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 D7.1a
Accident risk and flight efficiency of A^3 operation
-Scoping and safety target-

Version: 1.1

by

Henk Blom (NLR)

Start date of project: 22 May 2007 Duration: 51 months

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:	Accident risk and flight efficiency of A^3 operations - Scoping and Safety Target -
Authors of document:	Henk Blom
Deliverable number:	D7.1a
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
0.1	18-02-2008	All	First draft
0.2	22-02-2008	All	Second draft
0.3	07-04-2008	All	Internal review comments
0.4	16-04-2008	All	Consistent lay-out
1.0	26-09-2008	Minor details only	Internal and external review comments
1.1	03-02-2009	1, 5 and 6	Change in iFly

Version 1.1		Organisation	Signature/Date
Authors	Henk Blom	NLR	
Internal reviewers	Margriet Klompstra	NLR	
	Mariken Everdij	NLR	
	Jelmer Scholte	NLR	
	Pascal Lezaud	DSNA	
External reviewers	Uwe Voelckers	Braunschweig U.	
	Katarzina Gryc	EC-DGTREN	

Abstract

This report describes the scoping and safety target of the A^3 ConOps accident risk and flight efficiency assessment to be performed within iFly project WP7.

Table of Contents

1 Introduction

1.1 iFly project

iFly will perform two operational concept design cycles and an assessment cycle comprising human factors, safety, efficiency, capacity and economic analyses. The general work structure is illustrated in Figure 1. During the first design cycle, state of the art Research, Technology and Development (RTD) aeronautics results will be used to define a “baseline” operational concept. For the assessment cycle and second design cycle, innovative methods for the design of safety critical systems will be used to refine the operational concept with the goal of managing a three to six times increase in current air traffic levels. These innovative methods find their roots in robotics, financial mathematics and telecommunications.

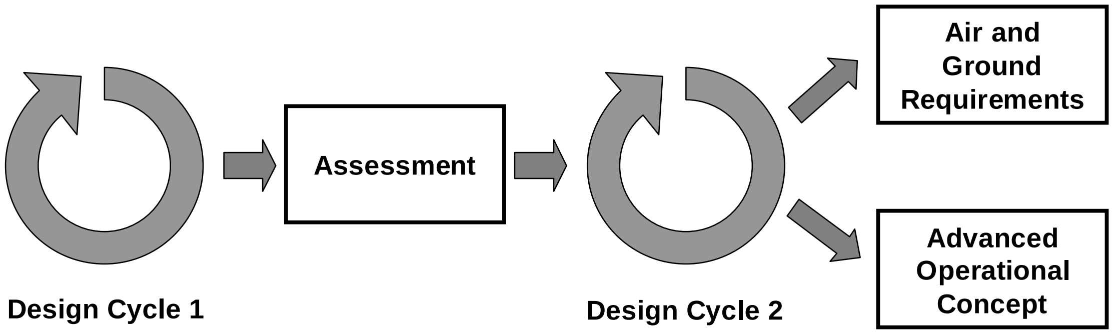

Figure 1. iFly Work Structure.

As depicted in Figure 2, iFly work is organised through nine technical Work Packages (WPs), each of which belongs to one of the four types of developments mentioned above:

<u>Design cycle 1</u>
The aim is to develop an Autonomous Aircraft Advanced (A^3) en-route operational concept which is initially based on the current “state-of-the-art” in aeronautics research. The A^3 ConOps is developed within WP1. An important starting and reference point for this A^3 ConOps development is formed by the human responsibility analysis in WP2.

<u>Innovative methods</u>
Develop innovative architecture free methods towards key issues that have to be addressed by an advanced operational concept:

- Develop a method to model and predict complexity of air traffic (WP3).
- Model and evaluate the problem of maintaining multi-agent Situation Awareness (SA) and avoiding cognitive dissonance (WP4).
- Develop conflict resolution algorithms for which it is formally possible to garantee their performance (WP5).

<u>Assessment cycle</u>
Assess the state-of-the-art in Autonomous Aircraft Advanced (A^3) en-route operations concept design development with respect to human factors, safety and economy, and identify which limitations have to be mitigated in order to accommodate a three to six times increase in air traffic demand:

- Assess the A^3 operation on economy, with emphasis on the impact on organisational and institutional issues (WP6).
- Assess the A^3 operation on safety as a function of traffic density increase over current and mean density level (WP7)

Desing cycle 2
The aim is to refine the A^3 ConOps of design cycle 1 and to develop a vision how A^3 equipped aircraft can be integrated within SESAR concept thinking (WP8). WP9 develops preliminary safety and performance requirements on the applicable functional elements of the A^3 ConOps, with focus on identifying the required technology.

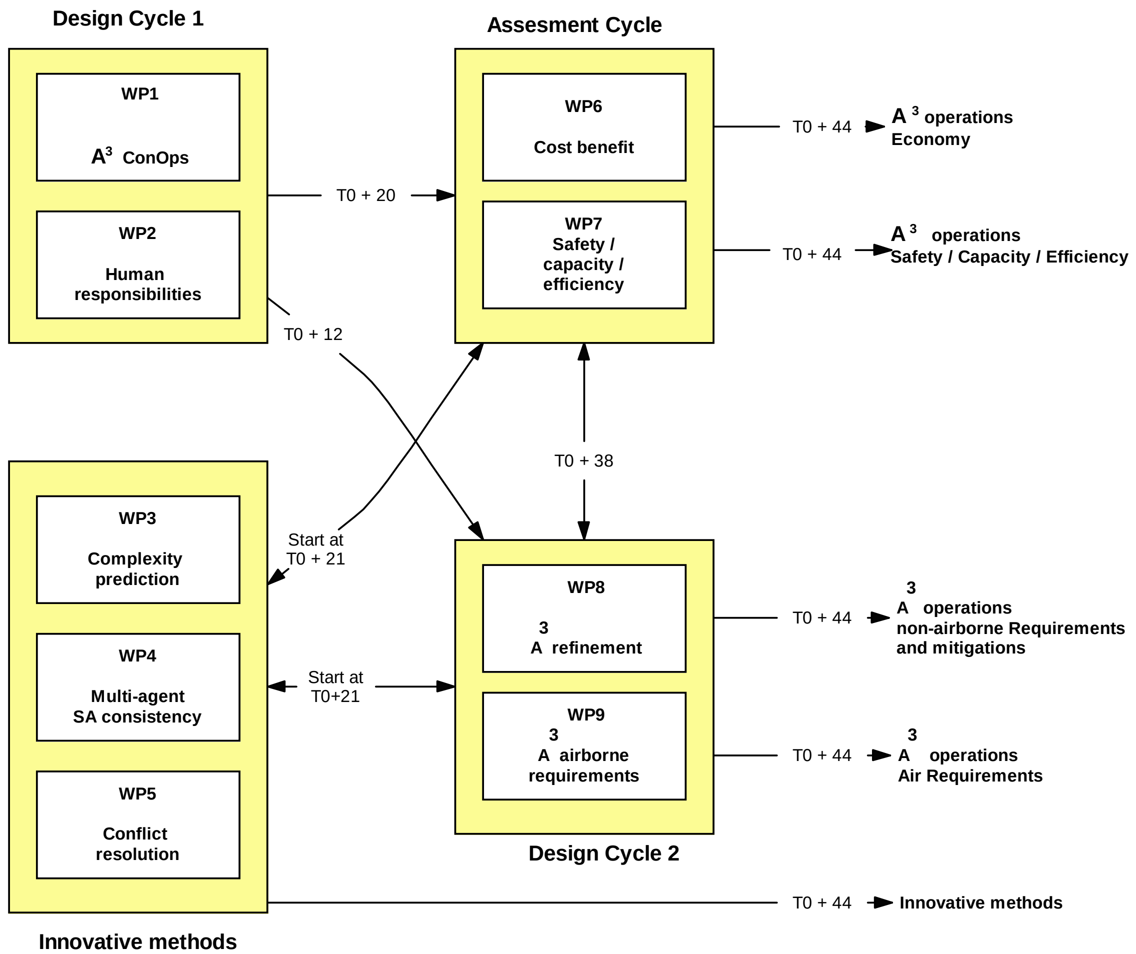

Figure 2: Organisation of iFly research

1.2 Safety assessment feedback to design

In providing safety risk assessment feedback to ATM design, there is one issue that always should get the attention it deserves: safety communication. The value of a safety assessment is largest when there is a sound feedback communication to operational concept design. Without such a feedback a safety assessment becomes a yes/no assessment. With feedback communication, safety assessment is a way for the designers to learn where their design should be improved in order to become sufficiently safe. Within iFly, the main aim of the safety assessment is to learn something about the initial A^3 ConOps operations from the first design cycle, which supports refinement of the A^3 ConOps during the second design cycle. This interaction between design and assessment is depicted in Figure 3.

Figure 3: Safety assessment feedback based ATM design

This feedback loop can take place at a more organizational level, in order that hazard and safety assessment information can be of use to the strategic decision makers regarding operational concept development. This may be of particular relevance when for example an assessment for a project uncovers new hazards that may apply to other projects or even existing operations. Designers and developers of new concepts also can benefit from feedback; though they are not necessarily habitual readers of safety assessments. Hence if such information could be presented in a usable way to designers/developers, then they would be considering safety aspects from a very early stage in their concept formulation processes. Safety assessors themselves can also benefit from structured feedback, since then assessors working on new operation assessments can see what hazards etc. were identified, with what risk levels, and with what mitigations. Assessors need not be constrained by prior assessments, but should be able to view them. Therefore a 'library' of safety assessments can be useful in this respect. Safety assessment practice is therefore a potential source of organizational learning for the industry, which could enhance safety management efficiency and effectiveness. This step has yet to be properly developed for ATM, but is a logical addition to the ATM safety management approach.

The golden rules of feedback-based ATM design are therefore:

- Safety should be a main issue in all stages of the design and implementation lifecycle of a new ATM operation, i.e. from the first stage onwards;
- The results of the safety assessment should be communicated back to the operational concept designers after or during each major lifecycle stage.

The aimed result is that safety is effectively being built into the design of an advanced ATM operation. However, when this feedback is missing in the earlier stages of the design, the result typically is that at a late moment in time, when an operational concept will be designed up to a high level of detail, one suddenly realises that sufficient safety may be compromised. All one can do at that point is either start from the beginning, or do damage control, i.e. try to "repair safety" by adding all kinds of costly features or safety nets that are not even guaranteed to work. The lack of effective safety feedback therefore represents a "break in the chain process" and can be reasonably identified as a gap or inefficiency in the development of an advanced ATM operation.

1.3 iFly WP7 objective and E-OCVM

The objective of iFly WP7 is to explore the safety boundaries of airborne self separation in en-route air-space. Thereto a safety risk assessment will be performed within WP7, of the Autonomous Aircraft Advanced (A^3) en-route operation with respect to safety as a function of a factor three to six traffic increase over current mean traffic demand. This will be compared against ICAO and ESARR accident risk criteria that apply under corresponding higher traffic levels. The difference between this curve and the ICAO/ESARR criteria will give a good indication of how much and in which directions a "state-of-the-art" A^3 operation has to be further improved in order to accommodate a factor three to six en-route traffic increase over Europe. In order to realize effective feedback to the advanced operation design, the safety assessment should answer the following questions "How safe is the air traffic operation design?", and "Which operational factors contribute most to risk", and "How much can risk be influenced by increasing reliability of technical systems".
This feedback may be used along two ways:

- Further improvement of the A^3 ConOps on any of its weak points;
- Development of a vision on how to integrate A^3 equipped aircraft within SESAR concept thinking.

In the initial iFly validation strategy [iFly D10.1i], it has been identified that WP7 fits the European Operational Concept Validation Methodology (E-OCVM) Phase V1 (Scope). In line with this, WP7 aims to evaluate the proposed A^3 concept regarding its capability in safely accommodating which traffic demand levels, and to gain the necessary insight into its potential costs and benefits. In order to enable these evaluations, the A^3 concept should be described in sufficient detail to enable identification of the potential benefits mechanism (i.e. the change to systems and/or operations that will enable a known barrier to be alleviated). Some aspects of the concept will be unknown or unclear at this stage. There may exist a number of options to be assessed during the further validation process.

Following [E-OCVM, 2007], the validation process starts in V1 (scope) of the concept life cycle. From this phase on, the E-OCVM structured planning framework (see table below) facilitates programme planning in a predictable way.

Step	Activity	Description
Step 0 "State Concept and Assumptions"	0.1	Understand the problem
	0.2	Understand the proposed solution(s)
Step 1 "Set Validation Strategy"	1.1	Identify the stakeholders, their needs, issues, and involvement in the validation
	1.2	Identify the level of maturity to ensure that expectations are realistic
	1.3	Describe the expected outcome of the validation process
	1.4	Identify high level performance objectives
	1.5	Establish initial validation needs, potential scope and draft plan
	1.6	Select validation tools or techniques
	1.7	Define validation strategy and plan
Step 2 "Determine the	2.1	Identify stakeholder acceptance criteria and performance

Experimental Needs"		requirements
	2.2	Identify low level validation objectives
	2.3	Refine validation strategy
	2.4	Identify indicators and metrics
	2.5	Specify scenarios
	2.6	Produce experimental plan
	2.7	Produce analysis plan
	2.8	Produce detailed experimental design
	2.9	Identify assessment requirements
	2.10	Prepare the platform or facility
	2.11	Conduct pre-exercise testing
Step 3 "Conduct the Experiment"	3.1	Conduct validation experiment
	3.2	Assess for unexpected effects or behaviors
Step 4 "Determine the Results"	4.1	Perform analysis specified in the analysis plan
	4.2	Prepare analysis contributions
	4.3	Prepare validation report
Step 5 "Information for Dissemination"	5.1	Disseminate information to stakeholders and decision makers
	5.2	Draw conclusions and decide on actions feedback to validation strategy.

Regarding step 0, the A^3 ConOps description will be received from WP1. The problem to be addressed within WP7 has been described in subsection 1.2. The remainder of this document addresses activity 1.1 through activity 1.7 of step 1 (Set validation strategy).

1.4 Organisation of this report

This report is organized as follows. Section 2 identifies the relevant stakeholders, the expected outcome and the level of maturity expected (steps 1.1, 1.2 and 1.3). Section 3 identifies the high level safety objectives and the expected outcome of the safety validation cycle to be conducted within WP7 (step 1.4). Section 4 identifies the scope of the safety validation cycle to be conducted within WP7 (step 1.5). Section 5 selects validation methods to be used (step 1.6). Section 6 defines the safety validation plan to be conducted within WP7 (step 1.7). Section 7 draws conclusions.

2 Relevant stakeholders

The validation of an operational concept is closely linked to the actors or stakeholders involved. The obvious question then is: who are these stakeholders? This section gives an overview. Subsection 2.1 identifies the stakeholders, Subsection 2.2 presents the different global objectives of these groups of stakeholders, Subsection 2.3 explains the working relations between stakeholders. Subsection 2.4 identifies the expected outcome and level of maturity aimed for by the safety assessment of the A^3 ConOps, and for which stakeholders.

2.1 Who are the stakeholders?

There are several studies that have addressed the question in the title, e.g. [GENOVA WP5-I], [VAPORETO WP5], [ARIBA WP6-I], [ARIBA WP6-II], [ECORYS, 2005], [SAFMAC, 2006]. The stakeholders identified in these studies can be divided into the following groups, see Figure 4:

- Airspace users
- Human society
- Regulatory and supervisory authorities
- Policy makers
- Air Navigation Service Providers
- Other Service Providers
- Airports
- Manufacturers
- Human operators
- Associations and Federations
- Other actors

In Annex A, each stakeholder group is elaborated regarding concrete examples of stakeholders. Note that a few stakeholders (e.g. ICAO) may fall under two or more groups; for others, the choice of group may argued (e.g. is AIS (Aeronautical Information Services) an ‘air navigation service provider or an ‘other provider’?)’, and it may also be argued if governments are stakeholders or organisations beyond the stakeholders. However, the division below provides a rather good picture.

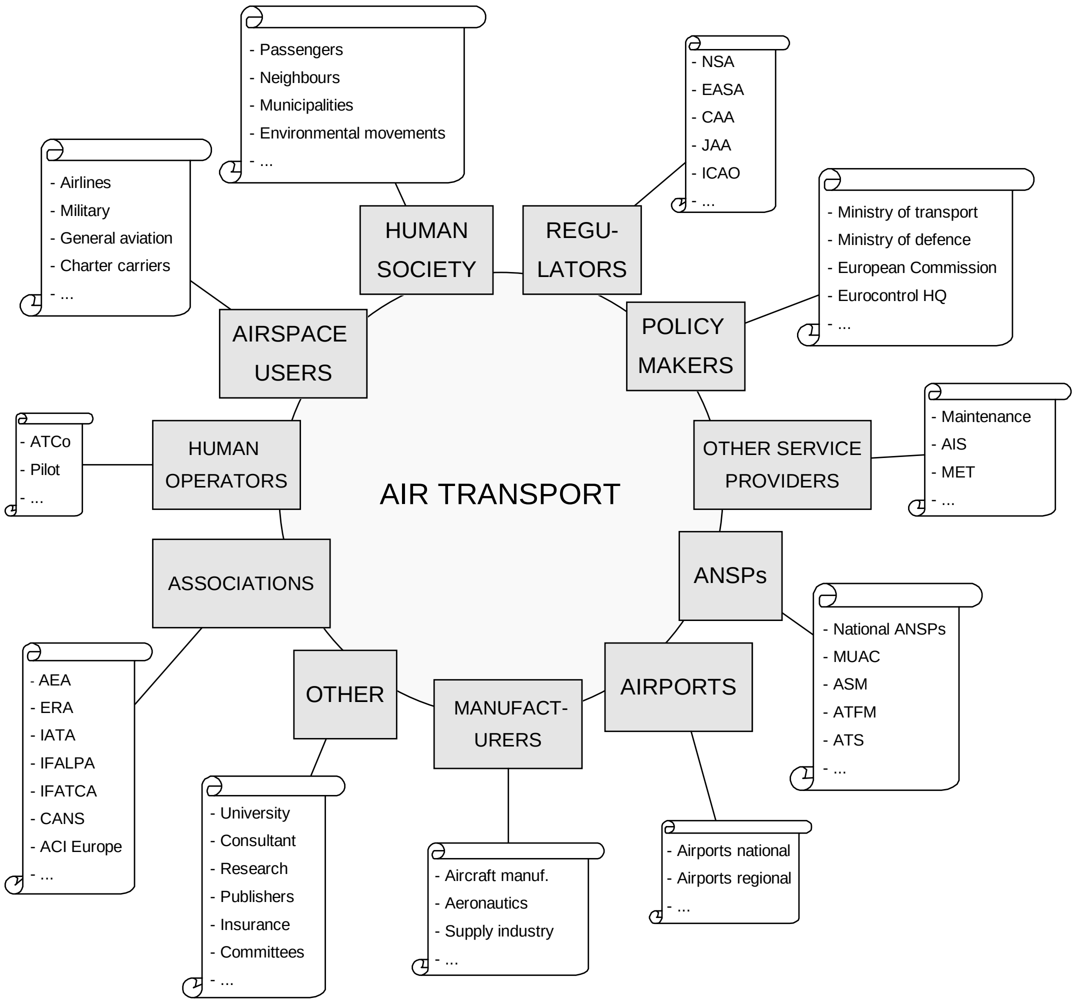

Figure 4: Overview of stakeholders in air transport operations

2.2 Global objectives of different stakeholder groups

The air transport operations overall validation strategies should take into account the different views of the various stakeholder groups which are directly or indirectly involved in air transport operations. In this way potential conflicts between objectives of different stakeholder groups will become clear in an early stage of the life-cycle. Once such a potential conflict has been identified, it even may appear technically possible to change the concept or architecture of a design in such a way that the different objectives become synergetic. Large changes, however, often are cost-effective only when they are introduced during an early air transport operations life-cycle phase.

To get a global idea about the different objectives of the various actor groups, a brief impression for each of the actor groups is given:

- Air traffic controllers and pilots: During their work they carry the full responsibility for a safe and expeditious handling of multiple aircraft. In return for carrying such huge responsibilities, they deserve a human centred approach rather than a technology driven approach during the design phase. This implies that human capabilities (e.g. knowledge, skills, strategies) and limitations should be the dominant factor in the evolution and validation of human role and automation strategy.

- ANSPs view: By its very nature air transport operations has an architecture which is distributed over multiple aircraft, multiple air transport operations centres/sectors and multiple CNS systems. This has a huge impact on the complexity of concept development, procurement and operation of a new air transport operations system, both on systems level and on human level. Without using a proper business-directed overall validation strategy it will be very difficult to organise this complex life-cycle efficiently.
- Industry view: The common situation is that industry participates in the execution of all validation and verification steps of engineering type. Since different future air transport operations concepts and architectures may require different functionalities and sub-systems from the airborne-side and ground-side, the corresponding manufacturers should also play active roles during the conceptual stage, in order to rapidly identify the best directions to be taken for their own developments. There are, however, significant differences for airborne-side and ground-side manufacturers. In contrast with the market for commercial aircraft, the market for air transport operations systems is so small that the product development often is tailored to the customer and the production counts in small numbers. The latter situation complicates both the inter-operability of air transport operations sub-systems from different manufacturers, and the re-use of previous validation results obtained elsewhere.
- Airlines view: Since airlines sell travel tickets, they try to satisfy the evolving wishes of their passengers. For example, a recent survey among British Airways passengers shows that both reliability and safety appear in the top three of passenger wishes on short haul and long haul flights [Lowe, 1995]. These wishes can only be satisfied in collaboration with the industry and the air transport operations service providers. When airlines buy aircraft they are treated as a customer. Obviously, they would like to receive a similar treatment when they are customers of air transport operations services, the more since the airlines form the core of air transport business. This simply means that they should actively participate in the validation during all life-cycle stages of future air transport operations.
- Airport view: Due to growing environmental restrictions, in the future available runway capacity should become the bottleneck rather than air transport operations system capacity. This requires an effective interaction between air transport operations service provision and airport traffic and passenger management, and means that airport service providers should actively participate in the validation during all life-cycle stages of future air transport operations.
- Regulatory authorities view: For the airborne side a widely accepted air-worthiness validation process and certification procedure exists. Such an air-worthiness validation process can be applied either for a pre-operational airborne system, or for an improved version of an airborne system for which “air-worthiness” temporarily has been withdrawn during operational life. In contrast with this, air transport operations have always evolved without certification procedures. For the ANS part, during the last decade a “ground-worthiness” validation and certification process requirement has been implemented [EU-CR, 2005].
- Human society: Humans are directly or indirectly impacted by air transport operations. Directly, either as a passenger or as a person living nearby an airport (noise, emission, third party risk). Indirectly, as part of human society who stays informed through the news agencies about safety and environmental impact of flying. Human society's influence largely works through political bodies, both direct (democratic elections) and indirect

(lobbying groups). This also raises the need for a better understanding of human society's air transport safety perception.

In order to handle these quite differing objectives of the various actors in an efficient way they should be taken into account as early as possible during the life-cycle of future air transport operations and also in the overall validation process.

2.3 Relations between stakeholders

Figure 4 below gives an overview of stakeholders (rectangles) and their relations (arrows). The left-hand-side of the figure gives the situation at stat
e level; the right-hand-side gives the international situation. The arrows marked with coloured circles represent formal responsibilities.

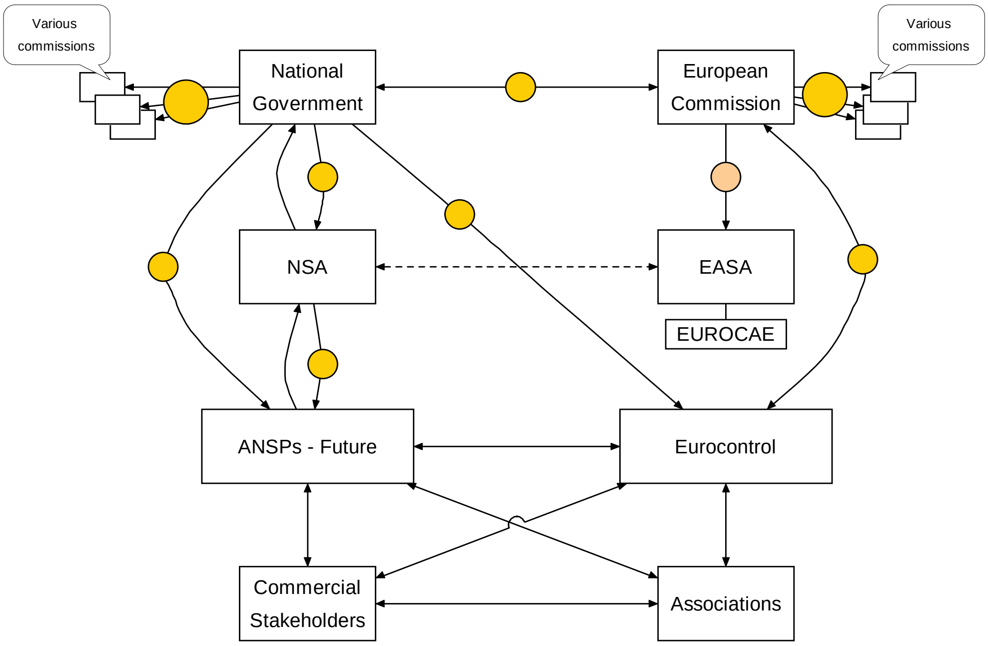

Figure 4: Relations between stakeholders. Formal responsibilities are indicated by a coloured circle

2.4 Expected WP7 outcome and level of maturity aimed for

The A^3 ConOps operation that is being defined by iFly WP1 is aimed to be a hypothetical concept rather than a realistic one. In line with this, the target audience consists of designers of advanced ATM to whom there currently exists a large uncertainty regarding the potential traffic demand that can safely be accommodated by a well developed airborne self separation concept of operation. For this reason, iFly validation activities have all been placed within E-OCVM phase V1. This means that the main stakeholders to be addressed by iFly are Airspace users, Policy-makers, ANSPs and Human operators who have an active involvement within SESAR/NEXTGEN developments.

The main objective of the safety assessment documented in this report is to provide optimal feedback to the operational developers about the safety of the developed A^3 ConOps operation. This means that the safety assessment aims to describe to which extent the developed operation is tolerably safe, to describe on which areas the developed operation should improve with respect to safety, and to explain why this is so. With the feedback from this safety assessment, it can be decided whether the developed operation needs further improvement with respect to safety, and if so, why and on which aspects the operation needs to be improved.

It is not an objective of the safety assessment to provide a detailed and completed safety case for review by regulatory authorities. The level of maturity of the developed operation is considered to be too low for reaching that purpose.

3 High level safety objectives

For the iFly project there are several relevant and valuable input sources of safety needs available. First of all there are the SESAR established safety needs; these are reviewed in Subsection 3.1. Because safety plays such a key role in the feasibility assessment of airborne self separation, we exploited several more specific sources in order to better understand the safety needs of future ATM. Subsection 3.2 reviews ATM relevant accident statistics. Subsection 3.3 presents the ICAO en-route TLS for mid-air collision risk. Subsection 3.4 addresses ESARR4 and EC common requirements relative to ICAO's TLS. Subsection 3.5 reviews SESAR safety observations regarding separation provision and collision avoidance.

3.1 SESAR established safety needs

In [SESAR D2, 2006], the SESAR safety performance objective builds on the ATM2000+ Strategy objective: "To improve safety levels by ensuring that the numbers of ATM induced accidents and serious or risk bearing incidents (includes those with direct and indirect ATM contribution) do not increase and, where possible, decrease". Considering the anticipated increase in the European annual traffic volume, the implication of the initial safety performance objective is that the overall safety level would gradually have to improve, so as to reach an improvement factor of 3 in order to meet the safety objective in 2020 (based on the assumption that safety needs to improve with the square of traffic volume increase). In the longer term (design life of the concept) safety levels would need to be able to increase by a factor 10 to meet a possible threefold increase in traffic.

In order to make SESAR's the high level safety objective concrete, the high level safety objective is based on past accident statistics and ICAO TLS values for en-route airspace. operations including the three involved domains ATS, aircraft systems, and aircraft operations. The regulations for the individual domains are of importance for the eventual implementation of A-SMGCS operations:

- ESARRs and Common Requirements for the ATS domain;
- FAA/ JAA/ EASA requirements for the aircraft systems domain; and
- JAR-OPS/FAR-OPS requirements for the aircraft operations domain.

3.2 Accident statistics

Following [ICAO, Annex 13, 2001], an **accident** is defined as: "an occurrence associated with the operation of an aircraft, which takes place between the time any person boards the aircraft with the intention of flight until such time as all such persons have disembarked, in which:

a) a person is fatally or seriously injured as a result of being in the aircraft, or of direct contact with any part of the aircraft, including parts which have become detached from the aircraft, or of direct exposure to jet blast (except when the injuries are from natural causes, self-inflicted, or inflicted by other persons, or when the injuries are to stowaways hiding outside the areas normally available to the passenger and crew); or
b) the aircraft sustains damage or structural failure which adversely affects the structural strength, performance or flight characteristics of the aircraft, and would normally require major repair or replacement of the affected component (except for engine failure or damage, when the damage is limited to the engine, its cowlings or accessories; or for damage limited to propellers, wing tips, antennas, tires, brakes, fairings, small dents or puncture holes in the aircraft skin); or

c) the aircraft is missing or is completely inaccessible."

In order to avoid ambiguity, [ICAO, Annex 13, 2001] also gives definitions of fatality and fatal accident. A **fatality** is defined as the death of a person resulting from injuries within thirty days of the date of the accident. A **fatal accident** is an accident with at least one fatality among the persons mentioned under a) above. Note that the ICAO definition counts one collision between two aircraft as two accidents. Also note that the ICAO definition largely excludes 3rd party damage, injuries and fatalities.

[Blom et al., 2003] have shown results of a statistical analysis of accidents, fatal accidents and fatalities by Large Aeroplanes (certified takeoff weight is 5670 kg or more) in commercial aviation (but excluding flights with Russian-built and business jet aircraft) over the period 1980 through 1999, and with emphasis on separation-related accidents, i.e.

- Accident involved two or more commercial aviation aircraft, or
- Accident involved one aircraft and one or more ground vehicles, or
- Accident induced by the wake vortex of another aircraft, or
- Accident induced by a near-miss escape manoeuvre.

Over this 20-year period, the total number of accidents in the sample considered amounts 2340, of which 613 are fatal accidents with a total of 15,554 fatalities, while the estimated number of applicable flights amounts 420 million. This statistical data is shown in Table 1.

Table 1 Accident statistics of Large Aeroplane flights in commercial aviation

	Accidents	Fatal Accidents	Fatalities
1980-1999 period	2340	613	15,554
Average per year	117	30.7	777.7
Average per flight	**5.57 E-6**	**1.46 E-6**	**37.0 E-6**
Separation related	185 (7.9%)	23 (3.75%)	783 (5.0%)

The separation related share of accidents is 185 (7.9%), of fatal accidents it is 23 (3.75%) and of fatalities it is 783 (5.0%). Roughly, this means about one separation related fatal accident per year. Further characteristics of the separation related accidents are shown in Tables 2 and 3. It should be noticed that a collision between an aircraft in the sample and an aircraft not in the sample (e.g. a general aviation aircraft or a business jet) has been counted as one accident. Hence, the number of mid-air collisions cannot be obtained by dividing the number of mid-air accidents in the tables by two. Table 2 shows that 79% of the separation related fatalities are due to mid-air collisions, although these constitute 22% only of all separation related accidents. The remaining 21% separation related fatalities are constituted by 78% of the separation-related accidents at the airport, and in particular between two aircraft.

Table 2 Separation related accident statistics of Large Aeroplanes in commercial aviation

	Accidents	Fatal accidents	Fatalities
1980-1999	185	23 (12.4%)	783
Per year	9.25	1.15	39.15
Per flight	**44.0 E-8**	**5.5 E-8**	**1.86 E-6**
Airborne	9.5 E-8 (22%)	3.35 E-8 (61%)	1.47 E-6 (79%)
Non-airborne	34.5 E-8 (78%)	2.15 E-8 (39%)	0.39E-6 (21%)

Figure 5. The distribution of separation-related accidents (light), fatal accidents (grey) and fatalities (black) over various accident types.

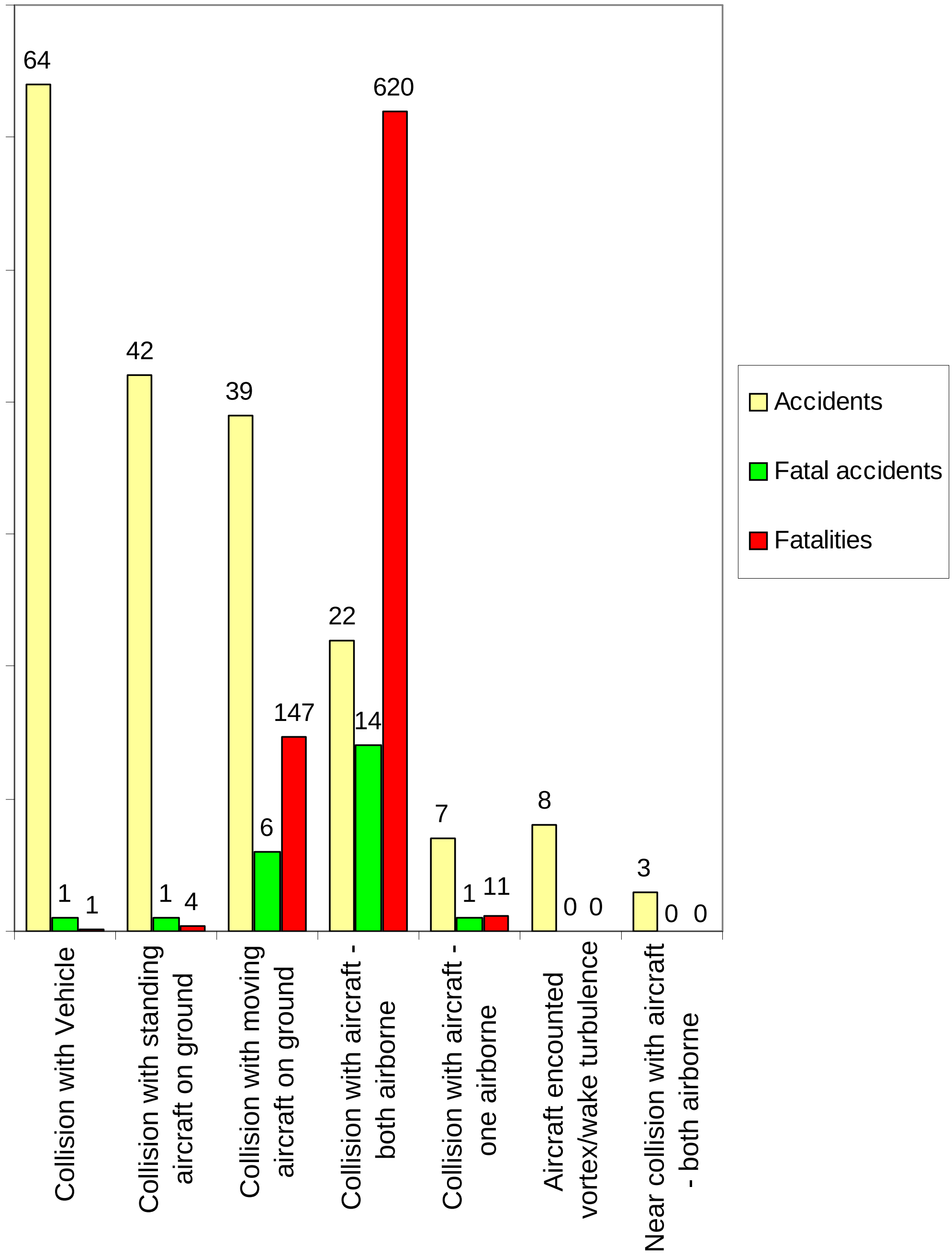

Figure 5 shows that 11 out of 185 accidents, i.e. 6%, are not constituted by a collision but by last moment manoeuvring to avoid a collision or by hitting the wake vortex turbulence from another aircraft. Moreover, these non-collision accidents did not cause any fatality. Statistical data has also shown that the number of separation related accidents per flight seems to be rather constant over different areas in the world (with a positive exception for the Australia/Pacific area), and rather stable over the years. However, one should be aware that the sample sizes often are too small to draw firm conclusions regarding this year and place invariance.

Finally, Table 3 shows the average number of fatalities per accident due to the various collision types in Table 2. This clearly shows that there are large differences in the consequences per type of collision. The average number of fatalities per accident varies from 0.016 for an accident due to collision with vehicle, to 28.2 for an accident due to a mid-air collision. Hence, if consequences are measured in number of fatalities then an accident due to a mid-air collision is a factor 1760 (= 28.2 /0.016) more severe than an accident due to a collision with a vehicle.

Table 3. Average number of fatalities per accident for various collision types

Type of collision determining the accident	Average # fatalities
Collision with aircraft – both airborne	28.2
Collision with moving aircraft on ground	3.8
Collision with aircraft – one airborne	1.57
Collision with standing aircraft on ground	0.095
Collision with vehicle	0.016

3.3 ICAO TLS for en-route fatal accidents

[ICAO Annex 11, 2003], Attachment B states in section 3.2.1: “Where ‘fatal accidents per flight hour’ is considered to be an appropriate metric, a target level of safety (TLS) of 5×10^{-9} fatal accidents per flight hour per dimension should be applied for determining the acceptability of future en-route systems that will be implemented after the year 2000.” It is quite important to notice that this TLS should apply when Airborne Collision Avoidance System (ACAS) is not taken into account. Apart of this ACAS aspect, the rationale used behind the argumentation in developing this TLS value is well developed, and this en-route TLS has regularly been adapted to traffic growth by ICAO’s Review of General Concept of Separation Panel (RGCSP) [Parker, 1996; DNV, 2005]. For example, prior to 2000, the TLS was a factor four higher, i.e. 2×10^{-8} fatal accidents per flight hour and per dimension, which equals 6×10^{-8} fatal accidents per flight hour. Based on accident statistics over 1980-1999, the estimated mid-air fatal accident risk is 3.35×10^{-8} fatal mid-air accidents per flight [Hybridge D2.2, 2003]. If we assume one flight takes about 2 hours, this comes down to about 1.7×10^{-8} fatal mid-air accidents per flight hour, which is about a factor 3.5 lower than the TLS value posed by ICAO during that period.

Part of the explanation of this factor 3.5 is that the ICAO en-route mid-air collision safety target setting does not take airborne based safety nets into account. This may lead to the undesired situation that the ICAO en-route mid-air collision TLS provides no incentive to improve airborne based safety nets, and to improve the collaboration between ground-based and airborne-based safety nets. For advanced developments of Airborne Separation Assistance System (ASAS) and further development of ACAS there is an obvious need to take this into account when defining future TLS values for mid-air collision. In [RESET D6.1, 2007] it has been argued that this needs to be changed in order to give airborne self separation a far chance.

Taking into account a traffic growth factor X since 2000, whereas the frequency of fatal accident headlines in the news may not increase, then the TLS should be reduced by this same factor X. This means that iFly should adopt a TLS of $3\times5\times10^{-9}/X$ fatal accidents per flight hour, and this should apply without taking ACAS into account. Moreover, ACAS should at least yield a factor 3.5 extra reduction in fatal accident risk.

3.4 ESARR4 and EC common requirements

[RESET D6.1, 2007] has reviewed ATM related safety requirements by ESARR, EC and SRC and compared this with ICAO safety requirements. Based on these evaluations the following conclusions have been drawn.

First of all it has become clear that SRC maintains consistence between ESARR and EC requirements.

Secondly, important differences between ICAO and ESARR/EC/SRC safety targets have become clear:

- ICAO and ESARR/EC/SRC differ in scope of their safety targets settings. ESARR4 considers safety targets for safety issues having an ATM direct contribution only, whereas ICAO does not adopt such limitation.

- ICAO and ESARR/EC/SRC differ in scope of their required safety assessments. ESARR4 requires that hazards combined effects have to be identified and assessed for ATM-related credible hazards only, whereas ICAO does not adopt such limitation. An additional limitation of ESARR4 is that combined effects of ATM-related credible hazard(s) and any other hazard are not required to be covered by the safety assessment.

- ESARR4/EC/SRC required safety assessment refers to maximum probabilities of occurrence and effect. As has been explained well by [Brooker, 2005] this leads to an overestimation of safety risks in advanced operations, and thus to placing an undesired extra hurdle in getting advanced operations accepted. ICAO does not require this.

- Currently, neither ICAO nor ESARR4/EC/SRC safety targets take any contribution of ACAS or ASAS to the reduction of safety risk into account. This means there currently is no mid-air collision risk reduction incentive regarding the improvement of airborne based systems and neither regarding improving the collaboration between airborne based systems and ground-based systems. For advanced developments of Airborne Separation Assistance System (ASAS) and further development of ACAS there seems to be a clear need to better balance the incentives.

The aim of iFly development and safety validation is to properly address the joint requirements posed by ESARR, ICAO and the potential introduction and improvement of airborne based systems and pilot roles.

3.5 SESAR safety observations on separation provision and collision avoidance

In [SESAR safety, 2007] an initial assessment of SESAR Concept of Operations has been conducted, which resulted into the following recommendations regarding separation provision:

- A regulatory approach should be established to manage the simultaneous application of different modes of separation taking in particular into account the impact on:
    - Safety rulemaking and oversight

  - o SMS (e.g. reporting schemes)
- A safety regulatory approach in line with clear responsibilities, rules and procedures should be established to manage the impact on related licensing schemes for pilots and ATCOs.

These recommendations are based on the following generic impact statements that relate to a high level understanding of the concept:

- The boundaries of responsibilities change with this function. Change of competences for pilots and controllers
- There is a significant impact from the introduction of ASAS in managed and controlled airspace
- Can the ANSP still be made responsible for separation assurance? Can they still own the risk for separation assurance?
- There is a requirement to enable monitoring functions (warning tools) that are in scope with the changes in the separation responsibilities
- Are the potential changes to the Safety Management approach similar to the current SMS requirements to “external services”?
- There is a significant impact from the introduction of ASAS in unmanaged airspace.
- Responsibility for separation assurance lies with the user. Can this conflict with State responsibility for airspace design

Regarding collision avoidance, [SESAR safety, 2007] comes to the following recommendations:

- There is a requirement for the establishment of a clear regulation on the role of safety nets (i.e. role of airborne safety nets and ground-based safety nets)
- This policy also needs to address
  - o the owner of the risk
  - o the owner of the safety case
  - o liability for risks in interrelated environments (e.g., human automation issues)
- There is a requirement to assign to an empowered safety regulatory authority responsibility for developing and implementing an overall regulation addressing collision avoidance
- There is a requirement for early clarification to support the development and validation processes: either to be taken up by SRC or EASA or another arrangement
- Other airborne and ground-based safety nets (e.g. APW, GPWS, runway incursion prevention, etc.) should also be addressed by the safety net regulation
- A new accident model should be developed that represents the SESAR operational concept (related to re-definition of ATM scope, functions and boundaries)
- Appropriate safety assessment and monitoring methods should be developed to deal with the SESAR operational concept
- Safety R&D programmes should be aligned in accordance with SESAR scope change level understanding of the concept:
- The proposed Target Concept of Operations did not explore all sorts of features to assure collision avoidance
- Safety nets appear to be a core part of the future operational target concept, with a different level of reliance compared to the current situation
- The proposed target concept of operations implies equipage requirements for all aircraft with the appropriate set of functions (the notion appears to be that all aircraft should

always be visible to ATM and each other), in addition there appears to be an inconsistency in this context with respect to managed and unmanaged airspace

- There is a requirement for a safety regulator that is enabled and competent to have an overall view on the system
- Safety nets at airports seem to be considered as part of safe capacity planning (stop bars concept)
- It appears that the current way in which quantified safety assessment is done is no longer appropriate for future collision risks: e.g. airborne influences, interdependencies: apportionment concept may no longer be in line with the new concept
- Safety assessment methodologies need to be further developed in order to meet the scope and potential safety issues of SESAR
    - o interoperability: interdependencies are changing
    - o aviation-wide methodologies are needed
- Different safety research programmes need to be better aligned to meet the SESAR objectives.

The SESAR Target Concept of Operations takes a clear position with respect to the liability principles involved with self separation:
"*It should also be noted that, even in the case of self-separation, the traditional liability principles which are currently ruling the distribution of legal liabilities remain appropriate. Consequently, the safety of such procedures does not depend on the definition of clear liability rules, but on whether the safety case demonstrates that the human factors issues have been correctly addressed and automation tools, rules and procedures are of sufficient reliability and accuracy, to support an air navigation context in which the pilot can be entrusted with additional separation tasks.*"
In order to effectively support this statement a number of issues on the safety regulatory side need to be resolved [SESAR safety, 2007].

The central question in this rationale is: where is the legal basis for the safety case? Currently only ANSPs are required to address the safety performance of separation provision through ESARR or EU equivalent regulations. If in practice the airspace user will take responsibility for separation provision in the airspace where ESARRs or EU equivalent regulations are applicable, will the airspace user then de facto become an Air Navigation Service Provider? If the answer to this question is yes, then the logical consequence would be that ESARRs and EU equivalent regulations would be applicable to those airspace users who take responsibility for self-separation. Another emerging issue in this scenario would then be how to address those airspace users that are not directly bound to ESARR or SES regulations (e.g. North American airlines)? It appears that the only feasible solution to this scenario would be a global approach through ICAO. But, even if ICAO would be able to deliver standards that would ensure safe operations, the question would remain of how the individual States would ensure continuous safety oversight of those airspace users that are outside their influence.
If however the airspace users in this concept assume that the responsibility for safety remains with the ANSPs, then the situation may be different.
Assuming that the current arrangement, which places the safety responsibility with the ANSP, remains unchanged then the situation arises where the concept implies that ANSPs delegate separation responsibility to an airspace user, but not accountability. However, it may be possible to delegate responsibilities but not accountability or liability (e.g. issue similar to the delegation of ATS in cross border arrangements), de facto the main accountability and liability in this concept remains with the State that has delegated the responsibility for the separation provision task to the ANSP.

In this scenario, the State now has to find a way to ensure that the delegation of the separation responsibility by the ANSP to the airspace user is done in such a way that the level of safety of the current arrangement is not reduced. In order to enable this scenario, States will have to make a choice: are the State going to ensure safety at the airspace user side with all the issues raised before, or are they going to ask the ANSPs to ensure that in the safety arguments provided by the ANSP, the delegation of the separation responsibility is covered appropriately and in a way which is acceptable to the State. If the latter solution is a valid option, then the question would be: how are the ANSPs going to ensure that what all the airspace users are doing is safe and how are they going to make this transparent and acceptable to the regulatory authority that is responsible for ensuring the State's responsibility to the general public for safety? This question is likely to be even more complicated where privatised ANSPs are involved.

An additional consideration is required with respect to the involvement of Unmanned Aerial Vehicles (UAVs) or Unmanned Aerial Systems (UASs). In the current approach the terms segregated and non-segregated airspace are used to assess the impact of UAVs/UASs on the ATM system. The safety regulatory framework will have to find a solution for this emerging market, probably through rulemaking, certification and oversight. However, the first impression is that issues that are identified for the delegation of separation responsibility to an airspace user may emerge even more strongly in this discussion. The basis for this hypothesis is that the ANSP will not accept responsibility for separation assurance when UAVs/UASs are involved.

4 Scope of safety assessment

In this section the scope of the assessment is specified. The scope is expressed below in **bold** statements; after each statement an explanation and/ or rationale is given.

A. The scope of the safety assessment does not cover the full path towards a completed safety case, but is restricted to one safety risk assessment cycle.
One safety risk assessment cycle is in scope, in which it is assessed up to which traffic demands, A^3 ConOps based operation is sufficiently safe. The safety assessment does thus not aim to cover the full path towards a completed safety case; in this stage of development the purpose is to provide optimal feedback to the operational developers about the safety of the developed operation as a function of traffic demand.

B. The scope is restricted to safety assessment of the A^3 ConOps operation as developed within WP1
The scope is furthermore restricted to the safety assessment of the A^3 ConOps operation as developed within WP1. Operational developments that take place during the safety assessment and thus after consolidation of this description are not taken into account, as it is impossible to assess the safety of an operation that changes in the meanwhile.

C. The scope includes technical equipment, procedures, humans, and all interactions.
The assessment considers the safety of A^3 ConOps operation consisting of the following three elements and their interactions:

- Technical equipment (hardware and software for e.g. labelling, multi-lateration, runway incursion alerting tool);
- Procedures (e.g. R/T protocol, identification, handling unequipped aircraft, runway incursion alerting procedure); and
- Human (e.g. pilots) roles, responsibilities and their organisation.

Furthermore, the interactions with the context of the operation, concerning for example weather situations or traffic demand can have significant influence on the level of safety, and are thus taken into account in the safety assessment.

D. The scope includes existing elements and new elements, and their interactions.
Furthermore, to assess the safety of an operation one cannot restrict the scope to the new elements of an operation only. For instance, when automating a certain service, one should in principle not restrict oneself to assessing the safety of this automation only, but one should assess whether the entire operation supported by the automated system is safe. Main reason for this is that when considering only the new elements of an operation one might overlook interactions between the original and the new elements. For example, automation of services might lead to changes in human roles and responsibilities, and therefore also in new unforeseen hazards.

E. The scope includes pilot roles
In the A^3 ConOps operation, pilots remain the most flexible and creative element to direct the performance of the overall A^3 ConOps operation, including the management of threats, errors and unpredictable events.

A³ ConOps implied changes relative to the current operation will involve a change in the pilot roles which requires an extensive change management process throughout the entire process of system development, design and implementation.
Continuous social dialogue between management and operational staff at a working level should be established as one important means in an advanced change and transition management process to identify and address the social impacts of introduced changes.

F. The operation includes ATS, aircraft operations, and aircraft systems, and their interactions

A³ ConOps operations comprise airborne services and ground services by making distinction between the following domains of safety certification, see e.g. [ED78A, 2000] and [EATMS SAM, 2004]:

- Air traffic services (ATS): Strategic Flow Control;
- Aircraft systems (equipment): aircraft and equipment manufacturers; and
- Aircraft operations: airline operators.

These domains and their interrelations are pictured in Figure 6.

When considering the A³ ConOps operations of iFly a large part of the changes is related to the Aircraft systems domain. However, the introduction of new Aircraft systems tools also has effect on the other two domains. Hence, all three domains are in scope of this document. This is important for safety assessment, as different regulations exist in each of the domains.

It is noted that in this document an A³ ConOps operation is considered to be an Air Traffic Management (ATM) operation. ICAO defines ATM to consist of a ground part and an air part. The ground part of ATM consists of ATS, Air Space Management (ASM) and Air Traffic Flow Management (ATFM).

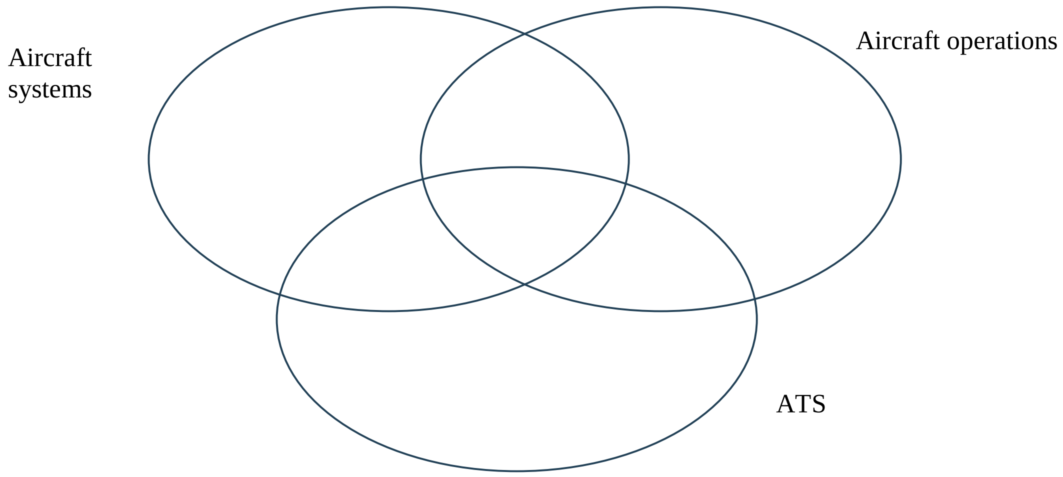

Figure 6: A³ ConOps operations are supported by strategic flow control (within air traffic services), aircraft systems, and aircraft operations. The interrelations between these domains are represented by the places where the ovals overlap.

G. The scope of air traffic and aircraft operations considered is formed by commercial air transport
Only General Air Traffic (GAT) is considered, as GAT encompasses all flights conducted in accordance with the rules and procedures of ICAO. This means that Operational Air Traffic (OAT) is not in scope.

Furthermore, three types of aircraft operations can be distinguished: commercial air transport operations, general aviation, and aerial work. We restrict to commercial air transport, i.e. we do not cover general aviation and neither military aircraft.

H. UAS and UAV are excluded from the scope
In [iFly D2.1] a human factors analysis has shown there are major unsolved issues regarding the incorporation of UAS or UAV in airspace allocated to commercial air transport. Because of this, UAS and UAV are excluded from the scope of WP7.

I. The geographic scope of the assessment is confined to en-route flight levels above 250
The "en-route" phase of flight is defined by the ICAO Common Taxonomy Team as:

> *"Under Instrument Flight Rules (IFR) "en-route" phase includes from completion of Initial Climb through cruise altitude and completion of controlled descent to the Initial Approach Fix (IAF)".*

Following [iFly D1.1], en-route phase of flight is not strictly confined to flight levels above some specific height. Within WP7, however, the assumption is adopted to consider the flight levels that are in use for cruise phase of commercial air transport operations.

J. The scope excludes security issues.
Finally, security issues (e.g., sabotage, terrorism, military actions) are declared out of scope of the safety assessment. Such issues can be assessed via e.g., a security assessment.

K. The scope of safety related occurrences is restricted to mid-air collisions between two or more aircraft
A safety assessment can consider a wide range of safety-related occurrences including different types of occurrences (e.g., Controlled Flight Into Terrain, Loss of Control) and occurrences of different severity (e.g., major incident, fatal accident). Being the most demanding ones, only mid-air collisions between two or more aircraft are considered.

L. The scope does include effects of ACAS/TCAS
Current regulations from the ATM domain prescribe that in a safety assessment following ICAO and ESARR 4, the collision avoidance functionality of TCAS should not be considered. Hence, in collision risk studies ACAS/TCAS typically is declared to be out of scope. In the current study however, we explicitly incorporate ACAS/TCAS in order to gain as soon as is possible the required insight of potential ACAS/TCAS interaction with ASAS.

M. Transition areas from Airborne Self Separation Airspace to Managed airspace fall outside the scope of WP7
Because we only need to develop insight in the hypothetical A^3 ConOps, we do not consider any impact of transition areas between Managed airspace and airborne Self Separation Airspace.

5 Safety validation methods

5.1 Emerging good practices

Recently, [CAATSII, D13i] has performed an evaluation of safety methods that emerged as good practices for Safety Assessment in R&D projects from an analysis of:

- CAATS target projects (R&D projects of the VI Framework Programme)
- CAATS II target projects (R&D projects of the VI Framework Programme and SESAR)
- Other relevant European R&D projects
- Experience of the CAATS Safety Team with other National and International collaborative ATM R&D projects.

Table 4 provides the [CAATSII, D13i] listing of these emerging approaches and their applicability to the E-OCVM proposed maturity levels V1 through V4 of a concept proposed in the E-OCVM.

Table 4: Applicability of emerging approaches to concept maturity levels V1 through V4

Emerging safety Analysis Approaches	**Applicable Concept Maturity Levels**
System Function Analysis	V1, V2, V3, V4
Safety Fundamentals & Safety Screening	V1, V2
Preliminary Hazard Analysis	V2, V3
Functional Hazard Assessment	V3, V4
Preliminary System Safety Assessment	V3, V4
System Safety Assessment	V4
TOPAZ methodology	V1, V2, V3, V4
Note: Only the maturity levels V1 to V4 are relevant for R&D projects and considered in this table	

From Table 4 it can be concluded that the following four safety approaches have been shortlisted by [CAATSII, D13] for application within the V1 phased safety validation of iFly:

- System Functional Analysis
- Safety Fundamentals
- Safety Screening
- TOPAZ methodology

5.2 Coverage of generic types of evaluation by emerging approaches

Table 5 summarises [CAATSII, D13i] ideas about the types of subassessments that are covered by each of the emerging safety analysis approaches presented above. The Table considers the main focus of each emerging approach. Of course, not all these approaches ensure the same level of depth in their investigation. During the initial phases of the concept definition, the safety analysis is done at a very preliminary level, and needs to be further refined, as soon as the concept is more mature.

Table 5: Coverage of Generic Safety Assessment Stages by the Emerging Approaches

Emerging safety Analysis Approaches	Applicable generic types of safety assessment
System Function Analysis	Learning the Nominal Operation
Safety Fundamentals & Safety Screening	Identify Hazards Evaluate Risk Identify Potential Mitigating Measures
Preliminary Hazard Analysis	Identify Hazards Evaluate Risk Identify Potential Mitigating Measures
Functional Hazard Assessment	Identify Hazards Combine Hazards Evaluate Risk
Preliminary System Safety Assessment	Identify Potential Mitigating Measures
System Safety Assessment	Safety Monitoring and Verification
TOPAZ methodology	Learning the Nominal Operation Identify Hazards Combine Hazards Evaluate Risk Identify Potential Mitigating Measures Feedback to Operation, Assessment and Design

Table 5 shows that TOPAZ covers each of the applicable generic safety assessment types that are covered by the others, with the exception of safety monitoring and verification of SSS. The aim of the sequel is to find out whether TOPAZ would suffice, or that there is a need to make use of other methods also. Prior to doing so, we first describe the TOPAZ methodology in subsection 5.3. Subsequently, in subsection 5.4, the TOPAZ methodology is evaluated against the [SAFMAC, 2006] developed safety validation quality indicators (see Annex A).

5.3 TOPAZ accident risk assessment methodology

TOPAZ is an advanced accident risk assessment methodology that supports a scenario and Monte Carlo simulation-based accident risk assessment of an air traffic operation, which addresses all types of safety issues, including organisational, environmental, human-related and other hazards, and any of their combinations. The main aim of TOPAZ is to model accident risks that are related to advances in ATM in order to provide feedback to the designers of the advanced operation regarding the main sources of unsafety as function of traffic and environment characteristics, including quantification. This produces for the advanced concept design unique insight on which safety/capacity aspects of the design can best be addressed to realize the high level objective of improving capacity without sacrificing safety. Part of the TOPAZ methodology is to develop a TOPAZ Monte Carlo simulation tool set for an advanced operation. For a number of advanced operations a dedicated TOPAZ tool set has already been developed.

An overview of the steps in a TOPAZ safety assessment is given in Figure 7. During step 5 use is made of Monte Carlo simulations for selected safety aspects.

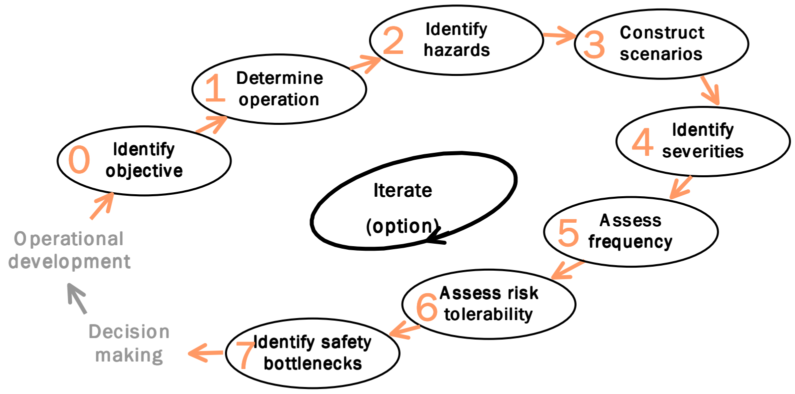

Figure 7. TOPAZ accident risk assessment steps, with Monte Carlo simulation based assessment step 5

In step 0 the objective of the safety assessment cycle is determined, as well as the safety context, the scope and the level of detail of the assessment. The actual safety assessment starts by determining the operation that is assessed (step 1). Next, hazards associated with the operation are identified (step 2), and clustered into conflict scenarios (step 3).). In step 4, the range of potential severity categories of the safety relevant scenarios are identified. In step 5, the occurrence frequency of the identified severity categories is assessed, which is done with support of Monte Carlo simulation modelling and analysis when needed. Using the severity and frequency assessments, the safety risk associated with each safety relevant scenario is classified (step 6). For each safety relevant scenario with a (possibly) unacceptable safety risk, the main sources contributing to the lack of safety (safety bottlenecks) are identified (step 7), which can help operational concept developers to find improvements for the operation. Should such an improvement be made, a new cycle of the safety assessment should be performed to investigate whether all risks have decreased to a negligible or tolerable level.

Whenever, for a particular aspect of the operation under analysis, step 5 is more demanding than what can be assessed on safety using conventional methods (e.g. fault/event trees), then the TOPAZ methodology is to develop and subsequently use a Monte Carlo simulation tool set for the an advanced operation. This TOPAZ supported Monte Carlo simulation approach has significant advantages: 1) the risk estimate quality improves, and 2) it is possible to estimate a 95% uncertainty area. In some applications, a suitable TOPAZ simulation tool may be available. Otherwise one should develop a novel TOPAZ simulation toolset for this, or extend an existing TOPAZ toolset. For a number of advanced operations a dedicated TOPAZ tool set has already been developed and applied to operational concepts that range from runway crossing operations to airborne self separation concept studies, and during maturity stages ranging from V1 (early concept studies) through V6 (true operations). The main aim always is to gain insight in the main risks of an operation and their causes. Once this understood well, operational concept designers typically are able to improve the operational concept design such that these main risks are mitigated significantly.

5.4 TOPAZ versus safety validation quality indicators

In [SAFMAC2, 2007], the TOPAZ accident risk assessment methodology has been evaluated against the SAFMAC developed set of safety validation quality indicators (see annex B). The main findings are that TOPAZ complies well with most of these safety validation quality indicators. For some safety quality indicators, recommendations have been provided to use some additional methods to complement or further improve the TOPAZ approach. In Table 5, these recommendations are specified below for the corresponding safety quality indicators, together with a short explanation of how this recommendation will be taken into account within iFly.

Table 6. [SAFMAC2] recommended TOPAZ improvements and complementary methods, and how these are planned to be taken into account within iFly.

CI#	[SAFMAC2] recommendation	How to take this into account within iFly
01	n.a.	-
02	Incorporate safety screening* as a complementary approach and formulate in line with this guidelines for a standard approach of writing a scoping section.	Apply Safety Screening to the A^3 ConOps and subsequently use this to potentially improve WP7 scope.
03	It is recommended to develop complementary methods that support regulatory authorities such as SRC, EASA and DGTL in breakdown of the safety target up to the level required.	This recommendation applies to TMA and airport.
04	n.a.	-
05	n.a.	-
06	If a deeper level of dependability analysis of technical systems is required then dedicated tools are recommended for complementary use.	This applies to follow up work within WP9. Then the MC simulation results obtained in WP7 are expected to form a powerful source towards getting the technical requirements right from an overall safety perspective.
07	Human performance is often a key determinant of operational safety. In order to validate human performance models, the link with human performance studies and real-time simulations should be built in within projects.	Within iFly WP7 some experience from real time simulations performed within MFF project may be used. Any need for additional human in the loop simulations applies to an iFly follow up project aiming for phase V2.
08	The Human Factors Case [Mellet and Nendick 2007] is recommended to be used as complementary method.	A qualitative human factors assessment will be performed by iFly WP2.3; this is aimed to identify bottlenecks on human responsibility

* Detailed information about the Safety Screening methodology are in the document [SafScreen, 07].

		issues.
09	n.a.	-
10	n.a.	-
11	n.a.	-
12	Further development of organisational and institutional modelling approaches may be valuable. Research addressing a broad view on the organisation of air traffic and its safety implications is currently done in a Eurocontrol CARE Innovative Research project [Stroeve et al. 2007].	If feasible use novel results within iFly WP7.
13	Development of methods to further improve hazard coverage in MC simulation modelling.	Outside WP7 scope.
14	n.a.	-
15	n.a.	-
16	There is room for improvement of the bias and uncertainty assessment along the following two directions: 1) Multi-dimensional regression analysis in combination with Monte Carlo simulations should be explored; and 2) The assessment of uncertainty should be formalized for the evaluation of other model differences than in parameter values.	Number 1) is in development within iFly WP7.2. Number 2) is in development elsewhere. As much as is feasible, both developments will be used within iFly WP7.
17	n.a.	-
18	It is recommended to formulate guidelines for organizing and moderating brainstorms with operational experts to identify mitigating measures.	A brainstorming workshop with experts on hazard mitigation has been scheduled within WP8.5. WP7 will prepare organization and moderation guidelines for this brainstorming.
19	n.a.	-
20	Analyse which elements in a TOPAZ risk assessment require most effort, and invest in those in order to reduce recource requirements.	If feasible, do so within WP7.
21	Develop ways of reporting to describe the Monte Carlo simulation model between the high-level overviews and detailed Petri Net representations. Develop tools that make it easier to extract results of the performance of individual agents (humans, technical systems) in the Monte Carlo simulations, which increase the understanding and trust in the risk assessment results.	If feasible, do so within WP7.
22	n.a.	-
23	n.a.	-
24	n.a.	-
25	n.a.	-
26	n.a.	-
27	Further development of simulation speed-up	To do so within WP7.

	techniques to be able to assess complex air traffic scenarios.	
28	In documentation of Monte Carlo simulation-based risk assessments emphasis often is on presentation of the accident risk results in various conditions. To promote the understanding of the Monte Carlo simulation models, more results should be simulated and documented on the performance of the agents (humans, technical systems) in the simulations.	To do so within WP7 documentation of Monte Carlo simulation studies.
29	n.a.	-
30	To better understand, through an example, the relation between TOPAZ results and SEE (Safety Environment Efficiency) reports, and the role this plays in the decision making process of the Dutch ANSP.	-
31	n.a.	-
32	n.a.	-

In the next section, the proposed ways of how to take the recommendations by [SAFMAC2] into account within WP7 are incorporated in the WP7 safety validation plan.

6 WP7 safety validation plan

WP7 assesses the A^3 operations developed by WP1 and WP2, through hazard identification and Monte Carlo simulation on accident risk as a function of traffic demand, to assess what traffic demand can safely be accommodated by this advanced operational concept, and to assess the efficiency of the flights. The accident risk levels assessed should be in the form of an expected value, a 95% uncertainty area, and a decomposition of the risk level over the main risk contributing sources. The latter verifies which of these sources should have been mitigated during the 2nd design cycle of the A^3 concept. This work is organized in four sub-WPs:

- WP7.1: Monte Carlo simulation model of A^3 operation
- WP7.2: Monte Carlo speed up methods
- WP7.3 Perform Monte Carlo simulations
- WP7.4 Final report

For each of these sub-WP's the work planning and resource allocation is provided below. The work planning forms an improved version of the one in the technical annex of the contract. The improvements are in line with those recommended in the right hand side column of Table 6.

Resource allocation within WP7

Partner	NLR	TWEN	INRIA	HNWL	UCAM	ENAC	Isdefe	PoliMi	UTartu	EEC	Total
WP7.1	10	8		3		0.5	1		0.5	0.5	23.5
WP7.2	7	11	8		6	4		2			38
WP7.3	5	9		2.5					0.5		17
WP7.4	4	1		1.5		0.5	1			0.5	8.5
Total WP7	26	29	8	7	6	5	2	2	1	1	87

WP7.1: Monte Carlo simulation model of A^3 operation

The development of a Monte Carlo simulation model of A^3 operation is accomplished through a sequence of steps. First a scoping has to be performed regarding the desired risk and capacity simulation study. An important aspect of this scoping is to identify the appropriate safety requirements to be derived from ICAO and ESARR4 regulation. Sections 3 and 4 of this report have provided initial drafts of these scoping and safety targets. Upon completion of the A^3 ConOps by WP1, then the Safety Screening approach will be applied, and possible improvements in scoping may be made. Next a hazard identification and initial hazard analysis is performed for the A^3 operation as has been developed by WP1 and WP2. After these preparations the main work can start: the development of a Monte Carlo simulation model that captures the accident risk and the flight efficiency of the A^3 operation. Such a simulation model covers the human and technical agents, their interactions and both the nominal and non-nominal aspects of the operation. Special attention will be given towards describing the Monte Carlo simulation model at some level that sits well in between one of a high-level overviews and one of a detailed Petri Net specification.

Milestones and expected results

T0+6: Start of WP7.1, which runs for a while in parallel with WP1 and WP2. During this period WP7 has the possibility to identify operational concept issues which have not yet been defined well by WP1 & WP2. On these issues design decisions have to be made by WP1 and WP2. For issues where WP1 and WP2 have not decided at T0+10, within WP7.1 a hypothetical assumption is adopted and well documented in order to be taken into account during the bias and uncertainty assessment during WP7.3.

T0+18: Where needed, adopt hypothetical design assumptions and document these well. The specification of the Petri net model may now start.

T0+28: The Petri net model is completed. Hence the development and testing of the simulation code can start, in parallel with the development of the dedicated Monte Carlo speed up approach of WP7.2.

Deliverables:

D7.1.a: Scoping and safety target report (T0+9; Public)

D7.1.b: Hazard identification report (T0+22; Public)

D7.1.c: Report on Petri Net modeling of the A^3 operation (T0+28; NLR internal)

WP7.2: Monte Carlo speed up methods

In order to run this Monte Carlo simulation model up to the level of collision risk, a large factor in Monte Carlo simulation speed up is required. Thereto, WP7 incorporates a further development of the innovative HYBRIDGE speed up approaches in rare event Monte Carlo simulation. As such, we start with a review of the Monte Carlo simulation based accident risk assessment situation. Subsequently, potential candidates are identified that are expected to provide significant room for the development of complementary speed-up and bias and uncertainty assessment techniques. In order to spread the risk as much as is possible, within this task various options for improvement are identified and these are subsequently elaborated and tested within parallel tasks. Several options are already known at the moment of proposal writing, e.g.:

- Develop an effective combination of Interacting Particle System based rare event simulation with Markov Chain Monte Carlo speed up technique
- Develop a method to assess the sensitivity of multiple aircraft encounter geometries to collision risk, and develop importance sampling approaches which take advantage of these sensitivities.
- Develop novel ways how Interacting Particle System speed up techniques that apply to a pair of aircraft can effectively be extended to situations of multiple aircraft.
- Develop an efficient extension of Interacting Particle System based rare event simulation for application to hybrid systems
- Combine Monte Carlo simulation based bias and uncertainty assessment with operation design parameter optimization.

The most promising candidates are explored and subsequently the results are integrated with the innovative speed up approaches developed within HYBRIDGE. This way we prepare a speed up approach for application to the Monte Carlo simulation model of WP7.1.

Milestones and expected results

T0: Start of WP7.2

T0+20: A critical review is performed of the progress made so far within WP7.2, and where necessary a revision of the plan and the priorities will be identified. If the difference between expectations and findings stays too far behind the expected needs of WP7, then the follow up work within WP7.2 will be reformulated. This reformulation then may include a change in internal deliverables.

T0+28: WP7.2 should have developed sufficient speed up methods which in combination provide the Monte Carlo speed up factor needed for effective Monte Carlo simulation within WP7.2.

Deliverables

D7.2.a: Review of air traffic risk assessment situation (T0+6; Public)

D7.2.b: Report on combining Interacting Particle System with Markov Chain Monte Carlo simulation (T0+20, Public)

D7.2.c: Interim Report on importance sampling of multi aircraft encounter geometries (T0+20, Internal)

D7.2.d: Report on IPS extension to multiple aircraft (T0+20, Public)

D7.2.e: Report on interacting particle system extensions to large hybrid systems (T0+20, Public)

D7.2.f: Report on optimization combined with bias and uncertainty assessment (T0+28; Public)

D7.2.g: Final Report on Monte Carlo speed up studies (T0+32; Public)

WP7.3 Perform Monte Carlo simulations

Monte Carlo simulations are performed to assess flight efficiency and collision risk of the A^3 operation, including a bias and uncertainty assessment. Subsequently a final report is produced which shows the assessment results obtained for A^3 operation. In this report it is also shown which safety bottlenecks should have been mitigated by the A^4 ConOps of design cycle 2.

Regarding the factor X in traffic increase, the proposal is to use the en-route traffic data that has been used within the HYBRIDGE project [Hybridge, D9.4, 2005] as reference point, i.e. for this sample, X = 1. This traffic sample has been taken from Europe on a busy day in 1999, from one of the busiest en-route sectors in Europe (e.g. an en-route sector above Frankfurt). This X=1 traffic density is then assumed to apply homogeneously throughout the airspace. The aim is to make graphs of the probability of safety relevant events (mid-air, Near mid-air, Infringement of Minimum Separation, Short term conflict, Medium Term Conflict) as function of the factor X, at least ranging from 1 to 6 (and preferrably from 0 to 10). Similar graphs should be made of cost-effectiveness aspects.

During the Monte Carlo simulation-based risk assessment, and the documentation of the results obtained, special attention will be given to the influence of the performance of the various agents (humans, technical systems) on the simulation results obtained.

Milestones and expected result

T0+28: The Petri net model is completed. Hence the development and testing of the simulation code can start, in parallel with the development of the dedicated Monte Carlo speed up approach of WP7.2.

T0+32: The straightforward Monte Carlo simulation code should be working well. From this point on the dedicated speed up approach will be implemented and tested.

T0+34: The Monte Carlo speed up approach is working well. From this point on the accident risk simulations including bias and uncertainty assessment can be performed.

T0+36: Sufficient Monte Carlo simulation results have been collected to start drafting the final report with those results and initial analysis. The outcome of this initial analysis will identify what are the main still outstanding issues that have not yet been sorted out sufficiently well.

Deliverable

D7.3: Intermediate report on accident risk assessment of advanced autonomous aircraft operation (T0+38; Internal)

WP7.4 Final report

This is the finalization of the WP7 work and the fnal report. Special attention will be given to the communication and reporting of the TOPAZ results to decision makers, and the role this plays in the decision-making process. In support of this, WP7 will prepare guidelines for WP8.4 for the organization and moderation of a brainstorm with operational and design experts to identify mitigating measures for the main safety bottlenecks identified for the A^3 ConOps.

Milestones and expected results

T0+38: Intermediate report for requirements assessment use in WP8.4 and WP9.4.

T0+38: Guidelines for the organization and moderation of a WP8.5 brainstorming workshop in order to generate potential mitigating measures for the main safety bottlenecks identified.

T0+44: Final report, including bias and uncertainty assessment and safety bottlenecks.

Deliverables

D7.4: WP7 final report on accident risk assessment of advanced autonomous aircraft operation (T0+44; Public)

D10.2.1.sub: Scientific paper(s)

7 Concluding remarks

This report has developed the scoping, the safety target of the WP7 safety analysis within the setting of E-OCVM phase V1, and in line with E-OCVM's structured planning framework. In Section 1, the objective of WP7 is explained, both within the context of iFly and within the context of the E-OCVM framework. In Section 2, a detailed inventory of stakeholders and their expectations has been identified. In Section 3, the key safety target sources that are potentially of relevance to iFly WP7 have been identified, and ICAO's en-route Target Level of Safety setting, together with historical mid-air collision statistics, have been identified as the key sources for defining appropriate safety targets within iFly WP7. In Section 4, the preliminary scoping of the WP7 safety assessment has been identified; this may be improved as soon as the A^3 ConOps operation description has been completed, and this A^3 ConOps has undergone a Safety Screening assessment. In Section 5, TOPAZ has been identified as the right candidate safety method, together with some extensions, most of them can be accommodated either within iFly or fall outside the scope of iFly. In Section 6 the WP7 safety validation plan has been made fully in line with the technical annex to the iFly contract, and where possible with the kind of extensions and improvements identified in Section 5.

References

LIST OF REFERENCE DOCUMENTS	
Short Reference	**Author / Organisation, Title, Edition, Date and Reference**
[ARIBA WP6-I, 1999]	H.A.P. Blom and H.B. Nijhuis, Safety certification framework in ATM, ARIBA (ATM system safety criticality Raises Issues in Balancing Actors responsibility), WP6 Final Report Part I, 1999 (http://www.aribaproject.org/)
[ARIBA WP6-II, 1999]	H.A.P. Blom, M.H.C. Everdij and J. Daams, Safety Cases for a new ATM operation, ARIBA (ATM system safety criticality Raises Issues in Balancing Actors responsibility), WP6 Final Report Part II, 1999 (http://www.aribaproject.org/)
[Blom&al, 2003]	H.A.P. Blom, G.J. Bakker, M.H.C. Everdij, M.N.J. Van der Park, Collision risk modelling of air traffic, Proceedings ECC2003, European Control Conference, Cambridge, UK, September 2003.
[Blom&al, 1998/2001]	H.A.P. Blom, G.J. Bakker, P.J.G. Blanker, J. Daams, M.H.C. Everdij & M.B. Klompstra, Accident risk assessment for advanced Air Traffic Management, Eds; G. Donohue et al., Air transportation systems engineering, AIAA, 2001, pp. 463-480.
[BlomKlompstraBakker 2003]	H.A.P. Blom, M.B. Klompstra and G.J. Bakker, Accident risk assessment of simultaneous converging instrument approaches, Air Traffic Control Quarterly, Vol. 11 (2003), pp. 123-155.
[Blom&al. 2003]	H.A.P. Blom, S.H. Stroeve, M.H.C. Everdij and M.N.J. van der Park, Human cognition performance model to evaluate safe spacing in air traffic, Human Factors and Aerospace Safety, Vol. 3 (2003), pp. 59-82.
[Blom&al., 2006]	H.A.P. Blom, G.J. Bakker, B. Klein Obbink, M.B. Klompstra, Free flight safety risk modeling and simulation, Proc. Int. Conf. on Research in Air Transport (ICRAT), Belgrade, June 26-28, 2006.
[Blom&Corker&al, 2003]	H.A.P. Blom, K.M. Corker, S.H. Stroeve and M.N.J. van der Park, Study on the integration of Air-MIDAS and TOPAZ, Phase 3 final report, NLR contract report CR-2003-584, 2003.
[Brooker, 2005]	Peter Brooker, Air Traffic Management accident risk – Part 2: Repairing the deficiencies of ESARR4, Version 1, 6 May 2005, Cranfield Research Report PB/5/2/05.
[CAATS D1.4-II, 2006]	M.H.C. Everdij and H.A.P. Blom, Safety Assessment Methodologies, CAATS Deliverable D1.4 Safety Report, NLR-CR-2006-199-PT-2, National Aerospace Laboratory NLR, March 2006.
[CAATS D13i, 2008]	CAATSII, A. Pasquini, M.H.C. Everdij, H.A.P. Blom, Good practices for safety assessment in R&D projects, CAATSII intermediate report D13i, April 2, 2008.
[CAATS D14i, 2008]	CAATSII, J. Scholte, Guidance for safety activities in operational concept validation, CAATSII intermediate report D14i, April 2, 2008.

LIST OF REFERENCE DOCUMENTS	
Short Reference	**Author / Organisation, Title, Edition, Date and Reference**
[DAAS, 1995]	DAAS, Dependability Approach to ATM systems, Final report for EC-DG XIII, 1995.
[DNV, 2005]	DNV for Eurocontrol, Definition and use of target levels of safety, Task 1 report, TRS 046/04, Revision 3, 13th October 2005.
[EATMP SAM, 2002]	Air Navigation System Safety Assessment Methodology, SAF.ET1.ST03.1000-MAN-01, including Safety Awareness Document edition 0.5 (30 April 1999), Functional Hazard Assessment edition 1.0 (28 March 2000), Preliminary System Safety Assessment edition 0.2 (8 August 2002) and System Safety Assessment edition 0.1 (14 August 2002).
[EATMP SAM, 2004]	Air Navigation System Safety Assessment Methodology, SAF.ET1.ST03.1000-MAN-01, Edition 2.0, 30 April 2004. Including: Functional Hazard Assessment edition 2.0, Preliminary System Safety Assessment edition 2.0 and System Safety Assessment edition 1.0.
[ED-78A, 2000]	ED-78A/DO264 –“Guidelines for approval of the provision and use of Air Traffic Services supported by data communications” EUROCAE, December 2000. (This document is identical to the US equivalent RTCA DO-264)
[E-OCVM, 2007]	European Air Traffic Management Programme, “European” Operational Concept Validation Methodology E-OCVM, Version 2, March 2007.
[EATM Glossary, 2004]	EATMS glossary of terms, Eurocontrol, June 2004. http://www.eurocontrol.int/eatm/gallery/content/public/library/terms.pdf
[ESARR 3, 2000]	Eurocontrol Safety Regulatory Requirement (ESARR), ESARR 3, Use of Safety Management Systems by ATM Service Providers, Edition 1.0, 2000, http://www.eurocontrol.be/src/index.html (SRC deliverables).
[ESARR 4, 2001]	Eurocontrol Safety Regulatory Requirement (ESARR), ESARR 4, Risk assessment and mitigation in ATM, Edition 1.0, 5 April 2001, http://www.eurocontrol.be/src/index.html (SRC deliverables).
[Everdij&Blom, 2002]	M.H.C. Everdij and H.A.P. Blom, Bias and Uncertainty in accident risk assessment, TOSCA-II WP4 final report, 2 April 2002, NLR TR-2002-137, TOSCA/NLR/WPR/04/05/10.
[Everdij&Blom, 2003]	M.H.C. Everdij, H.A.P. Blom, Petri nets and hybrid-state Markov processes in a power-hierarchy of dependability models. In: Engel, Gueguen, Zaytoon (eds.), Analysis and design of hybrid systems, Elsevier, 2003, pp. 313-318.
[Everdij et al., 2006]	M.H.C. Everdij, H.A.P. Blo and S.H. Stroeve, Structured assessment of bias and uncertainty in Monte Carlo simulated accident risk, Proc. 8th Int. Conf. on Probabilistic Safety Assessment and Management (PSAM8), New Orleans, Louisiana, USA, May 2006.

LIST OF REFERENCE DOCUMENTS	
Short Reference	**Author / Organisation, Title, Edition, Date and Reference**
[HYBRIDGE D9.4, 2005]	H.A.P. Blom, G.J. Bakker, J. Krystul, M.H.C. Everdij, B. Klein Obbink and M.B. Klompstra, Sequential Monte Carlo simulation of collision risk in free flight air traffic, Hybridge project report D9.4 for EC, August 2005.
[iFly D2.1, 2007]	A. Luuk, J.A. Wise, F. Pouw, V. Gauthereau, Description of airborne human responsibilities in autonomous aircraft operations, iFly project report D2.1 for EC, December 2007.
[ICAO, 1998]	ICAO, Manual on airspace planning methodology for the determination of separation minima, Doc 9689-AN/953, First Edition, 1998.
[ICAO Annex 11, 2003]	ICAO, International Standards and Recommended Practices – Air Traffic Services, Annex 11, 13th edition, November 2003.
[ICAO Annex 13, 2001]	ICAO Annex 13 to the Convention on International Civil Aviation on Aircraft Accident and Incident Investigation, 2001.
[ICAO Doc 9854]	ICAO Doc 9854-AN/458, Global Air Traffic Management Operational Concept, First edition, 2005.
[ICAO SMM, 2006]	ICAO Doc 9859-AN/460, Safety Management Manual (SMM), first edition, 2006.
[ISO8402, 1994]	International Standard ISO 8402, Quality management and quality assurance – Vocabulary, 2nd edition, 1994.
[JAR 25.1309, 1994]	Joint Aviation Requirements JAR – 25, Large Aeroplanes, Change 14, 27 May 1994, and Amendment 25/96/1 of 19 April 1996, including AMJ 25-1309: System design and analysis, Advisory Material Joint, Change 14, 1994.
[Jones-Lee&Loomes, 1995]	M.W. Jones-Lee, G. Loomes, Measuring the benefits of transport safety, Proc. Safety-critical systems symposium, Eds: F. Redmill and T. Anderson, Springer, 1995, pp. 15-47.
[Laprie, 1995]	Dependability – Its attributes, impairments and means, Eds: B. Randell et al., Predictably dependable computing systems, Springer, Berlin, 1995.
[Laughery&Corker, 1997]	R. Laughery and K. Corker, Computer modeling and simulation of human / system performance, In: G. Salvedy, Congnitive engineering handbook, Wiley Interscience, 1997.
[Milloy, 1998]	C. Milloy, An introduction to risk acceptance criteria, Eds: H. Gluver and D. Olsen, Ship collision analysis, Balkema, Rotterdam, 1998, pp. 97-102.
[Moek&al, 1997]	G. Moek, J-P. Beaujard, C. Kelly, J. Mann, L. Clarke, D. Marsh, H.A.P. Blom and M.B. Klompstra, GENeric Overall Validation for ATM, WP 3 report: Methods and Techniques, EU-DGVII, NLR, 1997.
[Parker, 1996]	I. Parker, The history of the derivation and application of Target Levels of Safety, Eurocontrol workshop, 14/15 March 1996.
[RESET D6.1, 2007]	H. Blom, M. Everdij, B. Van Doorn, D. Bush and K. Slater, Existing safety assessment methods versus requirements, RESET project report D6.1 for EC-DG-TREN, Version 0.6, September 2007.

LIST OF REFERENCE DOCUMENTS	
Short Reference	**Author / Organisation, Title, Edition, Date and Reference**
[Ruigrok&Hoekstra, 2007]	R.C.J. Ruigrok & J.M. Hoekstra, Human factors evaluation of Free Flight issues solved and issues remaining, Applied Ergonomics, Vol. 38 (2007), pp. 437-455.
[SAFMAC, 2006]	M.H.C. Everdij, H.A.P. Blom, J.W. Nollet, B. Kraan, Need for novel approaches in aviation safety validation, Proceedings of Eurocontrol Safety R&D Seminar, Barcelona, October 2006.
[SAFMAC2, 2007]	M.H.C. Everdij, H.A.P. Blom, B. Klein Obbink, M.B. Klompstra, J.J. Scholte, S.H. Stroeve, Further development of SAFMAC principles, Phase 2007, NLR Report TR-2007-853.
[SAFSCREEN, 2007]	O. Sträter, H. Korteweg, M. Everdij, J. Smeltink, A. Burrage, J. Kovarova, G. Amar, Safety Screening Technique, Final draft, Edition number 1.0, Eurocontrol, 1 September 2007, http://www.eurocontrol.int/safesky/public/standard_page/safety_screening_technique.html
[SCDM, 2006]	Eurocontrol, Safety Case Development Manual, DAP/SSH/091, Edition 2.2, November 2006.
[SESAR D2, 2006]	SESAR, Air Transport Framework The Performance Target, SESAR Definition Phase Deliverable 2, DLM-0607-001-01-00, December 2006.
[SESAR D3, 2007]	SESAR, The ATM target concept, Report D3, DLM-0612-001-02-00, Version 2.0, September 2007.
[SESAR Safety, 2007]	SESAR, ATM safety regulation, Report WP1.6.2/D3, DLT_0000_162_00_07, Version 0.7, 2007.
[SESAR Case, 2007]	SESAR, Safety Case Development, Report WP4.2/Task 4.2.1, DLT_0000_421_0x_0y, Draft December 2007.
[SRC 27, 2006]	Eurocontrol SRC, Safety impact of unadopted ESARRs requirements, Working paper SRC 27.12, 27th September 2006
[SRC 28, 2007]	Eurocontrol SRC, SRC Policy on ground based safety nets, Action Paper SRC 28.06, 15th March 2007
[SRC DOC 1, 2000]	Eurocontrol SRC, SRC DOC 1: Safety Minima Study: Review of existing standards and Practices, 20th December 2000.
[SRC Pol 2, 2003]	Eurocontrol SRC, SRC Policy 2: Use of Safety Nets in Risk Assessment & Mitigation in ATM, Edition 1.0, 28 April 2003.
[SRU, 2006]	Eurocontrol SRU, Safety impact of unadopted ESARRs requirements, working paper, SRC27.12, 27/09/06, Item 5.1.
[SRU, 2006b]	Eurocontrol SRU, ESARR Compliance Checklist - Assessment of Relevant EC Regulatory Material, Edition 3.0, September 2006 (http://www.eurocontrol.be/src/public/standard_page/esims_compliance_checklist.html)
[Stroeve&al, 2003]	S.H. Stroeve, H.A.P. Blom, M. Van der Park, Multi-agent situation awareness error evolution in accident risk modelling, 5th FAA/Eurocontrol ATM R&D seminar, 23-27 June 2003.
[Stroeve&al, 2006]	S.H. Stroeve, H.A.P. Blom, G.J. Bakker, Safety risk impact analysis of an ATC runway incursion alert system, Eurocontrol Safety R&D Seminar, Barcelona, Spain, 25-27 October 2006.

LIST OF REFERENCE DOCUMENTS	
Short Reference	**Author / Organisation, Title, Edition, Date and Reference**
[VanBaren, 2002]	G.B. van Baren, L.J.P. Speijker, A.C. de Bruin, Wake vortex safety evaluation of single runway approaches under different weather and operational conditions, Proc. PSAM6, Puerto Rico, 2002.
[Wise et al, 1993]	Wise, J.A., Hopkin, V.D., and Stager, P. (eds.)., Verification and Validation of Complex Systems: Human Factors Issues, Springer, 1993.

Annex A. Elaboration of stakeholder groups

Airspace users

Examples of airspace users are:

- Airlines
- Military users
- Military operators
- General aviation
- Charter carriers
- Cargo operators
- Business aircraft operators

Human Society

Human society covers all people, e.g.:

- Passengers
- Potential passengers
- Airport neighbouring inhabitants
- Municipalities
- Environmental movements

Regulatory and supervisory authorities / bodies

These actors include National, European and International authorities, e.g.

- NSA (National Supervisory Authority), i.e. a body nominated or established by states which is independent of service providers at least at a functional level and according to the existing regulatory framework, supervises the implementation of requirements applicable to the provision of ATM services to general air transport. See [ESARR 1].
- EASA (European Aviation Safety Authority), established by the European Parliament and Council in 2002. The aim of EASA is to create a central Community body to promote the highest common standards of safety and environmental protection in civil aviation, to oversee their uniform application across Europe, and to promote them at world level.
- CAAs (Civil Aviation Authorities). Each CAA should represent the particular opinions and constraints of each country involved in the single ATM system in Europe. The systems which will be deployed in its territory should be approved by this authority.
- JAA (Joint Aviation Authority), which is an associated body of the European Civil Aviation Conference (ECAC) representing the civil aviation regulatory authorities of 39 European States (in September 2005). It is the current unified organisation in Europe for airborne equipment certifications. All configurations which include any elements any should be validated with the participation of JAA.
- Certification institutes
- ICAO (International Civil Aviation Organisation)
- EUROCAE (European Organisation for Civil Aviation Equipment)
- Eurocontrol Safety Regulatory Commission
- GASR (Group of Aerodrome Safety Regulators), a voluntary organisation with no formal institutional identity, which, through mutual co-operation, aims for harmonisation of the safety regulation of aerodromes encompassing both the airport infrastructure and the airport operations.

Policy makers

- Policy makers include:
- Ministry of Transport
- Ministry of Defence
- The European Commission as the main political authority in Europe. Political aspects to be taken into account in validation activities will, to a large extent originate in European Commission.
- Eurocontrol Headquarters (EHQ)
- ECAC Member states; The European Civil Aviation Conference currently consists of 42 Member States comprising almost all European States. Its objective is to promote the continued development of a safe, efficient and sustainable European air transport system. ECAC issues resolutions, recommendations and policy statements which should be brought into effect by its Member States.

Air Navigation Service Providers

These actors are:

- National ANSPs (Air Navigation Service Providers). Organisations such as LVNL, AENA, ANA, NATS, etc. use the current ATM systems to provide ATS services and will use the future ATM systems.
- Eurocontrol, as ATS service provider for a part of Europe, e.g. Maastricht UAC
- ASM (Air Space Management) service providers
- ATFM (Air Traffic Flow Management) service providers (CFMU (Central Flow Management Unit) of Eurocontrol)
- ATS (Air Traffic Services) providers (ATC (Air Traffic Control) centres, FIS (Flight Information Services))
- SAR (Search and rescue)
- Military airspace planners

Airports

These actors are:

- Airports national
- Airports regional
- Airport authorities

Manufacturers

These actors are:

- Aircraft manufacturers
- Aircraft equipment manufacturers
- Ground-based equipment / systems manufacturers
- Supply industry
- Aeronautics Industry

Human operators

These actors are:

- Controllers (Supervisors, Planning controllers, Executive controllers, CFMU operators)
- Aircraft crew (Pilot)
- Technicians

Other Service Providers

These actors are
- Maintenance service providers
- AIS (Aeronautical Information Services) providers
- Meteorological service providers
- Telecommunication service providers
- Satellite communication service providers
- Eurocontrol, as the body which manages and handles the en route charges which the airlines pay to ATS service providers. Any change in the system will impact air navigation operational procedures and the charges associated with them.
- Specialised organisations: Several organisations in Europe are specialised in some area of the ATM system. For example
    - SITA (Aeronautical Telecommunications International Society).
    - European Space Agency (ESA), which could be especially involved in the ATM space segment.

Associations and Federations
This group includes associations, organisations or unions related to air transport, e.g.:
- AEA (Association of European Airlines), which has 37 member airlines, see http://www.aea.be/AEAWebsite/Presentation_Tier/Pr_AboutUs.aspx
- ERA (European Regions Airline Association), an association of over 220 companies, including 67 airlines, 40 airports and over 115 associate and affiliate members comprising aircraft & engine manufacturers, international & regional airports and avionic suppliers & service providers, http://www.eraa.org/.
- IATA (International Air Transport Association). Represents some 265 airlines comprising 94% of international scheduled air transport.
- IFALPA (International Federation of Air Line Pilots Associations), http://www.ifalpa.org/
- IFATCA (International Federation of Air Traffic Controllers' Associations), http://www.ifatca.org/
- CANSO (Civil Air Navigation Services Organisation), http://www.canso.org/canso/web/
- ACI (Airports Council International) Europe, a professional association of airport operators; represents some 400 airports in 45 European countries, http://www.aci-europe.org/.
- ASD (Aerospace and Defence Industries Association of Europe), represents the aeronautics, space, defence and security industries in Europe in all matters of common interest with the objective of promoting and supporting the competitive development of the sector. ASD has 30 member associations in 20 countries across Europe and represents over 2000 companies with a further 80000 suppliers, many of which are SMEs. http://www.asd-europe.org/Content/Default.asp?
- ATCEUC (Air Traffic Control European Unions Coordination), http://www.atceuc.org/
- Aviation Meteo Group
- EBAA (European Business Aviation Association), http://www.ebaa.org/
- ECA (European Cockpit Association), association of Flight Crew Unions from across Europe. Based in Brussels, ECA presently has 27 Member Associations, representing 34300 pilots from 27 countries.
- ELFAA (European Low Fares Airline Association), http://www.elfaa.com/
- IACA (International Air Carrier Association), http://www.iaca.be/

- IAOPA (International Council of Aircraft Owner and Pilot Association), a non-profit federation of 53 autonomous, nongovernmental, national general aviation organizations. http://www.iaopa.org/

Other actors
The miscellaneous group includes:

- Universities
- Aviation consultants
- Independent research institutes
- Government researchers
- Education institutes
- Incident / accident investigation
- Publishers in aviation
- Public media
- Eurocontrol Research Centre and own programmes (EATCHIP & EATMS)
- Insurance firms
- Committees

Annex B. Safety validation quality indicators

Safety validation is the process aimed to validate[†] the safety of a particular operation. Depending on the user requirements, such method can be used e.g. to assess whether this operation satisfies a safety design target, it can indicate which aspects of the operation require attention and further development, and/or it can answer other safety-related questions. Obviously, a safety validation can be done in different ways, and the quality of the result will depend on how the safety validation process is done, on the quality of the input and the experts used, which safety issues were evaluated, and which aspects of the operation were sufficiently covered.

[SAFMAC, 2006] has developed a consolidated set of indicators that are of use to judge how well a given safety validation method satisfies the objective of developing a good safety case for a major change in air transport operations. An example candidate indicator is "Transparency", denoting that transparency of a safety validation process is considered a relevant aspect for developing a good safety case for such major change. Of course, transparency covers only one important aspect, and we are looking for a consolidated set of indicators that together cover all important aspects.

The process towards developing such consolidated set of indicators started with the identification of many potential candidate indicators. Main sources used were a brainstorm session with experts in air traffic operations, regulations and safety, and an extensive identification of indicators from several literature sources. This literature included sources in which techniques of various natures (e.g. human factors, computer processes, technical systems) were evaluated on different aspects. The result was a long list of more than 200 candidate indicators, amongst which some doubles.

Next, the resulting long list of candidate indicators was divided into initial groups, based on the types of requirements of the safety validation framework for major changes. Examples of initial groups were: Indicators related to interactions with air transport design, Indicators related to international acceptability, Indicators related to certain safety assessment steps. Subsequently, per initial group, by an iterative process, the list of candidate indicators was consolidated through discussion, evaluation, and expert review. Main challenges in this iterative process were to be consistent and exhaustive with respect to the study objectives, and to find a suitable formulation for each indicator, which allows to measure a given safety validation method against the indicator.

The consolidated set consists of 32 indicators, which were finally re-ordered, numbered CI-01 through CI-32 (where CI denotes consolidated indicator), and divided into the following six groups:

- Indicators related to the scoping of safety validation
- Indicators related to coverage of certain aspects of the operational concept
- Indicators related to risk assessment
- Indicators related to feedback to Concept of Operations (ConOps) development
- Indicators related to organisation of safety assessment
- Indicators related to supporting decision and policy makers

[†] Commonly, 'validation' is defined as answering the question "are we building the right system?", as opposed to 'verification', which is defined as answering the question "are we building the system right?"

Indicators related to the scoping of safety validation

The first group contains indicators related to scoping of a safety validation of major changes in air transport operations. It contains four elements, numbered CI-01 through CI-04, which are described and motivated below.

CI-01: Information / data needed. This indicator measures how well the method can produce effective results if there is only limited input information available from operational concept designers. The motivation for including this indicator is that especially in the early stages of operational concept development, there usually is only limited information available. The safety validation framework should still be able to produce effective results.

CI-02: Scoping the assessment. The second indicator measures how well the framework handles scoping, which entails writing a safety plan that specifies the scope of the safety assessment and outlines a "route map" for the safety assessment. It also measures if the safety target is defined outside the safety assessment. Motivation for including this indicator is that scoping of the assessment is one of the key steps of any safety assessment. If this step is skipped or not done properly, the effects on later steps can be significant, e.g. leading to miscommunication or to forgotten elements, and to deviations from expectations of decision makers or other authorities. Scoping should include the identification of safety targets, but independent of the safety assessment.

CI-03: Safety Target breakdown. This indicator measures if the method supports a breakdown of the overall safety target to the level of detail required, e.g. into risk budgets for sub-operations, during all stages of the lifecycle. The safety validation framework should support this breakdown.

CI-04: Learning the nominal operation. The final indicator in this group measures how well the safety assessment framework supports learning of the nominal operation, i.e. learning to understand the operation and systems as they should work or function. The safety assessor should invest time in learning how the operation and all of its elements work before the actual safety assessment can commence. Annex A. Safety Assessment Quality Indicators

Indicators related to coverage of certain aspects of the operational concept

The second group contains indicators related to coverage of certain aspects of the operational concept for a major change in air transport operations. It contains eight elements, numbered CI-05 through CI-12, which are described and motivated below.

CI-05: Identifying hazards. The first indicator in this group measures how well hazards are identified, including hazards that may not be known yet, but may occur in future operations. And it measures if the hazard identification covers all aspects of the future operation. The motivation is that hazard identification is important in any safety assessment. If certain aspects of the operation, e.g. procedures, organisation, or aspects that are not easily imaginable, are not covered, then these are likely also forgotten in following steps.

CI-06: Coverage of technical systems. This indicator measures how well technical systems (hardware and software) are covered by the safety assessment, including technical systems that can be expected for future operations. Motivation is that major changes in air transport will incorporate new technology. This should be addressed by the safety validation framework.

CI-07: Coverage of human factors for risk and CI-08: Coverage of human factors for human. Air transport typically has a major human factors component. Indicator CI-07 measures how well human factors are covered from risk perspective, including human factors that can be expected for future operations. It takes the human factors perspective of the safety risk of conducting the operation considered, which includes human error. Indicator CI-08 measures how well human factors are covered from human perspective, including human factors that can be expected for future operations. Motivation of including CI-08 in addition to CI-07 is that considering humans as a source of error only is much too limited a perspective in safety assessments.

CI-09: Interactions and environment. This indicator measures coverage by the method of interactions between multiple agents in the operation (e.g. air traffic controller, pilot, military ATM, navigation and surveillance equipment, search and rescue), and with the environment of the operation. Generally, certification of technical systems and human training ensure that each of the elements of the operational concept are ‘safety certified’ individually. However, usually, it is the interactions between these elements and with the environment that create most risk.

The three final indicators in this group are CI-10: Coverage of procedures, CI-11: Coverage of organisation and CI-12: Coverage of institutional elements. Here, CI-10 measures how well procedures are covered, CI-11 measures coverage of the organisation within and between stakeholders, and CI-12 measures coverage of institutional elements. All three also cover those elements that can be expected for future operations. The motivation for including these indicators is that major changes will usually involve replacement or change of procedures and re-organisation of air traffic control and/or airspace, and will also influence and be influenced by institutional elements, i.e. interactions between organisations at a higher level. The safety validation should address these changes and influences properly.

Indicators related to risk assessment

The third group contains indicators related to risk assessment of major changes in air transport operations. It contains four elements, numbered CI-13 through CI-16, which are described and motivated below.

CI-13: Combining hazards. This measures how well the identified hazards are combined, connected to safety-related scenarios and evaluated. Motivation is that the assessment of each identified hazard individually gives no insight in how the combinations of all hazards and other elements influence risk for the total operation. Therefore, hazards should be combined in a risk framework of safety-related scenarios.

CI-14: Evaluating risk. This measures how well the framework evaluates the risk according to the identified scenarios. This risk framework should be evaluated in a way that corresponds with reality as closely as possible. The adoption of assumptions, the effect of which cannot be estimated, should be avoided where possible.

CI-15: Coverage of nominal risk. The fifteenth indicator measures how well the method addresses the risks during normal (nominal) operations, i.e. the systems and procedures are designed and a hazard-free scenario is being considered. Incidents and accidents may happen even if there are no obvious causal hazards to be blamed. These situations may form an essential aspect of the safety of the operation.

CI-16: Approximations analysed. The final indicator in this group measures how well the framework identifies and evaluates approximations made with respect to reality. During any safety assessment many assumptions are adopted and approximations are made, e.g., there is an implicit assumption that all important hazards have been identified. The safety validation framework should encourage the safety assessor to identify and evaluate all these approximations, in order to check if they are reasonable and if the deviation from reality is not too large. Without insight into the combined effect of all approximations, the assessed risk result is meaningless.

Indicators related to feedback to ConOps development

The fourth group contains indicators related to feedback to ConOps (Concept of Operations) development of major changes in air transport operations. It contains three elements, numbered CI-17 through CI-19, which are described and motivated below.

CI-17: Feedback and communication. This indicator measures how well feedback (if any) is communicated with operation design. Key to the safety validation framework is that it should provide effective feedback to operational concept development, during all lifecycle stages. For major changes, the safety effect may not at all be predictable, even by experienced experts. Safety validation results that are conflicting with the intuition of experienced domain experts may be acceptable if the safety assessors can convincingly explain why.

CI-18: Supporting risk mitigation. The safety validation framework should not only give a yes/no answer to the question: is this operation sufficiently safe?; it should also provide support to operation designers on how to identify strategies that maintain or improve safety, now and in the future. These mitigation strategies are best identified by the operational concept designers themselves, but the safety validation should give effective support.

CI-19: Monitoring / verifying actual risk. The final indicator in this group measures how well the framework supports the monitoring and verification of actual risk. Once the operational concept is implemented and operational, the safety validation framework should continue and monitor safety, and verify if safety is indeed at the level predicted.

Indicators related to organisation of safety assessment

The fifth group contains indicators related to organisation of safety assessment of major changes in air transport operations. It contains seven elements, numbered CI-20 through CI-26, which are described and motivated below.

CI-20: Resource requirements (equipment and personnel). This measures if the level of resources needed is reasonable for the results delivered (where resources refers to number of personnel, their training, availability and length of their time required by the study, as well as equipment and administrative support requirements). The people who are going to pay for performing the safety assessment of a new operation will be interested to know what applying the framework requires in terms of resources.

CI-21: Criticism. I.e. is the method able to withstand criticism? For a safety validation framework to get support, nationally and internationally, not only technical but also political aspects need to be addressed. E.g., several organisations already invested in a safety assessment framework of their own, and will want to see that one implemented internationally, rather than another one. On the other hand, if the new framework can really show to have advantages above existing ones, e.g., withstand criticism better, the support will be found easier.

CI-22: Level of safety expertise required. This indicator measures how well the method poses requirements on the designated safety assessor to have the proper operational safety expertise background. The safety validation framework can only be used in an effective way if the safety assessors who use it satisfy the applicable expertise requirements. The framework should provide a way to test and ensure this.

For a safety validation framework to be acceptable, the safety process steps should be transparent. The problem is that transparency in itself may be hard to measure; it is strongly dependent on the expertise and experience of the person reviewing the method and results. Therefore, here, transparency is represented by two measurable indicators, the first one being CI-23: Documentability of process steps, i.e. what is the degree to which the framework lends itself to auditable documentation? and the second one being CI-24: Consistency, i.e. how well is the consistency of the use of the framework, such that if used on two occasions by independent experts, reasonably similar results are derived? If the process steps are not documentable, they can never be transparent. Consistency may also cover structuredness and reproducibility to some extent.

CI-25: Compliance to ESARRs, CR, ICAO. This indicator measures the level of compliance to international norms and regulations such as ESARRs, Common Requirements (CR) of the

EU, and ICAO requirements, or other international requirements (e.g. aircraft-related certification/performance requirements). There are relevant points of criticism regarding ESARR 4 and the CR, and it is possible that they will be updated in the near future to take this criticism into account. However, throughout the states, they are regarded as a standard, and in many places, their compliance is considered essential for acceptability.

CI-26: Flexibility. This indicator applies in case of a modification in the operational concept description when the safety assessment is already ongoing, and measures how much additional time/effort is required to update the safety assessment accordingly. Motivation is that the safety assessment should fit in the planning of the design, and must therefore not need too much time to produce results. Related to this is that the framework should be able to produce effective results even if the input is subject to change.

Indicators related to supporting decision and policy makers

The sixth and final group contains indicators related to supporting decision and policy makers involved in major changes in air transport operations. It contains six elements, numbered CI-27 through CI-32, which are described and motivated below.

First, there are three more indicators related to transparency. The first one is

CI-27: Transparency regarding applicability. This asks to what extent it becomes clear which applications (e.g. air transport operations, aircraft flight, runway incursions, Single European Sky) are accommodated. The framework should be applicable to the safety validation of major changes in air transport operations. Therefore, the framework should provide clarity on whether this is the case, and whether there are limitations to the types of operations that can be covered. The second indicator is

CI-28: Transparency of results. This indicator measures transparency of the results, where transparency is defined as understandable, traceable, and well documented. Even if the safety validation process steps followed are all transparent, it may still occur that the results are not. The audience of a safety case should be able to understand the results, and be able to trace how they were obtained. The third indicator is

CI-29: Transparency of safety assessment process. This indicator measures the extent to which the steps in the safety assessment process or framework are transparent to the safety assessor. A safety validation framework will not be used if the safety assessors are not able to understand what they are doing and why, even with the proper training.

CI-30, CI-31, CI-32: Finally, there are three groups of stakeholders in safe air transport operations who deserve an indicator of their own; the safety validation framework should provide them with proper support, for them to be able to do their job. They are decision makers (CI-30: Support to decision makers), regulatory authorities (CI-31: Support to regulatory authorities), and safety oversight (CI-32: Support to safety oversight). Regulators should get support in order to set or modify regulations for air transport operations. Safety oversight is a function by means of which states ensure effective implementation of the safety-related Standards and Recommended Practices and associated procedures. An individual state's responsibility for safety oversight is the foundation upon which safe global aircraft operations are built. Lack of appropriate safety oversight in one state therefore threatens the health of international civil aircraft operation.

Annex C. Acronyms

A^3	Autonomous Aircraft Advanced
A^4	Automated-ATM supported Autonomous Aircraft Advanced
ACAS	Airborne Collision Avoidance System
ACI	Airports Council International
AEA	Association of European Airlines
AIS	Aeronautical Information Services
ANS	Air Navigation Service
ANSP	Air Navigation Service Provider
AOC	Airline Operational Centres
APW	Airborne Proximity Warning
AQUI	University of l'Aquila
ASAS	Airborne Separation Assistance Systems
ASD	Aerospace and Defence Industries Association of Europe
ASM	Air Space Management
A-SMGCS	Advanced Surface Movement Guidance and Control System
ASOR	Allocation of Safety Objectives and Requirements
ATC	Air Traffic Control
ATCEUC	Air Traffic Control European Unions Coordination
ATCO	Air Traffic Controller
ATFM	Air Traffic Flow Management
ATS	Air Traffic Services
ATM	Air Traffic Management
AUEB	Athens University of Economics and Business Research Centre
BIP	Background Intellectual Property
CA	Consortium Agreement
CAA	Civial Aviation Authority
CAATS	Cooperative Approach to Air Traffic Services
CANSO	Civil Air Navigation Services Organisation
CARE	Co-operative Action of R&D in Eurocontrol
CNS	Communication, Navigation and Surveillance
ConOps	Concept of Operations
DSNA	DSNA-DTI-SDER (formerly CENA)
EASA	European Aviation Safety Authority
EATCHIP	European Air Traffic Control Harmonisation and Integration Programme
EATMS	European Air Traffic Management System
EBAA	European Business Aviation Association
EC	European Commission
ECA	European Cockpit Association

ECAC	European Civil Aviation Conference
EEC	Eurocontrol Experimental Centre
EHQ	Eurocontrol HeadQuarter
ELFAA	European Low Fares Airline Association
EM	Exploitation Manager
ENAC	Ecole Nationale de l'Aviation Civile
E-OCVM	European Operational Concept Validation Methodology
ERA	European Regional Airlines Association
ESA	European Space Agency
ESARR	Eurocontrol Safety Regulatory Requirement
ETHZ	Eidgenössische Technische Hochschule Zürich
EU	European Union
FAA	Federal Aviation Authority
FAR	Federal Aviation Regulations
FIP	Foreground IP
FIS	Flight Information Services
GAT	General Air Traffic
GPWS	Ground Proximity Warning System
HNWL	Honeywell
HYBRIDGE	Distributed Control and Stochastic Analysis of Hybrid Systems Supporting Safety Critical Real-Time Systems Design (EC 5th Framework Programme)
IACA	International Air Charter Association
IAF	Initial Approach Fix
IAOPA	International Council of Aircraft Owner and Pilot Association
IATA	International Air Transport Association
ICAO	International Civil Aviation Organisation
IFALPA	International Federation of Air Line Pilots Associations
IFATCA	International Federation of Air Traffic Controllers Associations
IFR	Instrument Flight Rules
INRIA	Institut National de Recherche en Informatique et en Automatique
IP	Intellectual Property
IPR	Intellectual property rights
JAA	Joint Aviation Authorities
JAR	Joint Aviation Requirements
LVNL	Luchtverkeersleiding Nederland
MET	Meteo
MUAC	Maastricht Upper Airspace Control
NATS	NATS En Route Ltd.
NEXTGEN	Next Generation Air Transportation System
NLR	National Aerospace Laboratory NLR

NSA	National Safety Authority
NTUA	National Technical University of Athens
OHA	Operational Hazard Assessment
OPA	Operational Performance Assessment
OPS	Operations
OSA	Operational Safety Assessment
OSED	Operational Services and Environment Description
PC	Project Co-ordinator
PMP	Project Management Plan
PoliMi	Politecnico di Milano
R&D	Research and Development
RGCSP	Review of General Concept of Separation Panel
RTD	Research, Technology and Development
R/T	Radio Telecommunication
SA	Situation Awareness
SAR	Search and Rescue
SES	Single European Sky
SESAR	Single European Sky ATM Research
SITA	Societe Internationale de Telecommunication Aerienne/Aeronautiques
SME	Small and medium sized enterprises
SPR	Safety and Performance Requirements
SRC	Safety Regulation Commission
SWIM	System Wide Information Management
TCAS	Traffic Collision Avoidance System
TLS	Target Level of Safety
TOPAZ	Traffic Organization and Perturbation AnalyZer
TWEN	University of Twente
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UCAM	University of Cambridge
ULES	University of Leicester
UTartu	University of Tartu
WP	Work Package
WPL	Work Package Leader