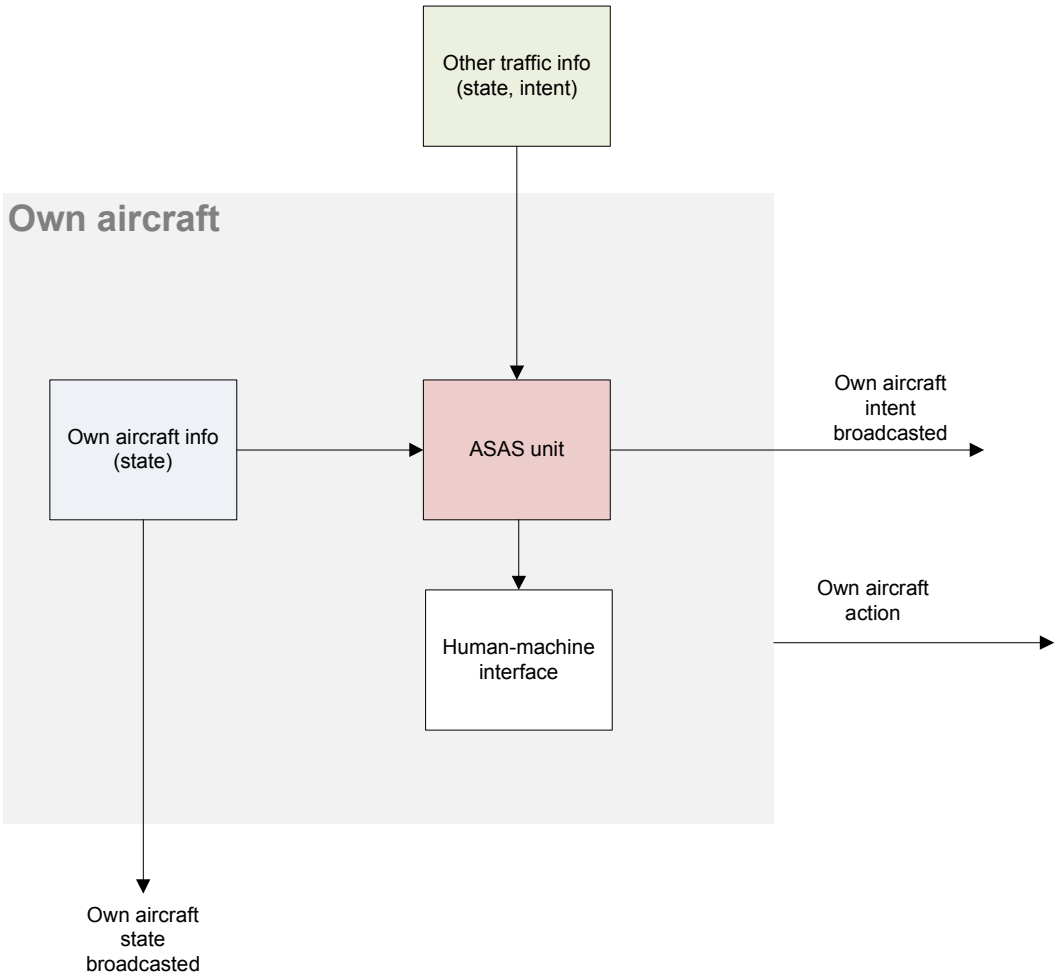

Figure 4-4: Schema of locations which shall provide correct outputs to avoid an operational hazard.

4.5.1 List of Failures – Basic Causes

Many basic causes proposed in Table 4-6 may be viewed not only strictly as functional/not functional, but in finer resolution as functional/degraded/not functional.
The following items allow only for "0/1" approach: e.g. 1, 4, 8, 9, 16, 17
The following items allow also for "degradation mode" approach: e.g.2,3,7,10,11,13,14,15.

Note: The underlined parameters and limits shall be further defined.

Identified Basic Causes may be grouped in following thematic units:

- Hardware/technical functionality failure - not directly related to ASAS (BC-1, BC-4)
- Data quality degradation (BC-2, BC-3, BC-15, BC-16)
- ASAS/*Autonomous aircraft* functionality degradation (BC-5, BC-7, BC-8, BC-9, BC-10, BC-11, BC-12)
- Pure Flight crew performance degradation (BC-13)

Table 4-6: List of identified basic causes.

Basic causes	Description	ASAS location	OH
BC -1 - EQP	**Transmission failure ***	Navigation FB	OH 4 OH 2.1 (other a/c)
BC-2	**Low quality of ADS-B messages concerning own aircraft state** – binding limits of assigned Equipage class (DO-242A). The assigned Equipage class puts requirements also on the position determination systems and flight performance precision.	Navigation FB	Not included

Basic causes	Description	ASAS location	OH
BC-3	**Flown and broadcast intent discrepancy** – see Figure 4-5. The flown and broadcast intent of own aircraft differ. The limits should be defined. a) **Improper execution initiation** (due to ASAS) **b) Imprecise/wrong execution of desired trajectory**, e.g. accepted solution not flown precisely – the realization of solution accepted by flight crew shall be maintained in given limits. These limits shall be valid for the whole flight, the realization of RBT. Above stated items covers aircraft intent but might be generalized also on c) Information reported and broadcast by SWIM and the true situation discrepancy. (e.g. weather reports, NOTAM) **d)** Information regularly reported by SWIM is not available.	Tactical maneuver FB, Trajectory modification FB Navigation FB	a) OH 1,2.1,2.2 b) OH 1,2.1,2.2
BC-4 - EQP	**Receiver failure ***	Surveillance FB	OH 2.1, 4
BC-5	Other aircraft wrong identification (ASAS). All information available, but aircraft not taken into consideration e.g. Failure of internal functions for data fusion	Surveillance FB	Not included
BC-7	**Conflict identification failure** a) **Conflict not identified within time limit** (Surveillance performance SP should not exceed given limit) b) **The location of conflict and RTTL do not meet required precision**. **c) Conflict detection process corrupted (general ASAS bug – permanent error)***	Surveillance FB	a) OH 2.1,4 b) OH 2.2,4 c) OH1,2.1,2.2, OH4
BC-8	**Own and other aircraft priority incorrect determination** (due to ASAS).	Events handling FB	OH 3

Basic causes	Description	ASAS location	OH
BC-9	**Incorrect conflict resolution process initialization** • When aircraft configuration changes and new conflict is detected and conflict resolution is not started correctly (including the "*restart*" of conflict resolution process). • When conflict is solved by an open maneuver, but the conflict free RBT up to MTTH is not provided (e.g. open maneuver is not followed by closed maneuver).	Events handling FB	OH 3
BC-10	**Conflict resolution process initialization failure** a) Logic performance (LP) should not exceed given time limit (due to ASAS – temporal failure). **b) Conflict resolution process initiation corrupted (general ASAS bug - permanent)***	Events handling FB	a) OH 3 b) OH4
BC-11	**Conflict solution not proposed by ASAS** – a) Conflict resolution performance (CRP) should not exceed given time limit. **b) Conflict resolution process corrupted (general ASAS bug - permanent)***	Tactical maneuver FB, Trajectory modification FB	a) OH 3 b) OH4
BC-12	**Insufficient quality of proposed conflict resolution** – proposed solution should follow AFRs (e.g. proposed trajectory is not conflict free). a) Due to ASAS failure b) Due to wrong input information	Tactical maneuver FB, Trajectory modification FB	a) OH 3 b) Not included
BC-13	**Flight crew does not accept proposed conflict resolution in time** – Execution delay(ED) should not exceed given limits, otherwise the proposed solution may not be valid any more.	Tactical maneuver FB, Trajectory modification FB	OH 3
BC-15	**The own aircraft position and state (e.g. weight) determined incorrectly** – see also connection with item number 3. State	Navigation FB	OH 1, 2.1, 2.2

Basic causes	Description	ASAS location	OH
BC-16	**ADS-B messages are missing due to environment**, e.g. messages lost in congested area or because of unfavorable atmospheric conditions. This BC covers also the scenario, when SWIM report is lost due to environment.	Environment	OH 2.1
BC-17	**Solution execution not initialized-** see State and intent realization and broadcast path, Figure 4-5.	Tactical maneuver FB, Trajectory modification FB	OH 3

Note on BC-3:

The flown and broadcast intent might be different. Thus own aircraft and other aircraft may work with different intent information concerning the same aircraft. The broadcast state and state the own aircraft believes is in, are identical. This is due to the fact that state is directly read from unit onboard sensors (within Trajectory execution) and this state is hand over and transmitted AFTER the performance. This state information is expected to be correct, but may be also corrupted due to navigation malfunction. State and intent realization and broadcast path is summarized at Figure 4-5.

General notes:

- *No data corruption is supposed due to internal data exchange among functions onboard.*
- *Case that Conflict resolution is not proposed because of too complicated airspace configuration is not taken into account (EC-3).*

Note on General ASAS failure (marked red with *):

These failures represent a general failure of communication and ASAS functional block, which is permanent and irreversible.

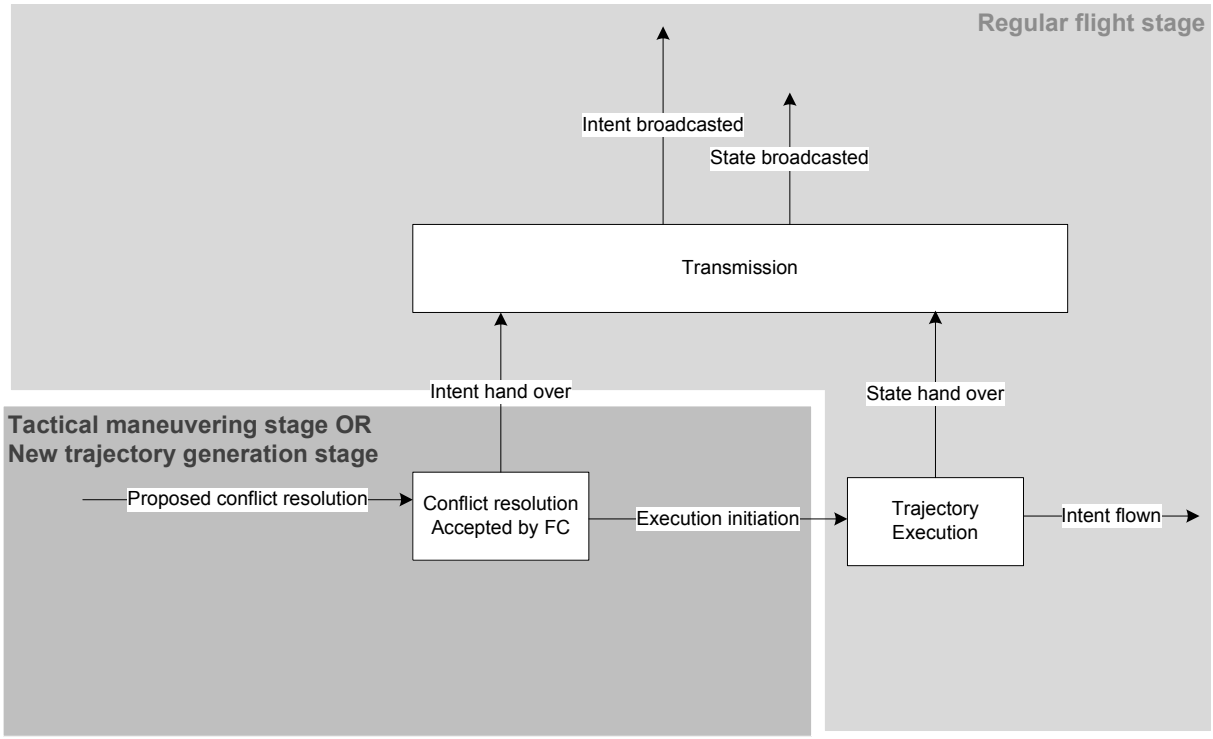

Figure 4-5: State and intent realization and broadcast path.

Table 4-7: Based on investigated Basic Causes, there have been identified additional Safety Requirements. We provide only a list of parameters to be defined further in SSEP procedure development. *NewPar* is a short for a New Parameter.

Safety Requirement	Description	Basic Cause Reference
SR-1 Limits + probability	*NewPar* - tolerable flown and broadcast intent difference - and probability of exceeding of *NewPar* shall be determined. (The same concerning state vector governed by ADS-B equipage class).	BC-3
SR-2 Limits+ probability	*NewPar* – the tolerable delay between acceptance of solution by flight crew and its realization shall be defined together with the probability that this limit is exceeded.	BC-3b
SR-3 Limits+ probability	Tolerable value/time of Surveillance performance SP and probability that this limit will be exceed, shall be determined.	BC-7a
SR-4 Limits+ probability	*NewPar* s– precision of conflict location and RTTL parameter estimate shall be determined together with probability that these limits will not be met.	BC-7b
SR-5 Limits+ probability	Tolerable value/time of Logic performance (LP) shall be determined together with probability that these limits will not be met.	BC-10a

Safety Requirement	Description	Basic Cause Reference
SR-6 Limits+ probability	Tolerable value/time of Conflict resolution performance (CRP) shall be determined together with probability that these limits will not be met.	BC-11a
SR-7 Limit	Value/time of Execution delay(ED) shall be determined.	BC-13
SR-8 Probability	Probability of transition failure shall be determined.	BC-1
SR-9 Probability	Probability of receiving failure shall be determined.	BC-4
SR-10 Probability	Probability that Conflict detection process will be corrupted and consequently lead to loss of airborne self-separation ability of an autonomous aircraft shall be determined.	BC-7c
SR-11 Probability	Probability that Conflict resolution process initiation will be corrupted and consequently lead to loss of airborne self-separation ability of an autonomous aircraft shall be determined.	BC-10b
SR-12 Probability	Probability that Conflict resolution process will be corrupted and consequently lead to loss of airborne self-separation ability of an autonomous aircraft shall be determined.	BC-11b
Shall be investigated within OPA process.	**ADS-B messages are missing due to environment**, e.g. messages lost in congested area or because of unfavorable atmospheric conditions.	BC-16

4.5.2 List of Internal Mitigation Means

Further we introduce means which could help to prevent operational hazard. These internal mitigation means are aimed at

- Hardware/technical functionality not directly related to ASAS (IMM-1, IMM-2, IMM-3)
- Data quality (IMM-5, IMM-6, IMM-7, IMM-8, IMM-12)
- Control of ASAS functionality and outputs (IMM-4, IMM-7 , IMM-12)
- Flight crew performance (IMM-9,IMM-10,IMM-11, IMM-12)

Identified IMMs shall prevent the operation hazard from its births and mitigate or eliminate the effect of BCs. Although not many BCs are directly formulated as human factors failures, many of IMMs rely on Flight Crew performance.

Table 4-8: Internal Mitigation Means

Internal Mitigation Mean	Description	ASAS location	OH
IMM-1	**Regular technical equipment revision** (transmitter/receiver/navigation unit/HMI/aircraft computers/buses-conductors/ASAS module for surveillance and conflict resolution/autopilot).	**NOT ASAS related:** Technical equipment maintenance and control	OH1-OH4
IMM-2	**Built in checks**, **alerts** when technical equipment is not functional properly Flight crew informed		OH1-OH4
IMM-3	**Back-up systems** a) e.g. complementary technologies for navigation b) back-ups of communication, flight realization c) ASAS hardware		OH1-OH4
IMM-4	**ASAS functionalities back-up** complementary technologies for ASAS functionalities – if available, e.g. a) several conflict detection methods (e.g. state-based CD is not sufficient, intent-based CD required) b) several conflict resolution algorithms	General ASAS	OH1-OH4
IMM-5	**Data quality check** Detection for systematic data shift/transformation in state data of own and other aircraft.	Surveillance FB: Data/information management (concerning other a/c)	OH1-OH2
IMM-6	**Information integrity check** a) Intent information look reliable with respect to state information (other aircraft/own aircraft) b) Other aircraft intent and state analysis from perspective of performance ability, check that broadcast trajectory (RBT) is conflict free and under AFR. c) Comparison of previous intent and current intent of other aircraft, aircraft sign tracking, state evolution d) Building a global picture of situation, analyzing of other aircraft flights e) Other information sources (SWIM – list of aircraft in neighborhood), airport radars?, information cross-check		OH1-OH2

Internal Mitigation Mean	Description	ASAS location	OH
IMM-7	**Additional diagnostics** a) Additional diagnostics for border cases (separation distance near threshold values which indicate conflict) such as longer follow up etc. b) Detected conflicts verification – detected conflicts are monitored (during the process of conflict resolution until the resolution is conducted)	Surveillance FB: ASAS output control	OH1-OH3
IMM-8	**Own aircraft data management** State, Intent and priority number of own aircraft used in ASAS procedure are checked out against the true flown trajectory and broadcast data.	Navigation FB (own a/c data)	OH1-OH4
IMM-9	**Flight crew training** a) Flight crew is aware of all requirements and is capable to perform regular flight b) Flight crew is capable to solve non-standard situations c) Flight crew is capable to substitute for (nonfunctional) machines d) Flight crew is aware of used ASAS functionalities limitations e) Failure ASAS scenarios trained	**General ASAS:** Human Factors	OH1-OH4
IMM-10	**Flight crew rights** Flight crew has got capability of interruption of ASAS process and may modify ASAS outputs e.g. FC notices, that priorities are determined incorrectly or FC substitute role of automatization.		OH3, OH4

Internal Mitigation Mean	Description	ASAS location	OH
IMM-11	**Flight crew in the loop** – in cooperation with automation FC fulfills the *Data management internal mitigation means* listed above a) Flight crew is doing timely all actions, which are required by SSEP operation. b) Flight crew is informed • E.g. alerts, when FC exceed time limit for conflict resolution processing • FC alerted when conflict detected • FC noticed about following process steps, e.g. after s tactical maneuver follows the trajectory modification resulting in conflict free RBT , FC informed concerning ASAS intentions • FC is seeking for confirmatory or disconfirmatory information to coop with contradictory information • FC is aware of consequences of actions implementations • FC has got a feedback about information taken into account by ASAS c) Flight crew is not overloaded. Flight crew pays attention.* d) Flight crew is monitoring and understands the global situation e) Flight crew is monitoring own aircraft performance, including ASAS f) Flight crew is able to notice ASAS failure (detection mean of OH4 -detected ASAS failure), recognize wrong ASAS recommendations g) Flight crew is cohesive and consistent – e.g. not contradictory orders from separate members h) The responsibilities of individual FC members are uniquely determined i) FC is present j) FC does not reduce its effort due to automation, keeps the decision quality		OH1-OH4

Internal Mitigation Mean	Description	ASAS location	OH
IMM-12	**Additional diagnostics** When conflict resolution is accepted by the flight crew a) checks for possible changes of airspace configuration has to be done to ensure that conflict resolution is actual b) AFR additional check (possibly role of FC)	**Conflict resolution:** Trajectory modification FB, Tactical maneuver FB	OH3

***Flight crew attention**– the system and flight crew can handle only limited number of conflicts per hour, FC needs a rest after given time period. When burden go beyond some limits, this may cause **flight crew fatigue** and decrease of efficiency, increase of mistakes, oversights etc..

5. Detailed Safety Analysis

Forthcoming part of the document will discuss the mechanism of birth, evolution and possible consequences separately, for each of identified operational hazards.

First of all there are presented Event Trees (ET) and corresponding barriers in OHA section. The barriers are described in details and linked with EMMs and ECs introduced in Chapter 4. There are identified barriers nested in mid-term time-horizon or short-term time horizon. Within these time horizons the barriers are functional simultaneously, thus their presented order in ETs is only orientational. We do not estimate the probabilities of barriers success. This quantitative evaluation will be possible (and more reliable) further when SSEP concept and its implementation will be developed in more details. The resulting operational effects are identified together with their severity classes. In general the operational effects in short-term time horizon belong to more severe classes than the ones in mid-term time horizon. In some cases we suggest as an operational effect more than one possibility. For example the OH1 operational effects are in general mild and it is a question of further implementation whether the resulting operational effects will be “No increase in FC workload” or “Slight increase of FC workload” with severity classes 5 resp. 4.

Fault trees for operational hazards will be introduced in ASOR section. The leaves of Fault trees are constituted by Basic Causes (BCs) described again in details in Chapter 4. Short comments on FT structure are available for each of fault trees. Again the probability that a BC will happen is not determined and as a consequence, the probability of an operational hazard is not computed.

5.1 OHA

5.1.1 Event Tree for OH1

Figure 5-1-1: Event Tree for OH1 - False Alarm (part 1: mid-term)

OH1	Mid-term conflict					Safety assessment	
						Operational effect	Severity
	FC does not recognize conflicting aircraft on CDTI	Other aircraft illogical/ unexpected maneuvers– thus the "conflict" is further investigated by FC	"Conflicting" other aircraft not found in own aircraft neighborhood	"Conflict" solved, because both aircraft share the same operational hazard.	"Conflict" solved by other aircraft, which has maneuvered because of other reason.		
	Yes					No increase in FC workload	5
	No	Yes				No increase in FC workload Slight increase in FC workload	5 4
		No	Yes			No increase in FC workload Slight increase in FC workload	5 4
			No	Yes		No increase in FC workload Slight increase in FC workload	5 4
				No	Yes	No increase in FC workload Slight increase in FC workload	5 4
					No	Continuation: Figure 5-1-2	

Figure 5-1-2: Event Tree for OH1 - False Alarm (part 2: short-term)

OH1	Short-term conflict							Safety assessment	
								Operational effect	Severity
	Flight crew of own aircraft visually does not recognize conflicting aircraft.	FC does not recognize conflicting aircraft on CDTI	Other aircraft illogical/ unexpected maneuvers- thus the "conflict" is further investigated by FC	"Conflicting" other aircraft not found in own aircraft neighborhood	"Conflict" not confirmed with state-based conflict detection step	"Conflict" solved, because both aircraft share the same operational hazard.	"Conflict" solved by other aircraft, which has maneuvered because of other reason.		
	Yes							No increase in FC workload Slight increase in FC workload	5 4
	No	Yes						No increase in FC workload	5
		No	Yes					No increase in FC workload Slight increase in FC workload	5 4
			No	Yes				No increase in FC workload Slight increase in FC workload	5 4
				No	Yes			No increase in FC workload	5
					No	Yes		No increase in FC workload Slight increase in FC workload	5 4
						No	Yes	No increase in FC workload Slight increase in FC workload	5 4
							No	No increase in FC workload Slight increase in FC workload	5 4

5.1.2 Barriers for OH1

Table 5-1: Barriers used in OH1 Event tree

Barriers	Description	Dependencies
Mid-term conflict		**EC-1 + EC-3 + EC-4**
FC does not recognize conflicting aircraft on CDTI	Flight crew monitors situation on CDTI and compares conflict alert with displayed situation. Flight crew of own aircraft does not recognize on CDTI conflicting aircraft, observes difference between conflict alarm and situation on CDTI. Flight crew tries to understand this situation.	EMM 1.2
Other aircraft illogical/ unexpected maneuvers – thus the "conflict" is further investigated by FC	Flight crew analyses actions of other aircraft and recognize that other aircraft do not act as expected. Flight crew tries to understand motives of other aircraft. For example: Other aircraft is expected to maneuver but releases new intent, which does not solve the (false) conflict.	EMM1.3
"Conflicting" other aircraft not found in own aircraft neighborhood	Flight crew has access to SWIM (or other external information sources) which provides list of a/c in neighborhood ("Push mode"). Flight crew realizes that conflicting aircraft is not in the list and tries to understand this situation. Other possibility is that FC has got any doubts and asks for position other aircraft (e.g. SWIM via "Pull mode").	EMM2.1
"Conflict" solved, because both aircraft share the same operational hazard.	On the basis of the same situation awareness (SA) flight crew (own or other aircraft) acts and solves "conflict".	EMM 3.1, EMM 3.3
"Conflict" solved by other aircraft, which has maneuvered because of other reason.	On the basis of other reasons flight crew of other a/c maneuvers and solves this "conflict".	EMM 3.2

Barriers	Description	Dependencies
Short-term conflict		**EC-2 + EC-3 + EC-4**
Flight crew of own aircraft visually does not recognize conflicting aircraft.	Flight crew of own aircraft visually does not recognize conflicting aircraft and realizes that discrepancy exists between conflict alarm and actual situation. Flight crew tries to understand this situation.	EMM 1.1
FC does not recognize conflicting aircraft on CDTI	Flight crew monitors situation on CDTI and compares conflict alert with displayed situation. Flight crew of own aircraft does not recognize on CDTI conflicting aircraft, observes difference between conflict alarm and situation on CDTI. Flight crew tries to understand this situation.	EMM 1.2
Other aircraft illogical/ unexpected maneuvers– thus the "conflict" is further investigated by FC	Flight crew analyses actions of other aircraft and recognize that other aircraft do not act as expected. Flight crew tries to understand motives of other aircraft.	EMM1.3
"Conflict" not confirmed with state-based conflict detection step	"Conflict" has not been detected based on state vectors and flight crew tries to understand this situation.	EMM 2.1
"Conflict" solved, because both aircraft share the same operational hazard.	On the basis of the same situation awareness (SA) flight crew (own or other a/c) acts and solves "conflict".	EMM 3.1,
"Conflict" solved by other aircraft, which has maneuvered because of other reason.	On the basis of other reasons flight crew of other a/c maneuvers and solves this "conflict".	EMM 3.2 EMM 3.4

5.1.3 Event Tree for OH2.1

Figure 5-2-1: Event Tree for OH2.1 – Conflict not detected (part 1: mid-term)

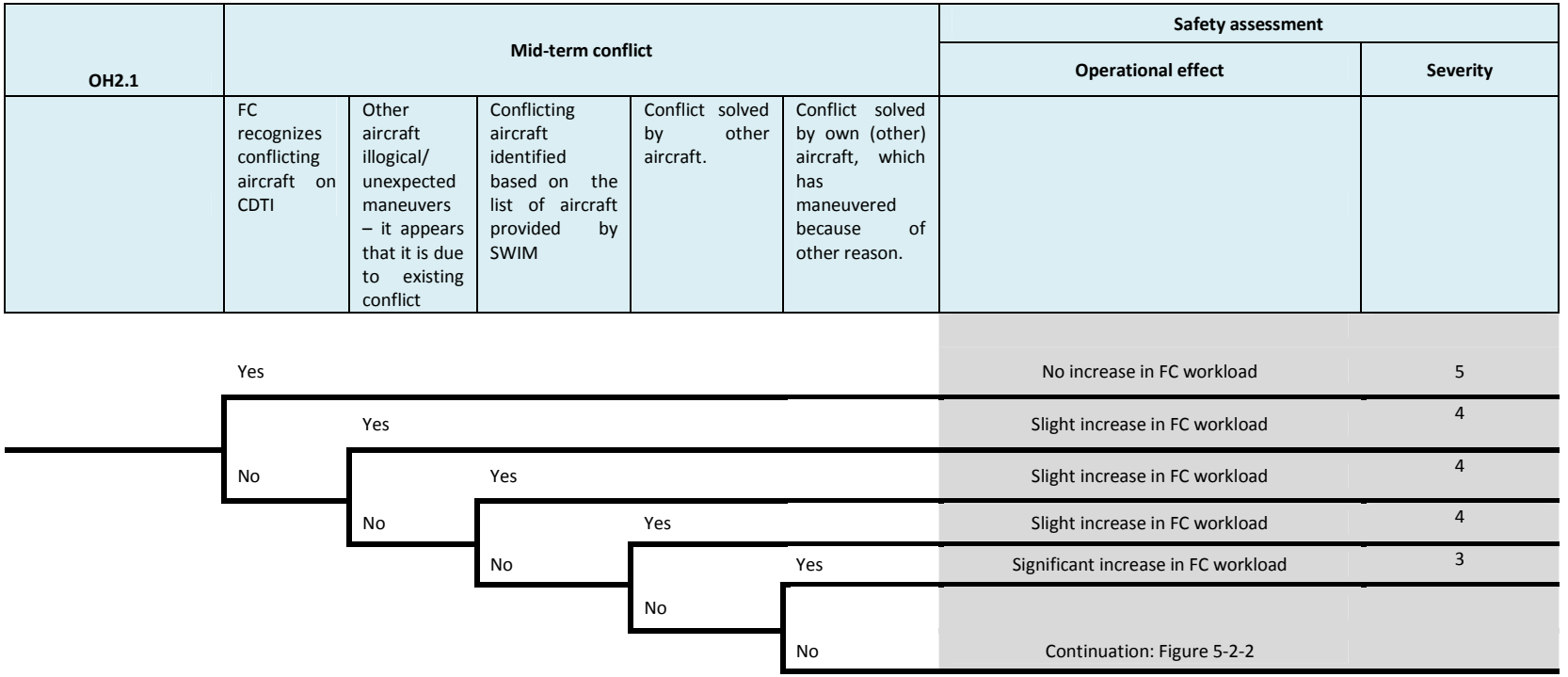

Figure 5-2-2: Event Tree for OH2.1 – Conflict not detected (part 2: short-term)

OH2.1	Short-term conflict						Safety assessment	
							Operational effect	Severity
	Flight crew of own aircraft visually recognizes conflicting aircraft.	FC recognizes conflicting aircraft on CDTI	Other aircraft illogical/ unexpected maneuvers – it appears that it was due to existing conflict.	Conflict detected with state-based conflict detection step	Conflict solved by other aircraft	Conflict solved by own (other) aircraft, which has maneuvered because of other reason.		
	Yes						Significant increase in FC workload, significant reduction in safety margins.	3
	No	Yes					Significant increase in FC workload, significant reduction in safety margins.	3
		No	Yes				Significant increase in FC workload significant reduction in safety margins.	3
			No	Yes			Significant increase in FC workload significant reduction in safety margins.	3
				No	Yes		Large reduction of safety margins.	2
					No	Yes	Large reduction of safety margins.	2
						No	Loss of separation	1

5.1.4 Barriers for OH2.1

Table 5-2: Barriers used in OH2.1 Event tree

Barriers	Description	Dependencies
Mid-term conflict		**EC-1 + EC-3 + EC-4**
FC recognizes conflicting aircraft on CDTI	Flight crew monitors situation on CDTI and compares conflict alert with displayed situation. Flight crew of own aircraft recognizes on CDTI a conflicting aircraft, realizes difference between conflict alarm and situation on CDTI. Flight crew tries to understand this situation.	EMM 1.2
Other aircraft illogical/ unexpected maneuvers – it appears that it was due to existing conflict.	Flight crew analyses actions of other aircraft and recognize that other aircraft do not act as expected. Flight crew tries to understand motives of other aircraft. For example: Other aircraft is not expected to maneuver but releases new intent.	EMM1.3
Conflicting aircraft identified based on the list of aircraft provided by SWIM	Flight crew has access to SWIM (or other external information sources) which provides list of aircraft in neighborhood ("Push mode"). Flight crew identifies an (unknown) aircraft in the list, further investigates and tries to understand this situation. Other possibility is that FC has got any doubts and asks for position of other aircraft (e.g. SWIM via "Pull mode").	EMM2.1
Conflict solved by other aircraft.	Other aircraft acts and solves conflict.	EMM 3.3
Conflict solved by own (other) aircraft, which has maneuvered because of other reason.	On the basis of other reasons flight crew of own/other aircraft maneuvers and solves this conflict.	EMM 3.2
Short-term conflict		**EC-2 + EC-3 + EC-4**
Flight crew of own aircraft visually recognizes conflicting aircraft.	Flight crew of own aircraft visually recognizes conflicting aircraft and realizes that discrepancy exists between conflict alarm and actual situation. Flight crew tries to understand this situation.	EMM 1.1

Barriers	Description	Dependencies
FC recognizes conflicting aircraft on CDTI	Flight crew monitors situation on CDTI and compares conflict alert with displayed situation. Flight crew of own aircraft recognizes on CDTI a conflicting aircraft, realizes difference between conflict alarm and situation on CDTI. Flight crew tries to understand this situation.	EMM 1.2
Other aircraft illogical/ unexpected maneuvers – it appears that it was due to existing conflict.	Flight crew analyses actions of other aircraft and recognize that other aircraft do not act as expected. Flight crew tries to understand motives of other aircraft.	EMM1.3
Conflict detected with state-based conflict detection step	Conflict has not been detected based on state vectors and flight crew tries to understand this situation.	EMM 2.1
Conflict solved by other aircraft.	Other aircraft acts and solves conflict.	EMM 3.4
Conflict solved by own (other) aircraft, which has maneuvered because of other reason.	On the basis of other reasons flight crew of own/other aircraft maneuvers and solves this conflict.	EMM 3.2

5.1.5 Event Tree for OH2.2

Figure 5-3-1: Event Tree for OH2.2 – Conflict detected incorrectly (part 1: mid-term)

OH2.2	Mid-term conflict					Safety assessment	
						Operational effect	Severity
	FC recognizes conflicting aircraft on CDTI, but the location of possible conflict seems to be different	Other aircraft illogical/ unexpected maneuvers – it appears that it was due to different expected conflict position.	True location of conflict identified based on information provided by SWIM	Conflict solved by other aircraft.	Conflict solved by own (other) aircraft, which has maneuvered because of other reason.		
	Yes					No increase in FC workload	5
	No	Yes				Slight increase in FC workload	4
		No	Yes			Slight increase in FC workload	4
			No	Yes		Slight increase in FC workload	4
				No	Yes	Significant increase in FC workload	3
					No	Continuation: Figure 5-3-2	

Figure 5-3-2: Event Tree for OH2.2 – Conflict detected incorrectly (part 2: short-term)

OH2.2	Short-term conflict						Safety assessment	
							Operational effect	Severity
	Flight crew of own aircraft visually recognizes conflicting aircraft but at unexpected location.	FC recognizes conflicting aircraft on CDTI, but the location of possible conflict seems to be different	Other aircraft illogical/ unexpected maneuvers – it appears that it was due to different expected conflict position.	Different Conflict position detected with state-based conflict detection step	Conflict solved by other aircraft.	Conflict solved by own (other) aircraft, which has maneuvered because of other reason.		
	Yes						Significant reduction in safety margins	3
	No	Yes					Significant reduction in safety margins	3
		No	Yes				Significant reduction in safety margins	3
			No	Yes			Significant reduction in safety margins	3
				No	Yes		Large reduction safety margin	2
					No	Yes	Large reduction safety margin	2
						No	Loss of separation	1

5.1.6 Barriers for OH2.2

Table 5-3: Barriers used in OH2.2 Event tree

Barriers	Description	Dependencies
Mid-term conflict		**EC-1 + EC-3 + EC-4**
FC recognizes conflicting aircraft on CDTI, but the location of possible conflict seems to be different	Flight crew monitors situation on CDTI and compares conflict alert with displayed situation. Flight crew of own aircraft recognizes on CDTI a conflicting aircraft, but realizes difference between announced conflict location and situation on CDTI. Flight crew tries to understand this situation.	EMM 1.2
Other aircraft illogical/ unexpected maneuvers – it appears that it was due to different expected conflict position.	Flight crew analyses actions of other aircraft and recognize that other aircraft do not act as expected. Flight crew tries to understand motives of other aircraft. For example: Other aircraft releases new intent, which tries to avoid different location than the expected conflict coordinates.	EMM1.3
True location of conflict identified based on information provided by SWIM	Flight crew has access to SWIM (or other external information sources). e.g. FC has got any doubts and asks for position other aircraft (e.g. SWIM via "Pull mode") and subsequently identifies different conflict coordinates.	EMM2.1
Conflict solved by other aircraft.	Other aircraft acts and solves conflict.	EMM 3.3
Conflict solved by own (other) aircraft, which has maneuvered because of other reason.	On the basis of other reasons flight crew of own/other aircraft maneuvers and solves this conflict.	EMM 3.2
Short-term conflict		**EC-2 + EC-3 + EC-4**
Flight crew of own aircraft visually recognizes conflicting aircraft but at unexpected location.	Flight crew of own aircraft visually recognizes conflicting aircraft and realizes that discrepancy exists between conflict alarm and actual situation. Flight crew tries to understand this situation.	EMM 1.1

Barriers	Description	Dependencies
FC recognizes conflicting aircraft on CDTI, but the location of possible conflict seems to be different	Flight crew monitors situation on CDTI and compares conflict alert with displayed situation. Flight crew of own aircraft recognizes on CDTI a conflicting aircraft, but realizes difference between announced conflict location and situation on CDTI. Flight crew tries to understand this situation.	EMM 1.2
Other aircraft illogical/ unexpected maneuvers – it appears that it was due to different expected conflict position.	Flight crew analyses actions of other aircraft and recognize that other aircraft do not act as expected. Flight crew tries to understand motives of other aircraft.	EMM 1.3
Different Conflict position detected with state-based conflict detection step	Conflict has been confirmed based on state vectors but different conflict coordinates determined. Flight crew tries to understand this situation.	EMM 2.1
Conflict solved by other aircraft.	Other aircraft acts and solves conflict.	EMM 3.4
Conflict is solved by own (other) aircraft, which has maneuvered because of other reason.	On the basis of other reasons flight crew of own/other aircraft maneuvers and solves this conflict.	EMM 3.2

5.1.7 Event Tree for OH3

Figure 5-4-1: Event Tree for OH3 – Conflict persists or new conflict generated (part 1: mid-term)

OH3	Mid-term conflict			Safety assessment	
				Operational effect	Severity
	Flight crew detects a change of airspace configuration and initializes new conflict resolution process.	Conflict solved by other aircraft.	The automation is substituted by flight crew, when conflict resolution is not provided.		
	Yes			No increase in FC workload	5
	No	Yes		Slight increase in FC workload	4
		No	Yes	Significant increase in FC workload	3
			No	Continuation: Figure 5-4-2	

Figure 5-4-2: Event Tree for OH3 – Conflict persists or new conflict generated (part 2: short-term)

OH3	Short-term conflict			Safety assessment	
				Operational effect	Severity
	Flight crew detects a change of airspace configuration and initializes new conflict resolution process.	Conflict solved by other aircraft.	The automation is substituted by flight crew, when conflict resolution is not provided.		
	Yes			Significant reduction in safety margins	3
	No	Yes		Significant reduction in safety margins	3
		No	Yes	Large reduction safety margin	2
			No	Loss of separation	1

5.1.8 Barriers for OH3

Table 5-4: Barriers used in OH3 Event tree

Barriers	Description	Dependencies
Mid-term conflict		**EC-1 + EC-3 + EC-4**
Flight crew detects a change of airspace configuration and initializes new conflict resolution process.	Flight crew monitors the situation and thus is able to notice any airspace configuration change. FC may initialize new conflict resolution process when required.	EMM 1.1, EMM 1.2
The automation is substituted by flight crew, when conflict resolution is not provided.	Flight crew is aware of the automation processes and analyzes outputs of SSEP functions. Flight crew substitutes, when automation processing exceeds given reaction limit. Note: *When proposed conflict resolution is not conflict free, the flight crew acts as internal mitigation mean, because this resolution is flown if and only if accepted by the flight crew.*	EMM 1.2, EMM 1.4
Conflict solved by other aircraft.	Other aircraft (with lower priority) acts and solves conflict.	EMM 3.3, EMM 3.2
Short-term conflict		**EC-2 + EC-3 + EC-4**
Flight crew detects a change of airspace configuration and initializes new conflict resolution process.	Flight crew monitors the situation and thus is able to notice any airspace configuration change. FC may initialize new conflict resolution process when required.	EMM 1.1, EMM 1.2
The automation is substituted by flight crew, when conflict resolution is not provided.	Flight crew is aware of the automation processes and analyzes outputs of SSEP functions. Flight crew substitutes, when automation processing exceeds given reaction limit. Note: *When proposed conflict resolution is not conflict free, the flight crew acts as internal mitigation mean, because this resolution is flown if and only if accepted by the flight crew.*	EMM 1.2, EMM 1.4
Conflict solved by other aircraft.	Other aircraft acts and solves conflict.	EMM 3.4 EMM 3.2

5.1.9 Event Tree for OH4

Figure 5-5-1: Event Tree for OH4 – Airborne-self separation failure (part 1: mid-term)

OH4	Mid-term conflict	Safety assessment	
		Operational effect	Severity
	Emergency procedure is initiated		
	Yes	Significant increase in FC workload	3
	No	Continuation: Figure 5-5-2	

Figure 5-5-2: Event Tree for OH4 – Airborne-self separation failure (part 2: short-term)

OH4	Short-term conflict		Safety assessment	
			Operational effect	Severity
	Emergency procedure is initiated	Possible conflict solved by other aircraft		
	Yes		Significant reduction in safety margins	3
	No	Yes	Large reduction safety margin	2
		No	Loss of separation	1

5.1.10 Barriers for OH4

Table 5-5: Barriers used in OH4 Event Tree

Barriers	Description	Dependencies
Mid-term conflict		**EC-1 + EC-3 (EC- 4 or ASSUMP-7-COM)**
Emergency procedure is initiated	Flight crew knows about the total and fatal malfunction of ASAS equipment, announces its emergency status to other aircraft (via ADS-B, SWIM or by voice communication). Other aircraft receive this emergency status. This information assigns the largest priority number to own aircraft. On the basis of emergency procedure own aircraft only flies the shortest way to get out of SSA and other aircraft maneuver to solve all possible conflicts.	EMM 4.1, EMM 4.2, EMM 3.3
Short-term conflict		**EC-2 + EC-3 (EC- 4 or ASSUMP-7-COM)**
Emergency procedure is initiated	Flight crew knows about total fatal malfunction of ASAS equipment, announces its emergency status to other aircraft (via ADS-B, SWIM or by voice communication).Other aircraft receives this emergency status. On the basis of emergency procedure own aircraft does not maneuver to solve possible conflicts and conflict resolution is ensured by other aircraft.	EMM 4.1, EMM 4.2, EMM 3.4
Possible conflict solved by other aircraft	Other aircraft acts and solves this conflict	EMM 3.4

5.2 ASOR

5.2.1 Fault Tree for OH1 – Conflict False Alarm

The operational hazard OH-1, the False alarm is, in short, a detection of any conflict in a conflict-free environment. This may happen due to imprecise input information concerning the own or other aircraft or due to any malfunction in conflict detection process onboard of an own aircraft.

The own aircraft state vector (position and velocity) may be determined incorrectly (BC-15). Other confusion may happen in connection with own aircraft intent. The own aircraft ASAS may work with an intent which is different from the flown one (BC-3). This might be caused by improper execution initiation (BC-3a, see Figure 4-5: State and intent realization and broadcast path) or by any imprecise execution of desired trajectory (intent) by an own aircraft (BC-3b).

Similarly as in own aircraft case, the other aircraft state vector (position and velocity) may be determined incorrectly (BC-15) on a board of other aircraft. The intent may be different from the flown one because of improper execution initiation or by any imprecise execution of desired trajectory (intent), BC-3a,b.

The surveillance functional block is responsible for the synthesis and processing of own and other aircraft data. When the conflict detection process is corrupted (BC-7c), there may appear incorrect resolutions concerning the conflict existence, even in case that all input information about own aircraft state or surrounding traffic information are both of a high quality. The surveillance failure may be an short-term issue or a temporal ASAS general bug.

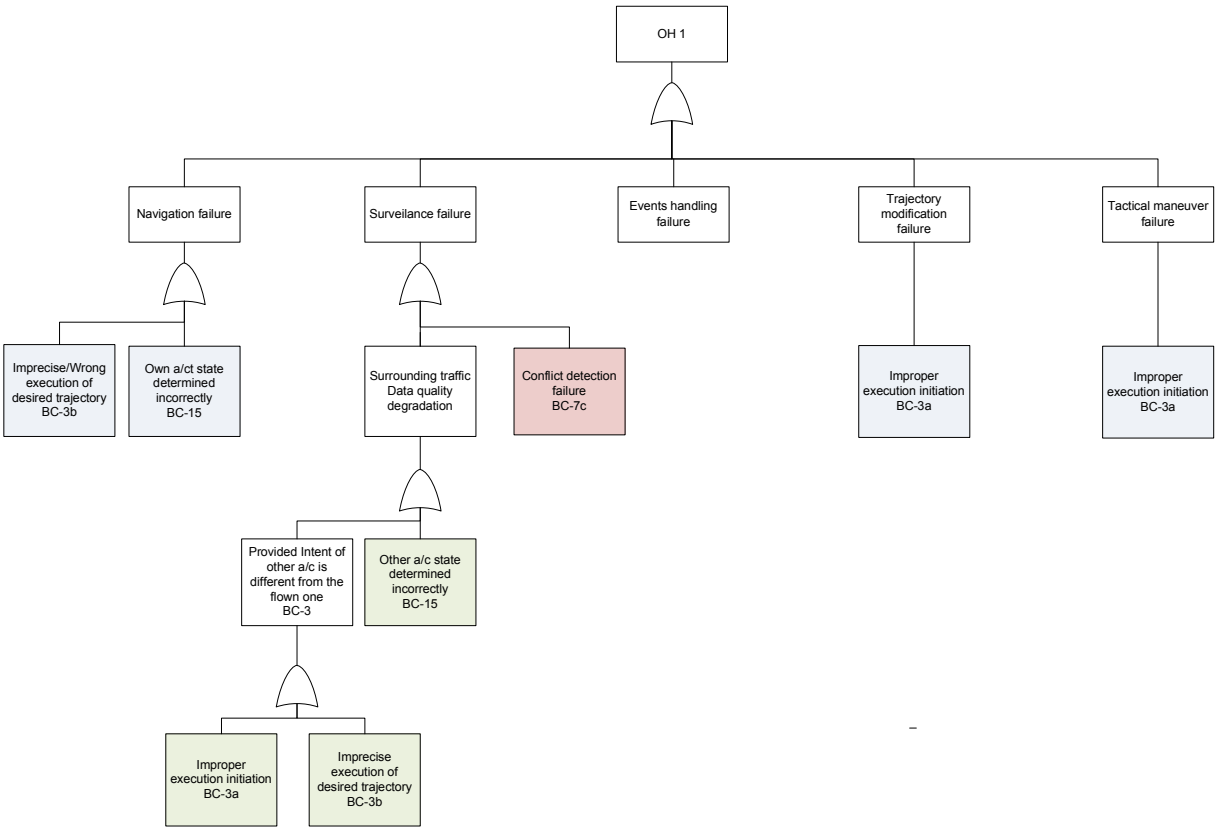

Figure 5-6: Fault Tree for OH1.

5.2.2 Fault Tree for OH2.1 – Conflict Not Detected

The operational hazard OH-2.1, points to a situation when true conflict with other aircraft is not detected at all. This may happen due to imprecise input information concerning the own or other aircraft or due to any malfunction in conflict detection process onboard of an own aircraft. Besides these causes identical to causes of OH1, there might be the total lack of other aircraft information. So even the own aircraft may not be aware of presence of any other aircraft along its RBT.

The own aircraft state vector (position and velocity) may be determined incorrectly (BC-15). Other confusion may happen in connection with own aircraft intent. The own aircraft ASAS may work with an intent which is different from the flown one (BC-3). This might be caused by improper execution initiation (BC-3a, see Figure 4-5: State and intent realization and broadcast path) or by any imprecise execution of desired trajectory (intent) by an own aircraft (BC-3b).

Similarly as in own aircraft case, the other aircraft state vector (position and velocity) may be determined incorrectly (BC-15) on board of other aircraft. The intent may be different from the flown one because of improper execution initiation or by any imprecise execution of desired trajectory (intent). Moreover, the information about other aircraft state and intent might be completely unavailable due to other aircraft transmission failure (BC-1) or due to own aircraft receiving failure (BC-16). The ADS-B messages with state and intent information may be lost (for a longer time period) due to unfavorable environmental conditions (BC-16)

The conflict detection in Surveillance FB may be functional in case of OH2.1 only the conflict identification is not delivered within time limit (BC-7a) or the conflict detection process is corrupted and as a special case, the existing conflict is not detected at all (BC-7c).

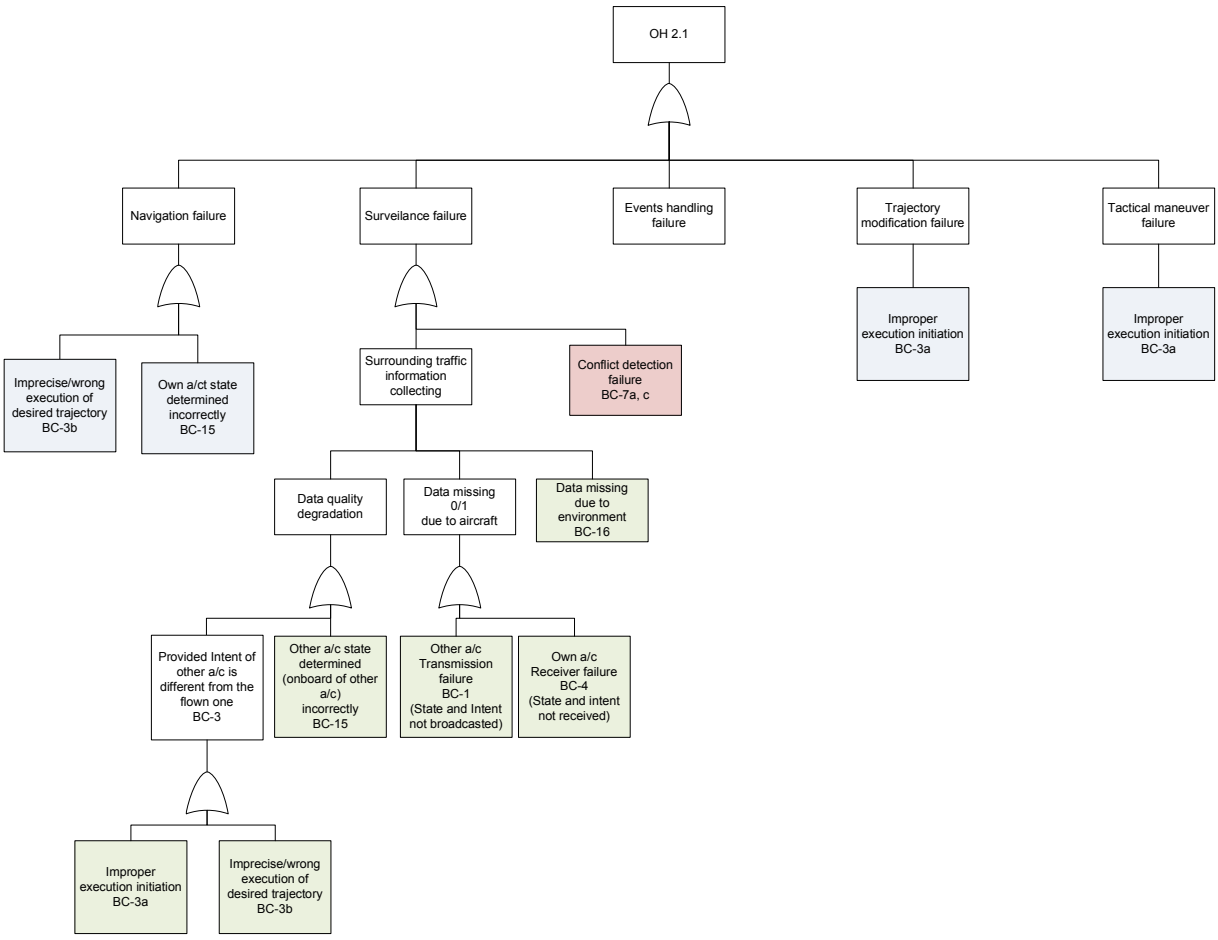

Figure 5-7: Fault Tree for OH2.1.

5.2.3 Fault Tree for OH2.2 – Conflict Detected Incorrectly

The operational hazard OH-2.2, points to a situation when true conflict with other aircraft is detected but its position or RTTL is determined incorrectly. This may happen due to imprecise input information concerning the own or other aircraft or due to any malfunction in conflict detection process onboard of an own aircraft. The OH2.2 has got exactly the same mechanism of the birth as OH1 so the Fault trees for both OHs are identical with the only exception of BC-7b (**The location of conflict and RTTL do not meet required precision)**

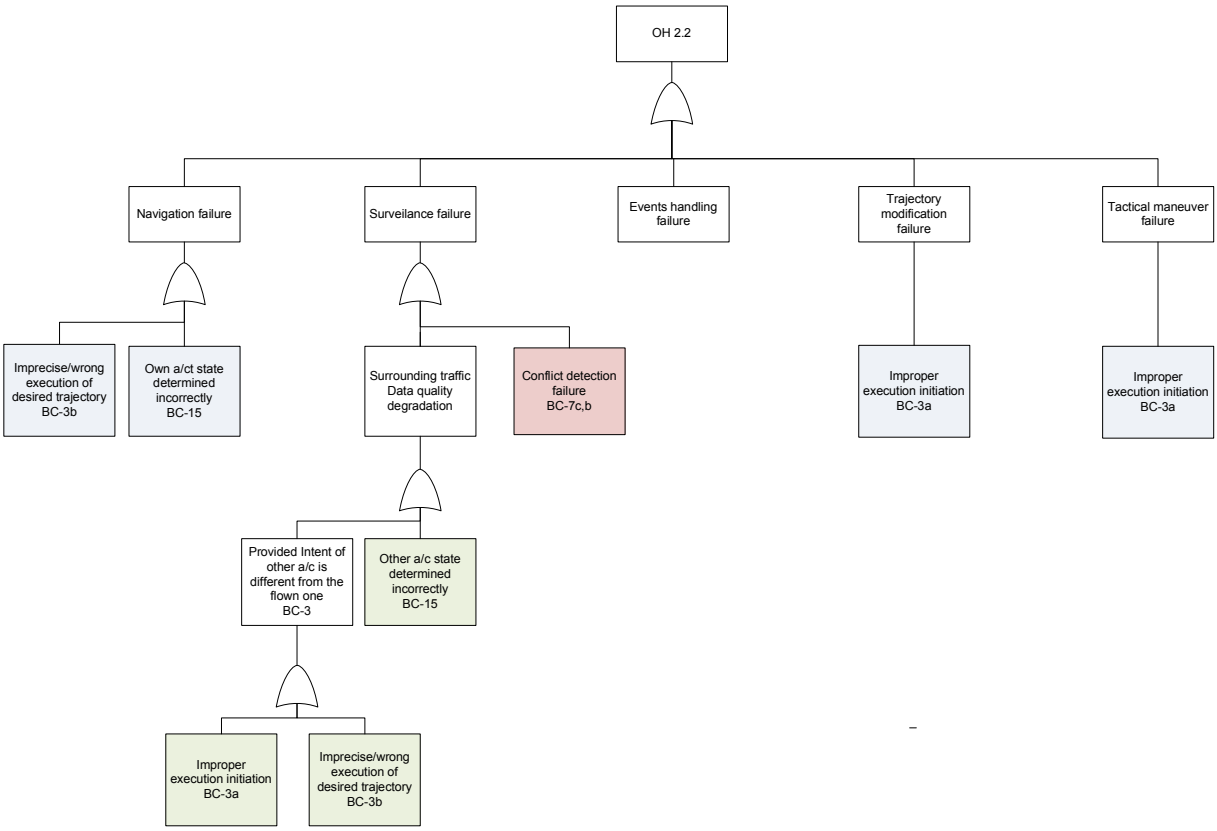

Figure 5-8: Fault Tree for OH2.2.

5.2.4 Fault Tree for OH3 – Conflict Persists or New Conflict Generated

First, Operation hazard OH 3 covers situations, when conflict is detected, but the proper conflict resolution is not provided and consequently the **conflict persists**. The proposed fault tree consists of a set of basic causes solely related to absence or degradation of ASAS functionalities. Surely, when there is no traffic information (state and intent of own and other aircraft including), the conflict resolution cannot be provided as well. But OH3 follows the regular state RS4, which would not be initiated without conflict detection based on traffic information. Of course, this information may be imprecise or not up-to-date, but still the own aircraft is aware of the conflict and other aircraft existence.
When an OH3 fault tree had been constructed, it was assumed that:

- **The surroundings traffic information is considered to be available (but not necessarily correct).**

Conflict resolution is not provided, when conflict processing is not initiated correctly, conflict resolution is not provided or the proposed conflict resolution is not executed. Problematic conflict resolution process initiation is connected with following basic causes: BC-8, BC-9 and BC-10. Case of open maneuver not followed by the closed one is also covered by BC-9 and BC-10.

Conflict resolution is not provided when ASAS does not propose any solution (BC-11) or the flight crew does not accept conflict resolution in time (BC-13). The case of not initialized conflict resolution execution is covered by BC-17. Also improper conflict resolution (BC-3a) contributes to conflict resolution execution problems.

Conflict resolution provision and execution failures may happen within closed maneuver (Trajectory modification failure) or open maneuver (Tactical maneuver failure).

The second compound of OH3 is the case that proposed **RBT is not conflict free**. New conflict is generated or the former one is not solved, even if any conflict resolution is proposed and accepted by the FC. The label placed in FT (*Proposed solution does not follow AFR*) refers to a broader class of RBTs, but technically the BCs point only to not-conflict-free trajectory problem.
Insufficient quality of proposed conflict resolution (BC-12 a,b) may be caused by

- ASAS failure
- Wrong input information.

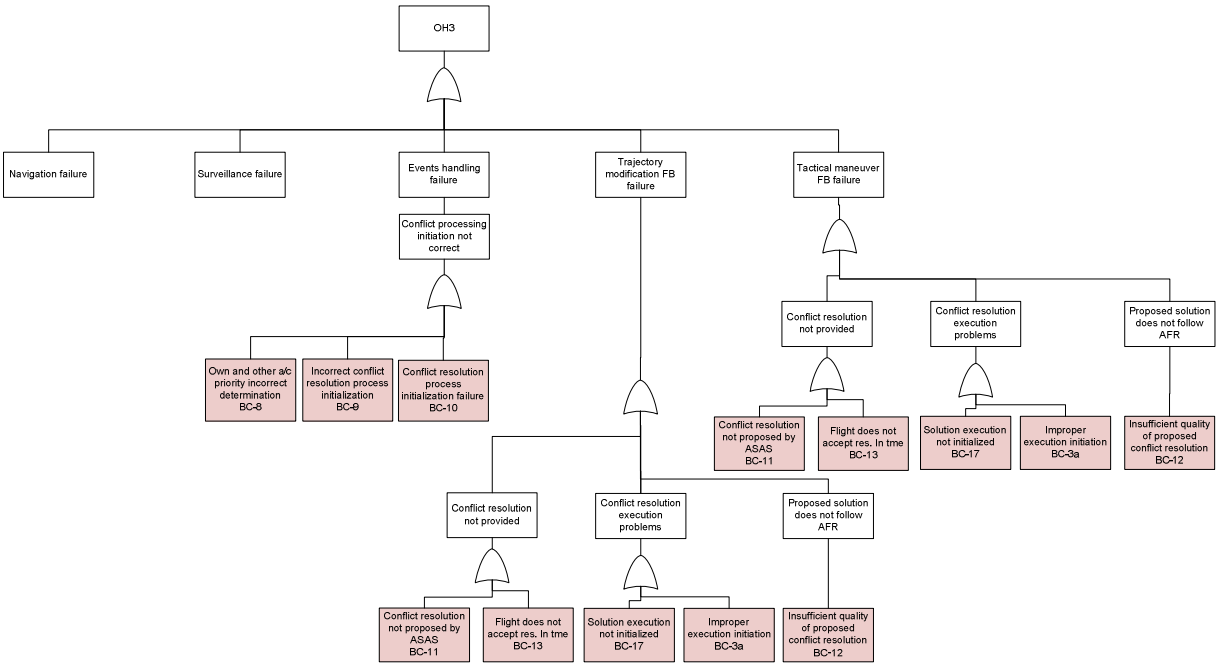

Figure 5-9: Fault Tree for OH3.

5.2.5 Fault Tree for OH4 - Airborne Self-Separation Failure (detected)

Operation hazard 4 is indicated when aircraft is not capable to continue in the airborne self-separation mode. This operational hazard is caused by irreversible fatal malfunction of ASAS equipment responsible for any step of airborne self-separation process:

- Own aircraft state and intent transmission failure (BC-1)*
- Surveillance – when own aircraft receiver is not functional (BC-4)* or conflict detection process is corrupted (BC-7c)
- Conflict processing
    - Events handling – Conflict resolution process initiation is corrupted (BC-10b)
    - Trajectory modification and Tactical maneuvering – Conflict resolution process is corrupted (BC-11b)

The ASAS equipment failure is supposed to be permanent. It is not a temporal loss of functionality and flight crew is not able to ensure substitution for non-functional ASAS. It is assumed, that airborne self-separation failure is always detectable and detected.

*Note on BC-1 and BC-4:

Transmission and surrounding traffic information receiving is not ASAS specific, but this technology functionality is essential for the successful flow of SSEP.

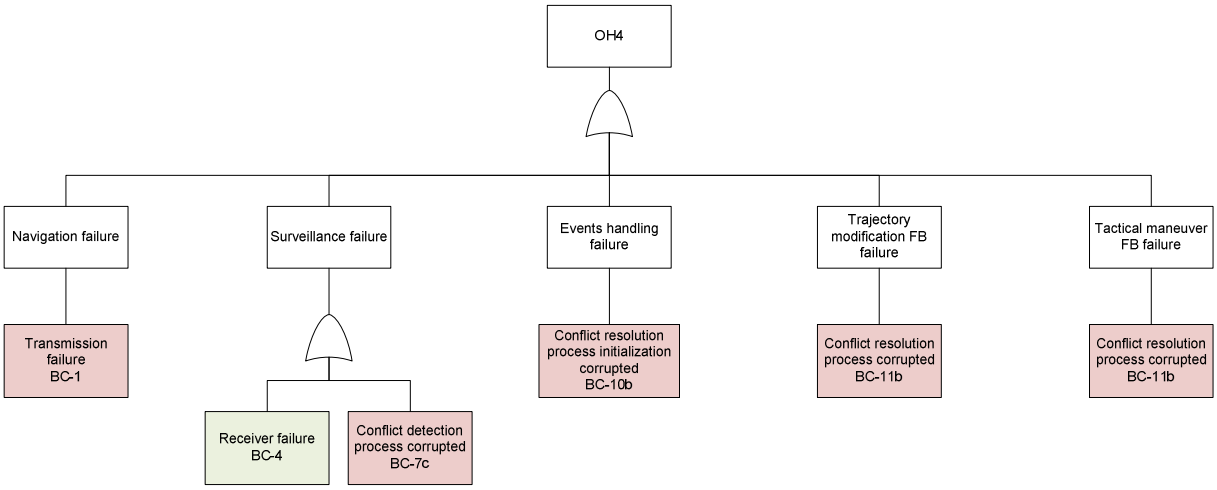

Figure 5-10: OH4 Fault Tree.

6. Conclusions

The aim of the iFly WP9 is to proceed with the operational assessment of self separation operations described in the A3 Concept of Operations (iFly:D1.3) using the ED-78a/DO-264 methodology. The first step towards this goal is represented by the Operational Services and Environment Description (OSED) provided in iFly:D9.1. The present document together with iFly:D9.3 build on OSED and continue along the ED-78a/DO-264 framework by providing Operational Safety (D9.2) and Performance (D9.3) Assessment.

Already from the very beginning of the iFly project it was known that the application of ED-78a/DO-264 will not be straightforward due to the innovative nature of the iFly project whose research activities are aligned with the phase V1 of E-OCVM methodology. Typically, a lot of details required for conducting a full ED-78a/DO-264 analysis are not known yet in this stage of concept development. Hence, A3 ConOps currently defines an operational framework and specifies the onboard system in terms of high-level functional requirement. This does not allow a detailed allocation of low-level tasks, detailed analysis of human-automation interaction, etc.

In this situation, this document presents the results of a preliminary OSA focused on high-level operational hazards without quantitative (probabilistic) analysis of the related fault and even trees. Due to the lack of details considering specifications of onboard system and the related HMI, the analyzed hazards are focused on the behavior of a self separating aircraft in the overall ATM system, i.e., on aircraft's behavior potentially directly affecting the surrounding traffic. The following situations are considered in this context: aircraft is reacting on a non-existing conflict (OH1 – False alarm), aircraft is not properly reacting on an existing potential conflict (OH2 - Conflict not detected, OH3 – Improper conflict resolution), and a general (detected) failure of ASAS system (OH4). The OSA itself then describes the initial concept, as well as the logic and causality structure of the identified hazards (external/internal mitigation means, fault trees, event trees, hazards classification).

The aim of the presented analysis is to provide a solid basis for subsequent connecting research in this area (based on the refined concept) and to support the future development by identifying key elements (missing or insufficiently defined) required for conducting a full ED-78a/DO-264 operational assessment. At the same time, the presented analysis of potential failures can provide important guidelines for the A3 concept refinement. In this context, it is important to mention that in addition to the analysis according ED-78a/DO-264 methodology conducted in WP9, the hazards related to A3 operations were also studied in iFly's WP2 and WP7.1 using alternative methods. The corresponding results partially complement the outcomes of this OSA and provide another valuable input for follow-up study.

Appendix 1: Safety Requirements – New Proposals

This chapter includes proposals, which could reduce the risk of operational hazards development or lower the severity class of final worst Operational effects. These proposals are not covered by SSEP original description in iFly:D1.3 or iFly:D9.1 but might be further investigated and their contribution assessed.

Information sharing among aircraft – the aircraft may share some additional pieces of information except from state and intent.

- **SR-N -1.1: Detected conflicts sharing -** Aircraft notices all aircraft, which are in conflict and via peer-to-peer communication ask for confirmation of detected conflicts. Other possibility is the usage of SWIM. SWIM may re-distribute all conflicts list in an area, which will include conflicts confirmed by all participants. In case the conflict is not confirmed, all/both participants are called upon the revision of onboard conflict detection process. This mitigation mean does not work, when own aircraft works with corrupted state and intent information (of any of conflict participants) and is not aware. The SR-1.1 could be efficient in detection of ASAS conflict detection failures.
- **SR-N-1.2:"Intent to be changed" notice –** in case the aircraft is planning trajectory change and the conflict resolution process is initiated. The special notice for other aircraft could be broadcast, to announce that currently broadcast intent is planned to be change. Possibly the **expected time of intent update** could be released.
- **SR –N-1.3: Suspicion sharing –** when own aircraft analyses the actions of other aircraft, it may notice other aircraft actions may be incorrect/unexpected. E.g. other aircraft announces new intent, which is not conflict free. The own aircraft shall first check its own processes and then if doubts concerning other aircraft actions remain, send a notice to other aircraft. The confirmation concerning this notice need not be required.

SWIM and ground equipment support

- **SR-N-2.1: Back-up conflict detection -** Using state and intent (possibly RBT) information reported to SWIM any ground equipment may re-analyze the SSA and produce its own list of conflicts. This could be done under assumption that SWIM receives updates of aircraft data with sufficient frequency.
    - *Possible mitigation means in case of Surveillance functions failure.*
    - *If there are other data sources available (except from ADS-B reports)-a possible mitigation mean for Surveillance FB or Navigation FB.*
- **SR-N-2.2: List of aircraft in neighborhood** – extracted from RBTs provided to SWIM by aircraft before the flight. This list is a summary of EXPECTED aircraft in own aircraft neighborhood. This list is not identical to the one built upon received state and intent ADS-B reports of aircraft.
    - *Possible mitigation means in case of aircraft transmitter failure.*

New parameters of SSEP procedure

- **SR-N-3.1: Conflict processing performance (CPP)** introduced in iFly:D9.1 may be a time parameter, monitored/estimated by own aircraft for all aircraft involved in conflict. In case the other aircraft does not show an activity beyond this time horizon (despite the fact the activity is expected. E.g. by aircraft with lower priority number), it may be contacted. The activity may be a defined as new intent release, maneuver or release of "intent to be change" notice.

Conflict resolution

- **SR-N-4.1: Short –term conflict resolution algorithms demands -** A conflict should be optimally detected within mid-term time horizon and further solved by means of mid-term conflict resolution. When RTTL decreases, then the conflict shall be solved as a short term one and the on-board solution shall be searched by short-term conflict resolution algorithm. The short – term conflict resolution algorithm should fulfill the followings
  - It is a "1 to N" type of resolution algorithm (iFly: D1.3: chapter 8.6)
  - Only one maneuvering aircraft shall solve the situation (a pair-wise conflict scenario). The active participation of both aircraft is expected, but the proposed conflict resolution should enable the own aircraft to solve the conflict even when other aircraft, from any reason, do not conduct a complementary maneuver.
- **SR-N-4.2: Appropriate definition of "Restart conditions" –** when conflict is detected Events handling FB shall identify what type of maneuver and type of conflict resolution algorithm should be used and consequently activate the appropriate conflict resolution process. The conflict should be started to be solved as soon as possible. A problem arises when new conflict appears while the former one is not yet resolved, possibly the conflict resolution is still evaluated by flight crew. The flight crew shall not be interrupted or disturbed too often.
  So the set of proposals, when the conflict resolution process shall be restarted, has been formulated:
  - The conflict resolution process has not yet proposed the conflict resolution to the flight crew.
  - In general: a more serious situation appears and requires instant resolution.
    - A new short-term conflict appeared when mid-term conflict was assessed.
  - The conflict resolution proposal has been postponed to the FC assessment but new circumstances appeared. Such a circumstance might be
    - A new intent released by other aircraft would lead to a short-term conflict, if currently proposed solution would be accepted and flown by own aircraft.
    - A solved conflict is no more a current affair. The flight crew shall be informed, that conflict resolution process has been terminated.

Appendix 2: List of Operational, Performance and Functional Requirements

There has been identified a set of Operational, Performance and Functional Requirements in iFly: D9.1 document. The following appendix is a summary of these requirements. Table A2-1 defines, together with Tables 2-1, 2-2 and 2-3 from chapter 2, a departure SSEP characteristics used in SSEP OSA process.

Table A2-1: Operational (OR), functional (FR) and performance (PR) requirements together with priority rules determination (PRD).

Requirement	Description	Location in OSED iFly: D9.1
OSED-1-OR	Broadcast information shall include the data about accuracy and integrity of the transmitted trajectory information. The data shall reflect the actual navigation capability of own aircraft and flown guidance mode (including manual flight).	Regular flight stage Page 23
OSED-2-OR	Selected action shall conform to Autonomous Flight Rules.	Initiation stage Page 24
OSED -3-OR	a) Any kind of conflict has priority over the trajectory optimization. b) Short-term conflicts have priority over mid-term conflicts.	Initiation stage Page 24
OSED -4-OR	a) CR maneuver shall not generate a new short-term conflict. b) CR maneuver shall be conforming to AFR (implicit coordination if applicable, blunder protection, etc.) c) Tactical Maneuvering stage is followed by the New trajectory generation stage, which generates a new RBT.	Tactical maneuvering stage Page 24
OSED -5-OR	a) New trajectory must be conflict-free at least up to the mid-term time horizon. b) New trajectory shall be conforming to AFR (blunder protection, etc.)	New trajectory generation stage Page 25

Requirement	Description	Location in OSED iFly: D9.1
OSED -6-PR	a) The broadcast intent allows a prediction of the aircraft planned trajectory up to MTTH (SL2 and SL3). b) Whenever the intent information of an aircraft is changed, a new intent should be broadcast **immediately** (SL2 and SL3).	Navigation FB
OSED -7-OR	a) If the information about relevant traffic is not updated according to the performance requirements: a. The information must be marked as obsolete or invalid (both for state and intent data). b. If applicable (SL3), this information must be queried from the corresponding aircraft or from SWIM. b) SWIM provides a complete list of aircraft relevant to own flight up to Mid Term Time Horizon – traffic list (SL3). c) (SL3 only) In the case of missing information about an aircraft on the traffic list, the information must be queried from SWIM. d) Conflict detection will run continuously during the SSEP operation and all detected conflicts will be reported. **e) There is no change in communications as a result of detected conflicts.**	Surveillance FB Page 29
OSED -8-OR	a) Conflict detection is a continuous process which runs at a given frequency (TBD) with the best information available. b) SP should be maximally TBD seconds/minutes	Surveillance FB Page 29
OSED -9-OR	Situation assessment runs continuously, during the time when conflict information is available.	Events handling FB Page 30
OSED -10-PR	LP – should take maximally predefined time (TBD)	Events handling FB Page 30
OSED -11-OR	a) The algorithm does not rely on any actions from the conflicting aircraft. b) The proposed conflict solutions follow AFR, in particular, they are conflict-free up to or beyond the MTTH, blunder protection is considered, etc. c) Optimization process (in absence of any conflict) modifies the RBT only beyond the MTTH.	Trajectory modification FB Page 31

Requirement	Description	Location in OSED iFly: D9.1
OSED-12-FR	a) The proposed solution is valid at time of execution (i.e., it has to take into account ED). Flight crew is responsible to take action to solve the detected conflict. System provides only advisories.	Trajectory modification FB Page 31
OSED -13-OR	a) The algorithm does not rely on any action from the conflicting aircraft b) The proposed conflict solutions follow AFR (implicit coordination if applicable, blunder protection, etc.). c) Conflict resolution makes full use of all information available at time RT (Reference Time, see Figure 2, iFLY: D9.1). It remains to be investigated within OSA and OPA how to deal with updated information that is received after RT, whereas the crew has not yet decided what to do.	Tactical maneuver FB Page 31
OSED -14-FR	a) Algorithm is able to solve conflicts with multiple aircraft. b) The proposed solution(s) are valid at time of execution (i.e., it has to take into account ED). Flight crew is responsible to take action to solve the detected conflict. System provides only advisories. In other words, the trajectory update is executed only after flight crew approval.	Tactical maneuver FB Page 31

Requirement	Description	Location in OSED iFly: D9.1
OSED-15-PRD	Priority level utilization a) Priority rules are applied only to Medium Term Conflict Resolution. b) Priority rules determine the priority level of each aircraft, that means determine which aircraft has got the right way and which aircraft has to manoeuvre. c) Priority rules will be identical for all aircraft. Priority level considerations are the following d) Priority level will be broadcast so it can be used by other aircraft e) Priority level will be determined based on a. CTA requirements b. Manoeuvrability c. Mission statement f) Aircraft with lower priority level have to manouevres to prevent the conflict from becoming a short term conflict. g) In case of identical priority levels, an arbitrary procedure (based in the aircraft call signs for example) will be used to ensure that priority is always unambiguous.	Appendix 2: Priority rules Page 39

Appendix 3: Methodology – Definitions

For complete list of OSA definitions see (RTCA DO-312), pages 128-129. Selected terms defined differently in a framework of SSEP procedure are listed below.

Internal Mitigation Means (IMM) – factors that prevent operational hazard from birth.
RTCA DO-312 document states that IMM are factors within the application that help meet the Safety Objective assigned to the hazard. Since SSEP procedure is so complex, hardly any factors lie outside the procedure. It seems to be more natural to split mitigation means to those ones, which forestall the operational hazard and those ones, which moderate the resulting operational effect.

External Mitigation Means (EMM) - factors that help reduce the impact of an existing operational hazard once the hazard has occurred, reduce the severity of operational effect of existing OH.

Operational hazard Detection Means (DM) - class of external mitigation means which result in operational hazard detection.
The detected OH is likely to have less severe consequences (operational effect) in comparison with situations when OH remains undetected. Detected OH allows e.g. for effective utilization of emergency procedures.
The location of DMs is different from the one presented in (RTCA DO-312, p. 139), where they are located within the fault tree, ASOR section. We propose to discuss the possibility of detection in connection with operational effect further in OHA step.

Safety Requirements (SR) – are risk mitigation means. SR is a requirement that when implemented, will help the system meet the safety objective or reduce effects. SR may take various forms, including organizational, operational, procedural, functional, performance and interoperability requirements or environment characteristics (RTCA DO-312).
Within OSA, two types of SR are discussed. First group of SRs forms the proposals of new SSEP elements not covered in SSEP procedure as stated in OSED (iFly:D9.1).
The second group of SRs is a list of identified parameters, probabilities of accomplishment of several operational requirements/boundaries from OSED. Again the numerical assessment is not provided.

6.1.1 Other Terminology Used Through iFly: D9.2

Own aircraft / ownship – the autonomous aircraft, from which perspective the airspace situation is described and analyzed.
Other aircraft – the autonomous aircraft, which occurs along trajectory of own aircraft. This aircraft may be the conflicting one.

Appendix 4: Interconnections with iFly:D7.1b

iFly WP 7.1 identified the hazards during a set of brainstorm sessions with experienced pilots and controllers. In addition, iFly WP7.1 has performed an initial qualitative analysis of these hazards [5]. The identified hazards spread over all aspects of SSEP operations and they are typically focused to concrete onboard tasks (the level of detail intentionally avoided in this document). In this context, they complement very well the analysis provided in this document and, furthermore, provide important guidelines for the further concept refinement and design of onboard system.

For reference, the overview of the hazards identified in iFly:D7.1b is provided below together with the potential link to the elements of this OSA document. Some of the hazards overlap with the basic causes considered in the OSA, in particular considering:

- FC problems (e.g. IMM9-11, BC-13,18)
- Information quality: ADS-B performance, Navigation performance (e.g. BC-15,16,3,4).

The initial set of hazards (iFLy: D7.1b, Tables 1 and 3) covers a large variety of problems, such as human-automation communication problems, flight crew responsibilities, inner data exchange and aircraft technical problems during the flight execution. The analysis of these hazards conducted in WP7.1 determined a list of main intent related (non-nominal) conditions (iFly:D7.1b, Table 7) .

Many hazards covered in iFly:D7.1b (Tables 3,5) are beyond the scope of the current OSA study (see Assumptions formulated in Section 2 and Appendix 2 of this report) or considered higher level of detail (e.g., a particular cockpit design) and thus **have not been investigated.** It is possible to mention in this context namely aircraft technical problems (e.g. T4, T8), MA to SSA transfer and vice versa (e.g.M35, M58, M59), security issues and intentional AFR violation (e.g. M20), TCAS/ACAS interaction with ASAS (e.g. T44, M11), CDTI/ASAS design (e.g.M27), SSEP operations design (e.g. M60), MFF design specific issues (M57), not ASAS specific problems (e.g. T40), etc.

This appendix provides the full lists of hazards identified within D7.1b and links them with the work performed as part of D9.2. In case of non-existing link, that is, if the hazard was not studied within OSA, the rationale is given as follows:

OS – Out of Scope
D – The OSA is not so Detailed
DC – Different Concept specific

Table A4-1: Hazards identified during Tallinn brainstorming sessions and their role in iFly:D9.2 operational safety assessment.

iFly: D7.1b (Table 1)	iFly: D9.2
T1 Too much information on CDTI	Not studied (D)
T2 Situational awareness differences between crew members	Not studied (D)
T3 Pilot should take action but is unaware and waiting for information	BC-13 OR BC-17
T4 For Short Term Conflict (STC) only vertical and/or horizontal manoeuvre may be useful.	Not studied (D)
T5 Weather may deviate from prediction received through SWIM	BC-3 c
T6 Pilot perception of weather areas may differ from info received	Not studied (D)
T7 Individual fighter aircraft out of a flight may be invisible	Not studied (OS): ASSUMP-1-EC
T8 Passenger comfort of RTA	Not studied (OS): ASSUMP-5-OTH
T9 Unknown aircraft (e.g. weather-, leasure balloons)	Not studied (OS): ASSUMP-1-EC
T10 Aircraft with priority as a result of non-normal circumstances are in the neighbourhood	Not studied (OS)
T11 UAV in neighbourhood	Not studied (OS): ASSUMP-1 -EC
T12 Non-proper A3 ConOps equipped aircraft in SSA	Not studied (OS): ASSUMP-1-EC
T13 Global weather change, which implies weather changes for multiple aircraft	Not studied (OS)
T14 Rules of the air (unclear, misunderstood)	Not studied (D)
T15 Highjack or uncontrolled aircraft	For highjack: Not studied (OS): ASSUMP-4-OTH For uncontrolled aircraft: Not studied (OS): ASSUMP-5-OTH
T16 Pilots sleeping	Not studied (OS): ASSUMP-5-OTH
T17 SWIM bandwidth issues and lack of back-up in SWIM	BC-16
T18 Awareness confusion because of too much info / (autopop up)	Not studied (D)
T19 Multiple military aircraft en-route-formation (Standard- vs. non-standard formation) with leader squawking only	Not studied (OS): ASSUMP-1-EC

iFly: D7.1b (Table 1)	iFly: D9.2
T20 Positioning error (various reasons)	BC-15
T21 Emergency situations may lead to workload saturation at a moment that the crew is busy	Not studied (OS)
T22 Pilot can put input into FMS what they like	Not studied (OS): ASSUMP-4-OTH
T23 Pilot deviates from the assumed RBT	BC-3b
T24 Trajectory management box fails	OH4 BC-1 or BC-4 or BC-7c or BC-10b or BC-11b
T25 Out of envelope of RBT	BC-3b
T26 (National) events of closed airspace	Not studied (D)
T27 Volcanic eruption	Not studied (OS): ASSUMP-5-OTH
T28 Pilot can disconnect FMS and fly himself	Not studied (OS): ASSUMP-1-EC, ASSUMP-4-OTH
T29 Pilot disconnects FMS	Not studied (OS): ASSUMP-1-EC, ASSUMP-4-OTH
T30 State vector may not be useable to predict conflict	OH1, OH2.1, OH2.2
T31 Common cause for multiple systems going down	OH4 BC-1 or BC-4 or BC-7c or BC-10b or BC-11b
T32 NOTAM changes get delayed into SWIM (Eg special use in airspace)	BC-3d or BC-3c
T33 Structural design limits of airplane (e.g. speed range, buffeting)	BC-3 b
T34 Special use airspace that moves and which is not allowed to be entered into SWIM (e.g. Royal family)	Not studied (OS): ASSUMP-1-EC
T35 Performance limitations (e.g. heavier than aircraft system)	BC-3b
T36 Aircraft in-flight damage	Not studied (OS): ASSUMP-5-OTH
T37 Weight uncertainty	BC-12b OR BC-15
T38 Performance degradation over time	Not studied (OS) ASSUMP-5-OTH
T39 Coffin corner	Not studied (OS) ASSUMP-5-OTH
T40 Icing	Not studied (OS): ASSUMP-5-OTH
T41 Meter versus feet	Not studied (D)
T42 Inability to assess the track of other traffic	BC-4-EQP, BC-7, BC-16

iFly: D7.1b (Table 1)	iFly: D9.2
T43 TCAS not useable for lateral maneuvers	Not studied (OS): ASSUMP-2-OTH
T44 TCAS/CDTI is unstable	Not studied (OS/D): ASSUMP-2-OTH
T45 Quality of position fusion results	BC-5
T46 Quality of weather	BC-3c
T47 Individual differences of pilots	Not studied (D)
T48 Sequence of actions varies	Not studied (D)
T49 Airlines cultural differences	Not studied (D)
T50 Areas to be avoided due to icing	Not studied (OS): ASSUMP-4-EC
T51 Contingency management remains to be defined	Not studied (D)
T52 Reliability of pitot-static	Not studied (OS): ASSUMP-5-OTH
T53 Reliability of sensors	Not studied (OS): ASSUMP-5-OTH
T54 System requirements of anti-icing systems influence performance	Not studied (OS): ASSUMP-5-OTH
T55 GPS failure affects present position / ground speed used by autopilot / FMS	BC-15
T56 Failure reports get not through in airline	Not studied (D)
T57 Spatial disorientation	Not studied (D)
T58 Loss of being ahead of events.	Not studied (D)
T59 Failure reporting is more complex (might require more recording systems in the aircraft)	Not studied (D):

Table A4-2: Hazards identified during MFF 2004 and their role in iFly:9.2 operational safety assessment.

iFly: D7.1b (Table 3)	iFly: D9.2
M1 Pilots making own judgement on relevance of conflicts and acting only on conflicts judged relevant; misjudgement may lead to not reacting to an important alert.	Not studied (OS): ASSUMP-4-OTH
M2 Pilots making own judgement on relevance of (reported, alerted) failures and acting only on failures judged relevant; misjudgement may lead to not reacting to an important alert.	Not studied (OS): ASSUMP-4-OTH
M3 If situation is judged safe, no further action is taken though ASAS or ACAS still speaks of conflict.	Not studied (OS): ASSUMP-4-OTH

iFly: D7.1b (Table 3)	iFly: D9.2
M4 Nuisance alerts enhance the effect that pilots make own judgements of conflicts.	Not studied (D)
M5 Nuisance alert: An aircraft climbing and an aircraft descending to each other, but levelling off 10 FL before meeting. In case of intent-less ASAS this causes an alert.	Not studied (D)
M6 Nuisance alerts may be expected near the transitions between MAS and FFAS, due to the sizes of the protected areas.	Not studied (OS): ASSUMP-2-EC
M7 Nuisance alert: aircraft flying level on FL 370, another aircraft climbing to FL 380 and levelling off too slowly to prevent conflict.	Not studied (D)
M8 'Irritating P-ASAS bands' decrease the confidence in ASAS, and enhance the effect of nuisance alerts.	Not studied (D)
M9 P-ASAS bands and alerts caused by small vertical speeds in turns can be regarded as 'nuisance'.	Not studied (D)
M10 P-ASAS bands and alerts caused by small vertical speeds in turbulence can be regarded as 'nuisance'.	Not studied (D)
M11 ACAS/ASAS inconsistencies decrease confidence in ASAS, enhancing the probability that pilots overrule ASAS solutions or ACAS advisories.	Not studied (OS): ASSUMP-2-OTH
M12 ACAS/ASAS inconsistencies: ACAS TAs occurring while no ASAS conflict is detected.	Not studied (OS): ASSUMP-2-OTH
M13 ACAS/ASAS dependencies may cause that in case of one failure a conflict is not detected by either of them (depending on final implementation).	Not studied (OS): ASSUMP-2-OTH
M14 Presented ASAS solution may bring pilot to overrule ACAS advisory (TA/RA) (depending on final implementation).	Not studied (OS): ASSUMP-2-OTH
M15 Suppression of ASAS solutions in case of ACAS advisory (TA/RA) may lead to sudden loss of situational awareness of pilots (depending on final implementation).	Not studied (OS): ASSUMP-2-OTH
M16 In case of an erroneous but long lasting ACAS advisory (TA/RA), suppression of ASAS Conflict Detection and Resolution may lead to the situation where both separation assurance and conflict avoidance are corrupted.	Not studied (OS): ASSUMP-2-OTH
M17 If ACAS and ASAS are fed by one power bus, a failure could lead to a loss of both	Not studied (OS): ASSUMP-2-OTH

iFly: D7.1b (Table 3)	iFly: D9.2
M18 Decreased confidence in ASAS caused by TCAS alerts 'out of the blue' in case of navigation failures.	Not studied (OS): ASSUMP-2-OTH
M19 Creative pilots managing to create their own priority. This can lead to situations in which aircraft follow unexpected routes or go all into one direction.	Not studied (OS): ASSUMP-4-OTH
M20 Pilots misusing the priority status by choosing crowded parts of airspace, or by bothering a different aircraft.	Not studied (OS): ASSUMP-4-OTH
M21 Crew self inflicting a failure (e.g., pulling circuit breaker) to be allowed to switch on the priority switch.	Not studied (OS): ASSUMP-4-OTH
M22 In an emergency procedure, switching on the priority switch may be done late or it may be forgotten, especially in case of serious emergencies such as a rapid de-compression	Not studied (DC)
M23 In an emergency procedure, aircraft may have to descend quickly and not have time to look out for other traffic.	Not studied (OS)
M24 The crew may also switch on the priority switch while it should not, because of mixing up emergency procedures.	Not studied (DC)
M25 If the crew thinks to have switched on the priority switch, while they still have not, they expect other aircraft to solve the conflict, while the other aircraft do not even see the conflict yet.	Not studied (DC)
M26 Traffic overtaking from behind, especially when having priority, causing a conflict while they can still not be seen on the CDTI.	Not studied (D)
M27 CDTI set up such that a conflicting aircraft cannot be seen on the CDTI.	Not studied (D)
M28 Some aircraft symbols may not be seen well in sunlight, e.g., dark grey symbols.	Not studied (D)
M29 A workload that is too low.	Not studied (D)
M30 Suddenly having to switch from a very low workload to a high workload may cause ?	Not studied (D)
M31 Switching ASAS off (accidentally, or on purpose e.g. to see if it helps to get it working again later on).	Not studied (D)
M32 Switching ASAS in the wrong mode.	Not studied (D)

iFly: D7.1b (Table 3)	iFly: D9.2
M33 Typing in a wrong separation distance (mistyping, confusing separation distance for another airspace).	Not studied (D)
M34 Typing in a wrong look-ahead time (mistyping, confusing separation distance for another airspace).	Not studied (D)
M35 Forgetting to switch on ASAS when entering FFAS.	Not studied (OS): ASSUMP-2-EC
M36 Switching ASAS in the wrong mode when entering FFAS.	Not studied (OS): ASSUMP-2-EC
M37 Switching ASAS on and off to reset the system or to recover from a failure. Crew may be interrupted by something else and continue with ASAS switched off.	Not studied (D)
M38 Fuel problems may be caused by descending into MAS.	Not studied (OS): ASSUMP-5-OTH
M39 Circumventing poor weather and Special Use Airspaces causes more fuel usage.	Not studied (OS): ASSUMP-5-OTH
M40 R/T position reports (after e.g. ADS-B transmission failure) can be unclear, be misunderstood or be imprecise.	BC-2, BC-16, BC-1-EQP, BC-4-EQP
M41 Position reports can be given on the wrong R/T frequency, e.g. ATI instead of the one for the airspace users.	BC-1-EQP
M42 Multiple aircraft flying around in FFAS having a failure.	
M43 Crew not being informed about failures of other aircraft when entering FFAS.	Not studied (OS): ASSUMP-2-EC
M44 Crews deciding not to leave FFAS when a failure occurs.	Not studied (OS): ASSUMP-2-EC
M45 Flight control related errors occur, possibly in combination with transponder problems. Especially smoke or rapid decompression.	Not studied (OS): ASSUMP-5-OTH
M46 A crew not realising to have to solve a conflict after an own ADS-B transmitter failure, because they think to have priority since priority is indicated on the CDTI.	BC-1-EQP, BC-8
M47 A crew switching priority after an own ADS-B transmitter failure (mistakenly thinking that this might help), and then assuming that they can take right of way.	Not studied (DC)
M48 Lack of a buffer area between FFAS and Special Use Airspace.	Not studied (OS): ASSUMP-2-EC

iFly: D7.1b (Table 3)	iFly: D9.2
M49 Autopilot turning over ('over steer').	BC-3b
M50 Conflicts popping up when already being in a next phase. For instance, when turning into a conflict, the conflict may already be very nearby.	BC-7a
M51 Bands closing in from both sides, such that you cannot turn left or right.	Not studied (DC)
M52 Bands closing in from all sides, such that you cannot turn left nor right, and neither climb nor descend.	Not studied (DC)
M53 Taking too much time to give a 'distress' call, because of unfamiliarity with the emergency procedure or the system.	Not studied (D)
M54 Within a conflict, the aircraft without priority switches on the priority button. By delays (priority update) or reduced vigilance, conflict resolution is not taken care of.	Not studied (DC)
M55 Crews always giving way and solving and preventing conflicts may cause the aircraft to use much fuel.	Not studied (D)
M56 Crews always giving way and solving and preventing conflicts may cause an unstable traffic pattern.	Not studied (D)
M57 Crews turning through an amber band.	Not studied (DC)
M58 The pilot forgets to tell the controller of MAS about a failure when leaving FFAS.	Not studied (OS): ASSUMP-2-EC
M59 The pilot forgets to tell the controller of FFAS about a failure when entering FFAS.	Not studied (OS): ASSUMP-2-
M60 Ambiguously written emergency procedures, leading to incorrect or late crew actions.	Not studied (D)
M61 Difficult emergency procedures, leading to incorrect or late crew actions.	Not studied (OS)
M62 Pilots having a poor awareness of free flight logic (various examples; none particularly relevant).	Not studied (D)
M63 A navigation map shift.	Not studied (D)
M64 Priority determination based on FLOS leads to ambiguities at North and South Pole.	Not studied (D)

iFly: D7.1b (Table 3)	iFly: D9.2
M65 The relevance of an emergency message is missed as callsigns are not indicated on CDTI, and the actually nearby aircraft is assumed to be far away.	Not studied (D)
M66 Cluttered display by inappropriate range setting.	Not studied (D)
M67 Two or more aircraft with priority switched on in same airspace.	BC-8
M68 Disagreement between crew members on how to solve conflict.	BC-13
M69 Misinterpreting or disregarding ASAS horizontal conflict solution manoeuvre by heading/track confusion.	(Not studied (D)
M70 Pilots distrust ASAS information, wonder whether ASAS works fine, and, in order to check it, make some manoeuvres with the purpose to generate a potential conflict.	Not studied (OS): ASSUMP-4-OTH
M71 ANP value is calculated conservatively. Common cause for all aircraft.	Not studied (D)
M72 Failure to engage NAV after flying heading	Not studied (D)
M73 GPS jamming by radio pirates	Not studied (OS): ASSUMP-4-OTH
M74 Interference of ADS-B by radio pirates	Not studied (OS): ASSUMP-4-OTH
M75 Interference of ADS-B is getting worse	BC-16
M76 No crew	Not studied (D)
M77 Routing across military airspace	Not studied (D)
M78 TCAS interference by radio pirates	Not studied (OS): ASSUMP-4-OTH, ASSUMP-2-OTH
M79 Volume of alerts is turned down on headset/speakers	Not studied (D)
M80 Volume of R/T is turned down on headset/speakers	Not studied (D)

Appendix 5: Emergency and Non-Normal Procedures

Let us summarize definitions and main features of Emergency & Non-normal procedures as stated in iFly:D1.3, A^3 ConOps .

Definitions

Emergency *operations if there is degradation in any, several or all.*

- Insufficient information exchange
  - SWIM network performance degradation
  - Air-Air or Air-Ground data link performance degradation
  - Broadcast capabilities lost in one or more aircraft
- On-board equipment performance degradation
  - MEL – a minimum equipment list; a lists of the instruments and equipment that may be inoperative without jeopardizing the safety or capabilities of the aircraft, includes procedures for flight crews to follow when securing or deactivating inoperative instruments or equipment).
- Flight crew performance degradation
- Aircraft performance degradation
- Hazard of such magnitude, that it is not possible to maintain the required safety level in the operations.

in own (or various others) aircraft that does not allow for the continuation of operations under the A^3 ConOps, while retaining the accepted safety levels.

Non-normal *operations if there is degradation in any, several or all*

- On-board equipment performance
- Flight crew performance
- SWIM network performance
- Aircraft performance

in own (or various other) aircraft, but the remaining performance of the overall system is such that self separation operations under the A^3 ConOps can be maintained, while the safety requirements are also kept. Those operations that require a modification of normal operations.

Note: The process of detecting and resolving conflicts is part of the normal operations performed by a self separating aircraft; the appearance of a conflict does not indicate a non-normal or emergency situation.

Examples:

- Emergency
  - Emergency – aircraft is in an emergency condition
- Non-normal
  - Non-own surveillance capable – a/c is unable to broadcast its state and/or intent, its position only detected through primary radar

- Non-self separation capable - Aircraft can perform all its normal tasks, except self separation.

General considerations for Non-normal and Emergency operations

- Concerning overall self separation capabilities:
  - Aircraft that are aware of the fact that they are no longer capable to self-separate will be required to enter Managed Airspace as soon as they are able.
  - Other aircraft will have to perform all separation requirements regarding that particular aircraft when it still is inside SSA.
  - Non-normal aircraft may be required to transmit their operational performance level, which is an indication of their self separating capabilities.
- Concerning medium term conflict management:
  - When an aircraft is in a non-normal or emergency situation the crew or automation will update the condition level of the aircraft.
  - The condition in which the aircraft operates will affect the priority level that will be broadcast.
  - Aircraft in a non-normal or emergency situation will broadcast a higher priority level.
- Concerning short term conflict management:
  - cooperative resolution manoeuvres in State Based CR will ensure that the conflict will be resolved even if the participating Non-normal aircraft is unable to manoeuvre.

    (See SR-N-4.1)
- Concerning surveillance capabilities:
  - Loss of Air-Air DL will have to be indicated to the SWIM network by any means possible.
  - Ground applications will continue to track the aircraft through position reports and/or radar returns.
  - Other aircraft will continue to receive surveillance updates for this aircraft through the SWIM network as long as the aircraft is in SSA.
  - When an aircraft trajectory information is not available through any of the normal means, SWIM might provide dynamic RAA around a non-self separating aircraft. Affected traffic will avoid that RAA as an area conflict.
    - That RAA area will move at the aircraft's speed but, will not provide trajectory information. Airborne systems should be able to infer the area's course and speed by interpolation of current and past positions, but this information would be inaccurate and incomplete.The relatively low update rate of SWIM may further complicate the situation.
- Concerning Separation minima:
  - The SM classification used for the emergency aircraft will take into account its condition (deviations from declared trajectory, surveillance capabilities degradation, a/c not providing any surveillance information thus available only less accurate from SWIM).

Communication in Emergency and Non-normal operations

The level of surveillance information can range from full communications/surveillance capabilities to just some very basic state information.

- Voice communication frequency - will be enabled in particular sector and used mainly for emergency operations and as backup for time-critical communications.
- Data link communication (if available) - will be used in the case of a contingency/emergency situation.
    - Aircraft emergency frequency (International Air Distress (121.5 MHz) for civil aircraft, Military Air Distress (243.0 MHz) for military aircraft).
    - Adjusting the SSR transponder to reply on Mode 3/A Code 7700.
    - A R/T frequency band will be devoted to flight crew contingency and emergency communications.
- SWIM (if available) - will also play a major role during Non-normal and Emergency operations. The aircraft emergency status plus priority status message will be made known to all actors through SWIM.
    - Switching from airborne surveillance to ground-based surveillance.

Stakeholders

- Own aircraft – emergency or non-normal procedures, follow guidelines.
- Nearby traffic – Separation responsibility from aircraft which have declared an emergency will fall upon nearby traffic.
- FOC – evaluate contingency or emergency, able to assess and adjust accordingly in near real-time.
- ANSP - The emergency aircraft will in collaboration with the governing ANSP be able to choose a preferred route into Managed Airspace. In order to prioritize the entrance of the emergency aircraft into MA, the governing ANSP may have to issue a new set of CTAs to all other aircraft. CTA changes to other aircraft, as a result of an emergency, will not be subjected to negotiation between the other aircraft and the ANSPs.
- ATC **NOT** considered - The procedures (which will involve ATC) concerning the transition of an emergency aircraft from SSA to MA are not considered.

Tasks to be done (identified in iFly: D1.3)

- Correctly define the procedures (covering normal procedures in SSA and contingency & emergency events);
- Develop reliable systems including safety and warning tools;
- Develop emergency and recovery procedures for Emergency and Non-Normal events;

Appendix 6: Hazard Classification Matrix

There has been defined Operational safety assessment hazard classification matrix in ED-78A/DO-264.

Table A6-1 shows this hazard classification matrix together with three rows devoted to hazard classes with respect to the SSEP – effect on aircraft separation and effect on airborne self-separation ability.

Hazard class – severity class	1 (most severe)	2	3	4	5 (least severe)
Safety targets - RSC per flight hour	1E- 08	1.00E-05	1.00E-04	1.00E-02	N/A
Effect on operations	Normally with hull loss. Total loss of flight control, mid-air collisions, flight into terrain or high speed surface movement collision	Large reduction in safety margins or aircraft functional capabilities	Significant reduction in safety margins or aircraft functional capabilities	Slight reduction in safety margins or aircraft functional capabilities	No effect on opeartional capabilities or safety
Effect on occupants	Multiple fatalities	Serious or fatal injury to a small number of passengers or cabin crew	Physical distress, possibly including injuries	Physical discomfort	Inconvenience
Effect on FC	Fatalities or incapacitation	Physical distress or excessive workload impairs ability to perform tasks.	Physical discomfort, possibly including injuries or significant increase in workload	Slight increase in workload	No effect on flight crew
Effects on air traffic services	Total loss of separation	Large reduction in separation or total loss of air traffic control for a significant period of time	Significant reduction in separation or significant reduction in air traffic control capability	Slight reduction in separation or slight reduction in air traffic control capability. Significant increase in airtraffic controlled workload	Slight increase in air traffic controller workload
Effect on aircraft separation – minimal RTTL	**Mid-air collision**: ACAS initialization, RTTL (open)<PLOS, **RA indicated**; SSEP failure	**Large reduction in separation**: implicit coordination required, RTTL(close)<STT In this case, possibly an abrupt maneuver is required to avoid a mid-term collision	**Reduction in separation**: conflict solution driven by priority rules; Signifficant increase in FC workload	**Reduction in separation:** conflict solution driven by priority rules; Slight increase in FC workload	No effect on operation capabilities or safety; no conflict exists within MTTH
Effect on airborne self-separation ability	Aircraft is **unable to self-separate**. Complete failure of ASAS and own a/c is **unable to broadcast**.	Aircraft is **unable to self-separate**. Complete failure of ASAS but own a/c is **able to broadcast**.	Slight **reduction in self-separation ability**. Flight crew work load significantly increase due to machine insufficiency. Own a/c is **unable to broadcast**.	**Slight reduction in self-separation ability**. Flight crew work load significantly increase due to machine insufficiency. Own a/c is **able to broadcast**.	Aircraft able to **fully self separate**, e.g. provide airborne self separation. Own a/c **is broadcasting** its state and intent.

* 2 aircraft conflict considered, not multiple aircraft

Appendix 7: Links with WP2: Human Responsibilities in Autonomous Aircraft Operations

The role of human factors is crucial within the self-separation concept, due to the fact that the responsibility for separation lies entirely on flight crew, who is supported by supporting tools. Considering human factors aspects, OSA benefits from the results **of iFly WP2** namely from the second research part "Bottlenecks and potential solutions" presented in deliverables iFly:D2.3 and iFly:D2.4. Active human participation and situation monitoring ("Human in the loop") may prevent the operational hazard from birth (role of internal mitigation means) or may help to cushion the effect of operational hazard (external mitigation mean, detection mean).

The main findings of iFly: D2.4 used during OSA development are:

- The proposed level of automation (iFly: D2.4, chapter 5.3), which was a key input into process of BCs, IMMs and EMMs identification. As at the current stage of SSEP procedure development the actions taken by the flight crew have not been defined in detail, only recommendations regarding the level of automation for an example of SSEP procedure implementation has been developed in iFly D2.4. Table A7-1 categorizes the Flight Crew actions considered in D2.4 into internal or external mitigation means. Note, that only the abilities and possibilities of FC of own aircraft have been investigated in fault and event trees and formulated as internal or external mitigation means.
- Identification of problems concerning Human-Automation Interaction described in section 4 of iFly:D2.4 which have been taken into account mainly during IMM formulation process. The mapping of automation related problems and IMMs might be found in Table A7-2.

Table A7-1: Proposed role of flight crew, based on iFly: D2.4, chapter 5.3 (Determining level of automation).

OODA categories* and tasks, which fall under**	**Tasks (handled by the SSEP operation) associated with OODA categories**	**SSEP Functional Blocks***	**Proposed level of automation (iFly: D2.4, p. 34)** for an example SSEP implementation described in (iFly: D1.3, p.67)**	**Proposed FC role in risk mitigation process of "Human in the loop" based on automation level****
OBSERVE – gathering, monitoring and filtering data	Collecting and maintaining surveillance information	Surveillance	Automation level 5 or 4 respectively (OBSERVE category)	External mitigation mean/Detection mean
ORIENT – deriving a list of options through analysis, trend prediction, interpretation and integration	Detection of conflicts, detection of other hazard, checking for opportunities of own flight optimization	Surveillance		External mitigation mean/Detection mean
DECIDE – decision-making based on ranking available options	Conflict processing , assessment, situation prioritization and choice of suitable CR process	Situation assessment	Automation level 4 up 6	External mitigation mean/Detection mean
	Conflict resolution process	Tactical maneuver & Trajectory Modification	Automation level 6 or 7 (Action automation does not exceed level 3). Sheridan's level of Automation for decision 3 or 4	Internal and External mitigation mean/Detection mean
ACT – execution or the authority to act on the chosen decision	Initiation of conflict solution execution and immediate broadcasting of approved solution (possibly sending RBT to SWIM) & Flying of a/c along the trajectory	Tactical maneuver & Trajectory Modification & Navigation*	Automation level 1-3	Internal mitigation mean

* The Functional block *Navigation* excluded from OSED version of this table, due to the fact, that the functionalities covered by *Navigation* are not SSEP specific. **In OSA, the ACT OODA category was enriched with Navigation FB.**

** For NASAs' Level of Autonomy Assessment Scale see iFly: D 2.4, p. 35, for Sheridan's levels of Automation for decision and action selection see iFly: D 2.4, p. 29. Tables 5 and 3.

*** Boyds' (1996) "Observe, Orient, Decide, and Act" loop.

**** The role of human in risk mitigation process is proposed based on D2.4, p. 34. There is stated that levels 1-2 (OODA) indicate that human is primary and computer is secondary actor; levels 3-5 computer operates with human interaction; levels 6-8 computer operates independently of the human, human has decreasing access to information.

Table A7-2: List of Automation-related problems (iFly: D2.4, chapter 4) and relevant OSA requirements, which shall help to overcome these problems.

iFly: D2.4 (chapter 4.1)	iFly: D 9.2
Out-of-the-loop unfamiliarity	IMM-11 (in particular IMM-11b,e)
Clumsy automation (e.g. FC is overconfident in automation, FC workload reduced in periods with low workload but overloaded in high workload phases)	 e.g. IMM-11f IMM-11c (some problems are out of operational scope and should be discussed mainly in SSEP design stage)
Automation induced errors	IMM-12a,b
Behavioral adaptation (FC reduces its effort, more responsibility to automation)	IMM-11j
Complacency, automation bias, commission errors and omission errors (misuse of automation-uncritical reliance, insufficient monitoring of ASAS functions)	IMM-9d, IMM-11def IMM-11f, IMM-11b+IMM-6e IMM-11b, IMM-9d+IMM-11a IMM-9e
Distinction between data availability and observability	IMM-11b,d,e
Inadequate training and skill loss	IMM-9

Appendix 8: Abbreviations

ACAS	Airborne Collision Avoidance System
ADS-B	Automatic Dependant Surveillance - Broadcast
AFR	Autonomous Flight Rules
ASAS	Airborne Separation Assistance Systems
ASOR	Allocation of Safety Objectives and Requirements
ASSUMP	Assumption
CD	Conflict Detection
CPP	Conflict Processing Performance
CR	Conflict Resolution
CRP	Conflict Resolution Performance
CTA	Controlled Time of Arrival
DM	Detection Mean
EC	Environmental Condition
ED	Execution Delay
EMM	External Mitigation Mean
FB	Functional Block
FC	Flight Crew
IMM	Internal Mitigation Means
LP	Logic Performance
MA	Managed Airspace
MFF	Mediterranean Free Flight
MLAT	Mid term Look Ahead Time
MTT	Mid term Time Threshold
MTTH	Mid Term Time Horizon
OE	Operational Effect
OH	Operational Hazard
OHA	Operational Hazard Assessment
OSA	Operational Safety Assessment
OSED	Operational Services and Environment Description
OPA	Operational Performance Analysis
PLOS	Predicted Loss Of Separation
RAA	Restricted Airspace Areas
RBT	Reference Business Trajectory
RNP	Required Navigation Performance

RMC	Required Maneuvers Conducted
RT	Reference Time
RTTL	Remaining Time To Loss of separation
SC	Severity Class
SL	Service Level
SLAT	Short term Look Ahead Time
SP	Surveillance Performance
SR	Safety Requirement
SR-N	Safety Requirement New
SSA	Self Separation Airspace
SSEP	Airborne Self-Separation Procedure
STT	Short term Time Threshold
SWIM	System Wide Information Management
TMA	Terminal Manoeuvring Area
TBD	To Be Defined

Appendix 9: List of References

IFly documents

1. iFly deliverable D1.3: Autonomous Aircraft Advanced (A^3) ConOps, January 2010
2. Cásek P., Keinrath C. (2008): Airborne system for Self Separation in a Trajectory-Based Airspace. EUROCONTROL Inovative ATM Research Workshop and Exhibition 2008, p. 25-31, http://inoworkshop.eurocontrol.fr
3. iFly deliverable D2.3: Description of bottlenecks identified in A^3 ConOps, version 1.3, April 2009
4. iFly deliverable D2.4: Potential human factors improvement for A^3 ConOps, version 1.3, January 2010
5. iFly deliverable D7.1b: Hazard identification and Initial Hazard Analysis of A3 ConOps based operation, draft 0.8, 11th September 2009
6. iFly deliverable D9.1: Operational Services and Environment Description (OSED) of Airborne Self-Separation Procedure (SSEP) – version 1.1, date of deliverable 24th August 2009
7. iFly deliverable D9.3: Operational Performance Assessment (OPA) of Airborne Self-Separation Procedure (SSEP)

OSA methodology and application documents

8. EUROCAE ED-78A/RTCA DO-264: Guidelines for approval of the provision and use of air traffic services supported by data communications, December 2000
9. RTCA DO-312: Safety, performance and Interoperability Requirements Document for In-Trail Procedure in Oceanic Airspace (ATSA-ITP) Application, June 2008
10. RTCA DO-242A: Minimum Aviation System Performance Standards For Automatic Dependent Surveillance Broadcast (ADS-B), June 2002
11. RTCA DO-319: Safety, performance and interoperability requirements document for enhanced traffic situation awareness during flight operations (ATSA-AIRB), March 2010
12. RTCA DO-303: Safety, Performance and Interoperability Requirements Document for the ADS-B Non-Radar-Airspace (NRA).
13. RTCA SC-214/EUROCAE WG-78: Air Traffic Services Safety and Interoperability Requirements
14. FAA DTFAWA-09-A-00001: Operational Safety Assessment (OSA) for the Enhanced Traffic Situational Awareness on the Airport Surface with Indications and Alerts (SURF IA) application.

Other documents:

15. MFF 2004: Hazards identified during the Amsterdam February 2004 MFF experiments
16. DO-260A: Minimum Operational Performance Standards for 1090MHz Extended Squitter. Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services – Broadcast (TIS-B), RTCA 2003