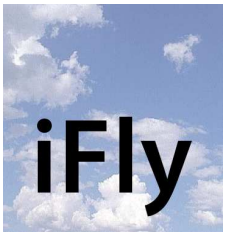

Project no. TREN/07/FP6AE/S07.71574/037180 IFLY

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 D10.1i
Initial Validation Strategy/Plan

Version: Draft 0.6

Due date of deliverable: 22 November 2007
Actual submission date: 7th January 2008

Start date of project: 22 May 2007 Duration: 39 months

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)		
Dissemination Level		
PU	Public	✓
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:	Initial Validation Strategy/Plan
Authors of document:	Henk Blom
Deliverable number:	D10.1i
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	16-10-2007	All	First draft
0.2	31-10-2007	All	Second draft
0.3	09-11-2007	All	Third draft
0.4	31-12-2007	All	Internal review comments incorporated
0.5	30-09-2008	All	Additional review comments incorporated
0.6	25-08-2009	All	Change in iFly

Version 1.0		Organisation	Signature/Date
Authors	Henk Blom	NLR	
Internal reviewers	Kostas Zografos	AUEB	
	John Lygeros	ETHZ	
	Ignacio Rodriguez	Isdefe	
	Jelmer Scholte	NLR	
External reviewers	Kasia Gryc	EC-DGTREN	

Abstract

This report describes the way how iFly activities comply with the E-OCVM validation approach.

Table of Contents

1 Introduction

1.1 Background

The iFly project definition has started as a response to the European Commission (EC) 6th Framework Programme call for Innovative ATM Research in the area of 'Aeronautics and Space'. The research is expected to develop novel concepts and technologies with a fresh perspective into a new air traffic management paradigm for all types of aircraft in support of a more efficient air transport system. It is aimed at supporting SESAR in the integration of collaborative decision-making in a co-operative air and ground Air Traffic Management (ATM) end to end concept, validating a complete ATM and Airport environment, and takes into account the challenging objectives of Single European Sky and EUROCONTROL's ATM2000+ strategy, as endorsed by the ECAC Ministers:

1. *Improve today's safety* levels taking into account projected traffic levels, by providing better information to both the pilot and the controller on surrounding traffic;
2. Increase system capacity to safely handle three times more air movements by 2020 through an increased planning capability, coupled with a *progressive distribution of tasks and responsibilities* between the aircraft and the ground for separation to satisfy projected traffic growth;
3. Improve system efficiency with a view to achieving an average maximum delay of one minute per flight;
4. Maximise airport operating capacity in *all weather conditions to support increasing traffic demand through improved systems to aid the controller and pilot*.

In order to significantly contribute to the realisation of these challenging objectives, the iFly proposal develops a paradigm step change in advanced ATM concept development through a systematic exploitation of state-of-the-art stochastic modelling, analysis, optimization and Monte Carlo simulation. The iFly project is shortly described in section 2.

1.2 Validation and development framework

Because a research project in support of SESAR addresses certain strategic objectives, it is quite important that it is embedded in an appropriate validation and development framework, which takes well into account the stakeholders involved with the operation under design. The validation and development framework adopted for iFly is the European Operational Concept Validation Methodology [E-OCVM, 2007]. This framework is shortly described in Section 3. Because [E-OCVM, 2007] does not explain yet how safety validation and safety case development activities are related to this framework, this is covered in Section 4. From this analysis it becomes clear which E-OCVM phases are covered by the iFly project. Subsequently, Sections 5 through 7 place the various iFly activities in the context of these iFly relevant E-OCVM phases. Finally, Section 8 draws conclusions.

2 iFly project

2.1 Motivation of iFly

During recent years the ATM community research trend is to direct large airborne self separation research projects to situations of less dense airspace. Typical examples of this trend are the EC research projects MFF (Mediterranean Free Flight) and ASSTAR (Advanced Safe Separation Technology and Algorithms). This is remarkable because airborne self separation has been "invented" as a potential solution for high density airspace. The iFly project aims to show which traffic demand levels can safely be accommodated by airborne self separation, and to identify the best complementary ground based support in safely accommodating higher traffic demands. iFly will do so though a systematic exploitation and further development of the advanced mathematical techniques that have emerged within the HYBRIDGE project of EC's 5th Framework Programme (http://www.nlr.nl/public/hosted-sites/hybridge/).

By using the novel mathematical techniques that emerged through HYBRIDGE, the Self Separation concept for Mediterranean Free Flight has been evaluated through Monte Carlo simulations. The results obtained show that this design works well for a two aircraft head-on encounter. For multiple aircraft encounter scenarios, however, the design is working less good because of a significant delay in finding resolutions. Moreover, the resolution found typically deviate significantly from the optimal coordinated resolution. This means there is great potential to design an airborne self separation concept of operation that is doing much better for demanding scenarios.

This forms sound motivation for iFly to further the HYBRIDGE approach with the aim to develop both an advanced airborne self separation design and a highly automated ATM design for en-route traffic, which takes advantage of autonomous aircraft operation capabilities and which is aimed to manage a three to six times increase in current en-route traffic levels. This incorporates analysis of safety, complexity and pilot/controller responsibilities and assessment of ground and airborne system requirements. The proposed iFly research combines expertise in air transport human factors, safety and economics with analytical and Monte Carlo simulation methodologies providing for "implementation" decision-making, standardisation and regulatory frameworks. The research is aimed at supporting SESAR and actively disseminates the results among the ATM research community.

2.2 iFly work structure

The proposed iFly research combines expertise in air transport human factors, safety and economics with analytical and Monte Carlo simulation methodologies providing for "implementation" decision-making, standardisation and regulatory frameworks.

Specifically, 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.

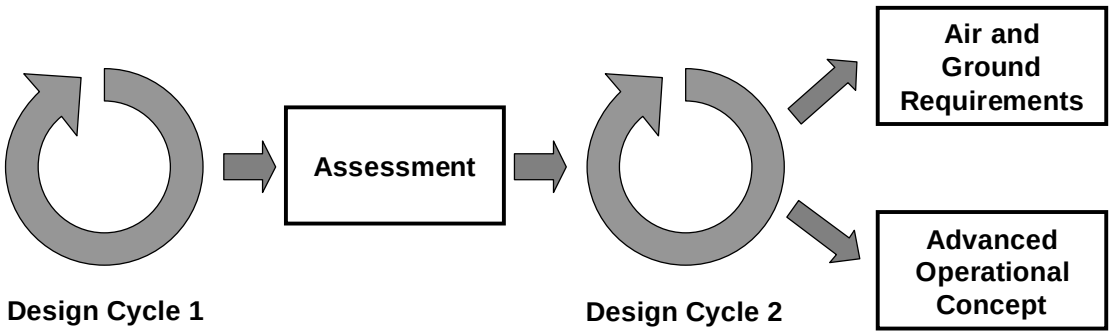

Figure 1: iFly Work Structure.

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, and have recently been identified by the RTD programme "HYBRIDGE" (EC 5th Framework Programme) as being of great use in the design of advanced ATM.

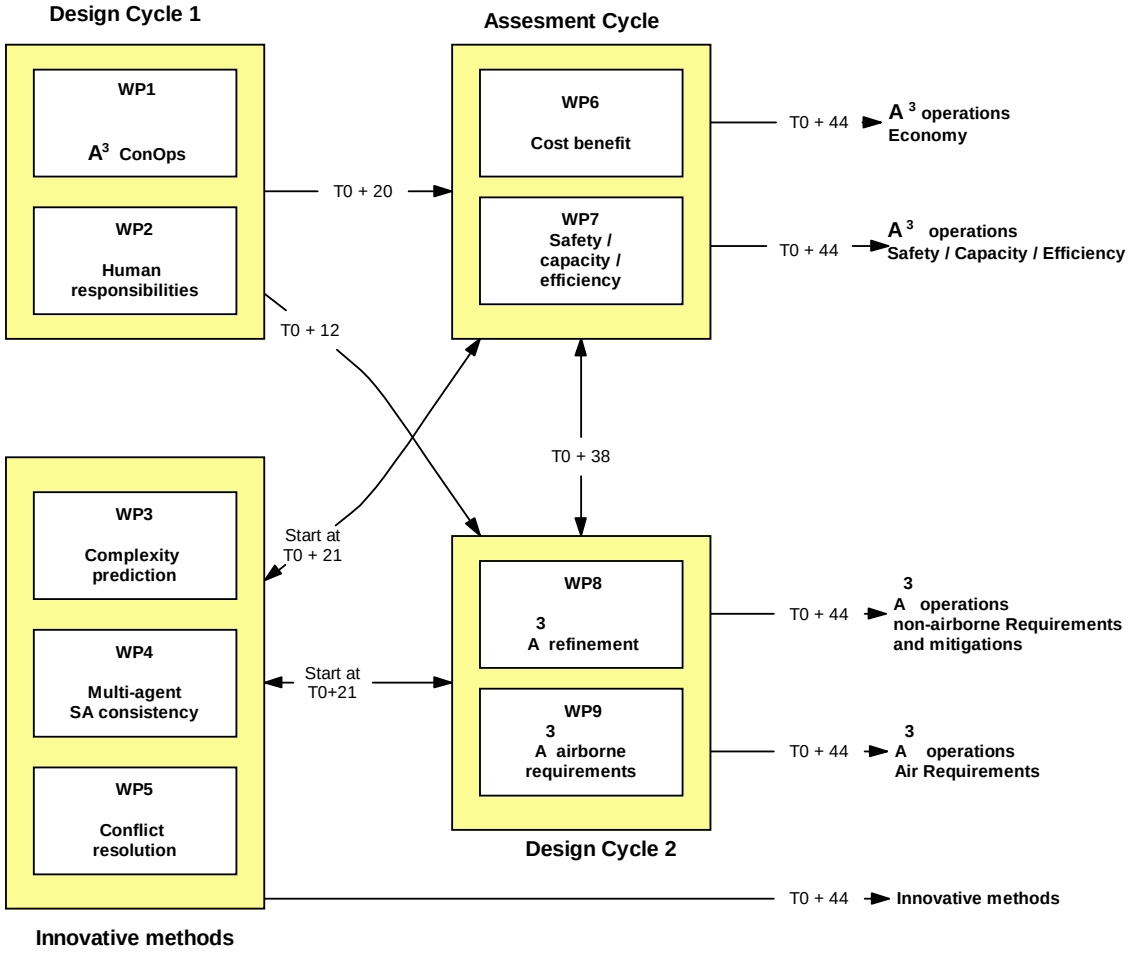

Figure 2: Organisation of iFly research

Description of the work

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 develop an operational concept capable 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.

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:

Design cycle 1

The aim is to develop an Autonomous Aircraft Advanced (A^3) en-route concept of operations (ConOps) 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.

Innovative methods

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 guarantee their performance (WP5).

Assessment cycle

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^3operation on safety as a function of traffic density increase over current mean density level (WP7)

Design 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 will be developed on the applicable functional elements of the A^3 ConOps focused in order to identify the required technology.

2.3 Measurable and verifiable project objectives

iFly has nine measurable and verifiable objectives; three of nature Assess (Group I), three of nature Innovative methods (Group II), and three of nature advanced ConOps (Group III):

I. Assess the state-of-the-art in autonomous aircraft 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:
   1. Assess a "state-of-the-art" Autonomous Aircraft Advanced (A^3) en-route operation with respect to safety as a function of traffic density increase over current mean density level. 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;
   2. Assess the same A^3 operation on economy, with emphasis on the impact on this caused by organisational and institutional issues;
   3. Assess the same A^3 operation on human factors issues, with emphasis on the human responsibilities and goal settings of pilots and of airlines.

II. Develop innovative architecture free methods towards key issues that have to be addressed by an advanced operational concept:
   4. Develop a method to model and predict complexity of air traffic without adopting *a priori* given separation minima, sector boundaries or human limitations;
   5. Model and evaluate the problem of maintaining multi-agent Situation Awareness and avoiding cognitive dissonance within en-route A^3 operations;
   6. Develop conflict resolution algorithms for which it is formally possible to guarantee their performance, compare these with "state-of-the-art" methods earlier developed within aeronautics research.

III. Develop an advanced en-route concept of operations (ConOps) which goes beyond the limits posed by the "state-of-the-art" A^3 operation referred to under objective 1:
   7. Develop an A^3 en-route operational concept which is initially based on the current "state-of-the-art" in aeronautics research, and which is later refined by taking advantage of the results referred to under objectives 1, 2, 3, 4, 5 and 6;
   8. Develop a vision how A^3–equipped aircraft fit best within the SESAR thinking regarding future ATM, such that the resulting operation goes beyond the A^3 en-route operation in such a way that it safely accommodates a factor three to six more traffic then at current busy traffic levels.
   9. Perform a preliminary cycle through the EUROCAE ED78A method to derive preliminary safety and performance requirements on the applicable functional elements of the A^3 operational concept focused in order to identify the required technology to make this concept a reality.

3 Validation and development framework

3.1 European Operational Concept Validation Methodology (E-OCVM)

A lack of clear and understandable information to support decision making on air traffic management system implementation in the mid 1990s motivated validation research in Europe. The European Commission provided support for this and brought together industry, R&D organisations, service providers and Eurocontrol. The findings eventually converged into the European Operational Concept Validation Methodology (E-OCVM). The E-OCVM has become the major source of reference for all European Commission and Eurocontrol validation activities [E-OCVM, 2007].
Generally, the E-OCVM is based on three different views:

(1) A concept lifecycle view (Figure 3), placing the operational concept in a timeframe and considering its maturity. This facilitates the setting of appropriate validation objectives, the choice of evaluation techniques, shows how concept validation interfaces with product development and indicates where requirements should be determined;

(2) A Structured Planning Framework, which facilitates programme planning and transparency of the whole process. This allows a stepped evaluation view, looking at the specific objectives of a certain project and its experiments on a detailed level and applying a stepwise approach to ATM validation; and

(3) A case-based view (Figure 4), gathering the information generated by various tests and experiments in a way that helps explain to stakeholders what can be expected in terms of performance and behavioural capabilities.

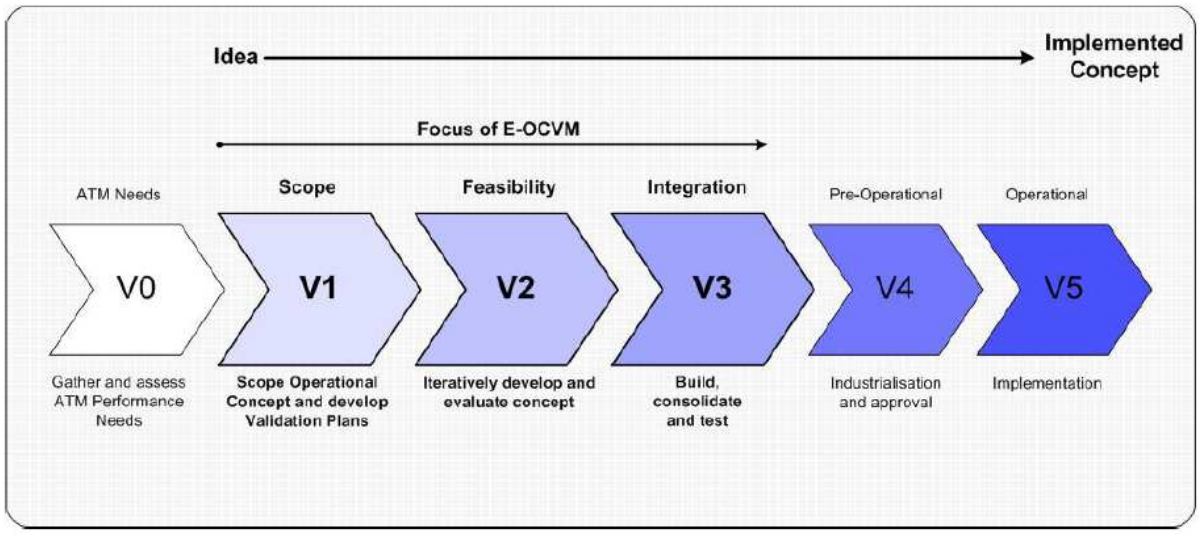

Figure 3: Concept Lifecycle model of the E-OCVM

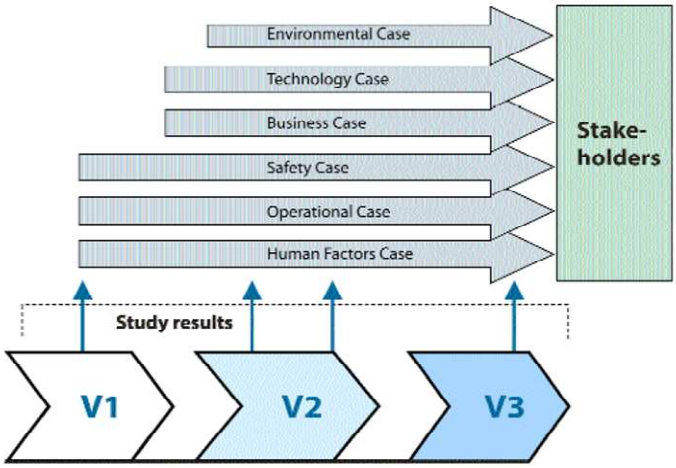

Figure 4: E-OCVM Case-based View

Together, these three views (Concept Lifecycle, Structured Planning and Case Based) form a process which help providing structure to an iterative and incremental approach to concept development and concept validation, and is focused on developing a concept towards an application while demonstrating to key stakeholders how to achieve an end system that is fit for purpose. The Concept Lifecycle is the central aspect of the validation process.

3.2 E-OCVM life cycle phases

The Concept Lifecycle Model is the central aspect of the validation process of E-OCVM, and for the other two aspects it can be described how they play a role in each of the phases of the Concept Lifecycle Model, as is done in Section 3 of the E-OCVM. Because of this central position of the Concept Lifecycle Model, the description of this aspect is also copied from [E-OCVM, 2007]:

"The 6 phases of the Concept Lifecycle Model are:

V0 ATM Needs – As a prerequisite of concept validation, the ATM performance needs and barriers must be identified. To complete the validation of the concept, the concept must show that it can alleviate these barriers enough thus enhancing ATM performance to the anticipated required level.

V1 Scope – The phase where the 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.

V2 Feasibility – This phase aims to develop and evaluate, in an iterative way, the concept until it can be considered operationally feasible. During this phase system prototypes will be used that make assumptions about technical aspects in order to avoid system engineering which can be costly and lengthy. Aspects that should be focused on are operability and the acceptability of operational aspects. It is during this phase that operational procedures and

requirements should become stable. The number of iterations depends on the complexity of the concept and how often unexplained situations occur that need to be explained. At the end of this phase HMI, Operating procedures (for normal and key non-normal conditions) and phraseology should be thoroughly tested. This stage will establish the behaviours of the new system.

V3 Integration – The phase to integrate any required functionality into pre-industrial prototypes. Engineering processes can be explored to provide experience that will be useful to building the endsystem. This phase is focused on integrating operating procedures by using realistic scenarios that are representative of what the concept must be able to manage in the target end-system. The focus is therefore on system level behaviour, performance and establishment of standards/regulations necessary to build and operate the required technical infrastructure. This work will enable costs and benefits to be clearly identified and provide information about the potential performance of the overall ATM system.

V4 Pre-Operational – Pre-operational preparation takes place during this phase. Pre-operational prototypes will be transformed into industrial products ready for implementation and all institutional issues concerned with procedures approval should be addressed (Out of direct scope for R&D).

V5 Implementation – This is the phase when products and procedures are combined to create an operational system at a specific site. Implementation is a complex and risky procedure and it can be expected that many pragmatic 'fixes' will be required to complete implementation successfully. (Out of direct scope for R&D).

The 'Concept Validation Methodology' is most applicable to the phases V1, V2 and V3 of the Concept Lifecycle Model. V0 is considered as pre-requisite information for validation to commence. During the later phases of Pre-operational (V4) and Operational (V5) different methodologies than those proposed here will be required (e.g. The V model)."

The E-OCVM also explains how the Case-Based Approach and the Structured Planning Framework play a role in each of the phases of the Concept Lifecycle Model. The EC project CAATS II aims the further development of the Case-Based Approach in the E-OCVM.

The iFly project addresses phases V0 (ATM needs) and V1 (Scope). Phases V2-V5 fall outside the scope of the iFly project. By the end of the iFly project, however, it makes sense to provide some further details of the follow-up activities to be foreseen within phases V2 and V3.

3.3 Structured Planning Framework

Following [E-OCVM, 2007] the following applies to V0 (ATM needs). The V0 relevant information on performance needs and constraints is considered as being generated away from the R&D environment and is continuously updated by teams involved in monitoring ATM performance. It is essential pre-requisite information that the validation process will need in order to show how a concept addresses both a performance need and circumvents known constraints. The candidate concepts are also considered as being generated elsewhere. The E-OCVM validation process does not generate concepts, it evaluates concepts.

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 Experimental Needs"	2.1	Identify stakeholder acceptance criteria and performance 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.

More specifically, the following steps are covered in V1:

- Step 0: State concept and assumptions (including problem description)
- Step 1: Set validation strategy (when evidence is needed to help determine strategy, then move to steps 2 through 5).
- Steps 2 through 4 may be used where exercises are needed to help determine a suitable strategy, e.g. fast time modelling activities to help identify the scale of the problem in different airspace or airports.
- Step 5 will collect any evidence from the exercises that will be used as input to the validation strategy. Supporting 'cases' will be created during this step. These cases will collect stakeholder issues and will identify where evidence will be required, and this feeds into the validation strategy.

As soon as a concept has been chosen for a specific application, then the follow-on validation moves to phase V2 (Feasibility). This validation phase falls outside the scope of the iFly project. However, based upon the outcomes of the iFly project, it should be possible to make sound choices regarding the applicability of the iFly developed A^3 concepts for further

development and validation in phase V2 (feasibility). In line with this, by the end of the iFly project, a validation plan for phase V2 will be developed.

4 Safety validation in E-OCVM perspective

Unfortunately, the relation between the various aspects of safety validation and safety case building at one hand, and the E-OCVM life-cycle phases and the structured planning framework at the other hand, are not well defined yet. The aim of this section is to improve the understanding of this relationship, using material from [RESET D6.1, 2007]. First, three safety perspectives are briefly described in sub-Section 4.1. Sub-Section 4.2 shortly describes the safety case development process. Subsequently, sub-Section 4.3 explains the difference between risk allocation and safety risk feedback to design and how this relates to E-OCVM phases. Sub-Section 4.4 further explains safety risk assessment feedback based ATM design.

4.1 Safety validation

Safety is a general notion, which deserves attention from three different ATM perspectives:

- Safety perception (e.g. by pilot, controller, passenger, human society, etc.). An ATM design that is perceived as being unsafe will not easily be accepted by the pilots and controllers involved. Fact is that their positive perception about the safety of an ATM design is a training and deployment critical requirement. By its very nature, however, safety perception is a subjective notion, and therefore insufficient to really guide the approval of safety-critical changes in ATM. Moreover, the safety perception by passengers and human society can not be identified on the basis of an ATM design.
- Dependability of a technical system (e.g. an automation support system, an aircraft navigation system, a satellite based communication system) denotes a collective term used to describe the availability performance and its influencing factors, reliability performance, maintainability performance and maintenance-support performance [ISO8402, 1994]. Metrics for dependability elements have been widely studied in literature for technical systems (e.g. [Laprie, 1995]; [DAAS, 1995]) and are in use e.g. by the JAA [JAR 25.1309, 1994] and Eurocontrol [EATMP SAM, 2004].
- Accident risk, e.g. for 1st (crew), 2nd (passengers) and 3rd parties (external persons) in air transport. Accident risk metrics are commonly in use for human controlled safety-critical operations in chemical and nuclear industries, and in civil aviation. Two well known ICAO-adopted accident risk metrics are for an aircraft to collide either with another aircraft during en-route phase, or with fixed obstacles during landing. Risk may also be expressed in economic terms (e.g. [Jones-Lee&Loomes, 1995]) or societal risk (e.g. [Milloy, 1998]). For reviews of various accident risk metric possibilities in air transport see [Moek&al, 1997]; [ICAO, 1998].

Safety validation is the process aimed to validate[1] the safety of a particular operation. Depending on the user requirements, safety validation 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.

[1] 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?"

[SAFMAC, 2006] has developed a set of safety validation quality 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. The set consists of indicators for each of 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

A full listing of these safety validation quality indicators is provided in Annex A.

4.2 Safety Case development

Prior to putting a new design in operation, i.e. prior to starting E-OCVM phase V5, an adequate Safety Case has to be produced in phases V3 and V4. And such a safety case has to be maintained and updated in phase V5 and beyond. Eurocontrol's Safety Case Development Manual [SDCM, 2006] provides an overview of a proposed methodology for the construction and development of Safety Cases. This Safety Case Development Manual provides guidance on the development of Safety Cases as a means of structuring and documenting the demonstration of the safety of an ATM service or new / modified System (including airspace, equipment, people and procedures).
The Manual is intended for use by those, employed on projects or in service-provider organisations, who have to:

- Produce Safety Cases – e.g. safety practitioners;
- Approve Safety Cases – e.g. programme managers and heads of ATSUs;
- Review Safety Cases – e.g. safety department staff.

The aim is to achieve sound, well-presented Safety Cases through the adoption of a logical, rigorous, consistent and accurate approach that is based on good safety practice.
Whereas the Manual should aid the process of developing and presenting a Safety Case, it cannot give assurance of the validity of the end product, and it does not, therefore, relieve its users of their responsibility to provide such assurance. The Manual does not provide guidance on how to carry out a safety assessment rather it describes how to present the results of a safety assessment, in the context of a Safety Case. As the Manual is intended to be used within the framework of a Safety Management System (SMS), it does not address questions, such as what is a change and when should a Safety Case be produced – these are assumed to be addressed by the SMS. Rather, the starting point for the Manual is the point at which it has been decided to produce a Safety Case for a particular ATM service or change.

Broadly, the Safety Case is the documented assurance (i.e. argument and supporting evidence) of the achievement and maintenance of safety. It is primarily the means by which those who are accountable for service provision or projects assure themselves that those services or projects are delivering (or will deliver), and will continue to deliver, an acceptable level of safety. As the main objective of safety regulation is to ensure that those who are accountable for safety discharge their responsibilities properly, then it follows that a Safety Case which serves the above primary purpose should also provide an adequate means of

obtaining regulatory approval for the service or project concerned. In the context of a Safety Management System, the Safety Case can be a means of documenting and recording the safety of a service or system. Conversely, the implementation of a Safety Management System would provide evidence to support a Safety Case.
The development of a Safety Case is not an alternative to carrying out a Safety Assessment, rather, it is a means of structuring and documenting a summary of the results of a Safety Assessment, and other activities (e.g. simulations, surveys etc), in a way that a reader can readily follow the logical reasoning as to why a change (or on-going service) can be considered safe.

Safety Cases may come in many forms but most, if not all, can be thought of as falling into one of two categories, as follows:

- those which are used to demonstrate the safety of an on-going service – these are known herein as Unit Safety Cases; and
- those which are used to demonstrate the safety of a substantial change to that service (and/or underlying system) – these are known herein as Project Safety Cases.

The two categories are interrelated, as explained below.
An ATSU (or other major, safety-related service / facility) may decide to produce, and maintain, a (Unit) Safety Case in order to show that the on-going, day-to-day operations are safe and that they will remain so indefinitely. A Unit Safety Case would include typically an a priori safety assessment (to show that service / system is predicted to be safe), together with the results of safety audits, surveys and operational monitoring (to show that, up that point in time, it actually has been safe). It should also demonstrate that processes are in place to ensure that all future changes to the ATSU's system will be managed safely through, inter alia, Project Safety Cases.
An ATSU (or other responsible organisation) may also decide to produce a Project Safety Case when a particular substantial change to an existing safety-related service / system (including the introduction of a new service / system) is to be undertaken. A Project Safety Case would normally consider only those risks created or modified by the change and rely on an assumption (or evidence from the corresponding Unit Safety Case) that the pre-change situation is at least tolerably safe. Project Safety Cases are used to update, and are usually subsumed into, Unit Safety Cases.

The Safety Case Development Manual provides guidance based on experience gained on the development of Safety Cases by EUROCONTROL on a wide range of EATM Programmes. It is intended to be applicable also to other environments – e.g. service provision. The guidance covers the following areas:

- determining the Safety Criteria;
- constructing a Safety Argument, using a recognised notation that is considered to be good practice – i.e., Goal-structuring Notation (GSN);
- general issues concerning gathering, collating, assessing and presenting Safety Evidence;
- specific issues concerning Evidence of Safety Requirements determination;
- general issues concerning Safety Requirements satisfaction;
- developing a Safety Plan;
- deciding the format, structure and layout of a Safety Case;
- verifying the Safety Case;

– ESARR compliance.

The Safety Case Development Manual also provides guidance on what to look for in developing and reviewing a Safety Case by means of a Safety Case Developers and Reviewers Checklist.

4.3 Risk allocation vs. Risk assessment feedback to design

In [CAATS D1.4-II, 2006] the following three different aims of safety assessment approaches have been identified:

- A pure risk assessment approach. This term is reserved for a process which intends to answer the question "How safe is this air traffic operation?". Typically, this process is done just to build a safety case. True safety case development applies to E-OCVM phase V4 (Pre-operation). In aviation industry such a safety case often is referred to as an SSS (System Safety Specification).
- A pure allocation approach. With this, we refer to an approach in which an overall Target Level of Safety (TLS) is in some way crunched down into requirements for the constituting functional elements (controller, pilot, particular technical systems, etc.). The feedback from the safety analysts to the ATM designers typically consists of:
  - safety objectives derived from a TLS, per functional element,
  - safety requirements, per functional element,
  - suggestions for mitigating means, per functional element,
  - recommendations for concept improvement, per functional element,
  - checks that all requirements are taken into account, per functional element.

  Typically, this process is driven by and done in parallel with the development of the concept, such that the feedback is timely and iteratively taken into the life cycle of the concept. This pure allocation approach can be applied during E-OCVM phases V2 (feasibility) and V3 (integration). In aviation industry it also is common practice to develop during phase V3 the PSSS (Preliminary SSS). Based on the experience gained through the EC-sponsored project MFF and the safety assessment methodology used in that project (i.e. mainly ED-78A), it has become clear that such pure allocation approach has some good and some less good characteristics for application in ATM.
- A risk assessment feedback approach. This is a combination of both pure risk assessment approach and allocation approach. It both answers the question "How safe is the air traffic operation design?", and it provides and indication of which operational factors contribute most to risk, and the influence of safety requirements posed upon technical systems. The risk assessment feedback approach is of use from during V1 (scope) on, and continues to be of use during phases V2 (feasibility) and V3 (integration).

It is important that safety analysts and those who commission the safety assessment are aware of the differences of these three approaches, especially in terms of the type of results. The first approach provides a risk assessment; the second and third approaches are ways to provide feedback to operation designers. The choice for one of these approaches should be made at the beginning of the assessment, as the methodology to be applied, the kind of results and techniques to be used and the collection of information about the operation depend on the approach to be used.

A pure risk assessment approach aims to give an assessment of the actual risk of the total operation, including all interactions and interfaces between the different operational elements. This risk can be compared with the TLS in order to see how safe the operation actually is and what the margins are. A direct comparison between applications with respect to safety is also

possible. A limitation of a pure risk assessment approach is that there is no information about what is causing any mismatch between TLS and risk level.
A (pure) allocation approach does not aim to assess the risk of the total operation, but it aims to assess the safety requirements and objectives to be posed on major elements of the design. As a consequence, in comparison with a pure risk assessment approach, a (pure) allocation approach can be performed without the need to perform systematic evaluation of all interactions between the major elements; also without the need to assess the safety impact of safety requirements. Because there are multiple ways in which requirements are allocated in choices about which major element in the design should realise which safety requirement or objective (e.g., in terms of equipment redundancy or training levels), the safety analysts involved are expected to make design choices. For example, the allocation of requirements to human and procedure elements is subject of discussion.
The aim of a risk assessment feedback approach is to combine the advantages of the (pure) allocation approach and the (pure) risk assessment approach, i.e. provide both the risk of the total operation and requirements feedback to the design. In order to assess the risk of the total operation, all interactions between the main elements have to be taken into account. The risk assessment level can be compared with the TLS in order to see how safe the operation actually is and what the margins are. A direct comparison between applications with respect to safety is also possible. In case the TLS is not (or only just) reached, potential mitigating measures and safety requirements are derived that take into account the interactions between the different elements.
In terms of expertise required the three methods also differ: Both in a pure risk assessment approach and in a risk assessment feedback approach, the roles of safety analysis and concept design are separated, so that the safety analysts do not have to step in the shoes of the concept designers and do not have to analyse the safety of their own recommended improvements. In a (pure) allocation approach, the roles of safety analysis and concept design are mixed. Some safety analysts may be uncomfortable to assess the safety of their own recommendations or improvements, in particular since potential mitigating measures may involve potential new hazards.
For each particular application these differences should be timely weighed in order to decide which type of approach is more appropriate for the application considered.

4.4 Safety Risk Assessment Feedback-based ATM design

The aim of this section is to further elaborate the approach of safety risk assessment feedback to ATM design. Within this approach, the principle aim of any safety assessment, and one of the major outputs of a safety assessment process, is an issue that does not always 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. The aim of the whole safety assessment is to learn something, so that the design can be improved. This interaction between design and assessment is depicted in Figure 5: .

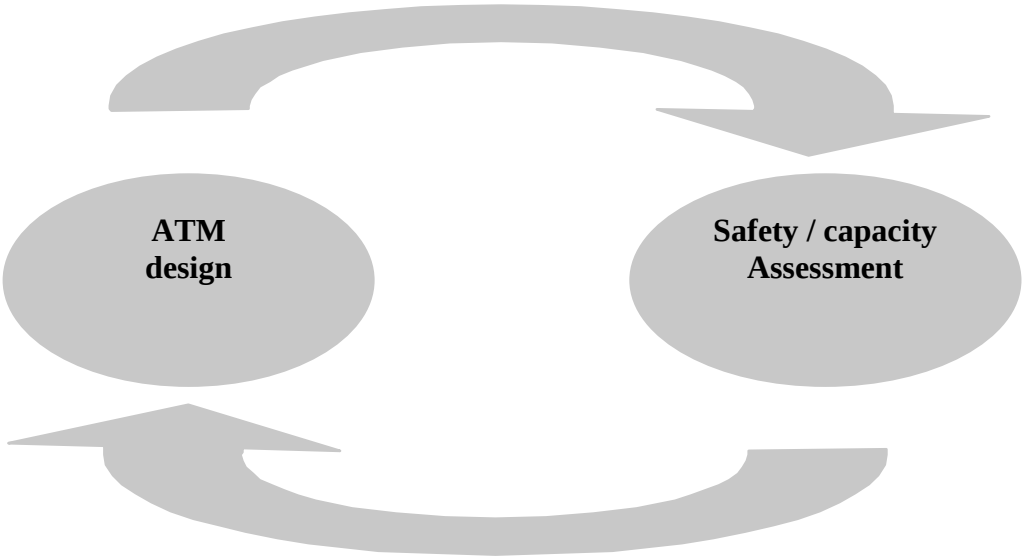

Figure 5: Feedback-based ATM design

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. The second party that can benefit from structured feedback are safety assessors themselves, 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. The third party that can benefit from feedback are designers and developers of new concepts. Such people are not necessarily habitual readers of safety assessments, and yet 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. This also includes effective communication to bridge the gap between safety assessment and safety perception. 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.

5 iFly and E-OCVM Phase V0; ATM needs

As a prerequisite of concept validation, the ATM performance needs and barriers must be identified. To complete the validation of the concept, the concept must show that it can alleviate these barriers enough thus enhancing ATM performance to the anticipated required level. Throughout the iFly project, ATM is being seen as including all ASAS aspects, including air crews. Because this deviates to a certain degree from the ICAO definition of ATM, the approach taken within iFly is to refer to wide-sense-ATM or to advanced air traffic concept.

For the iFly project there are several relevant and valuable input sources of ATM needs available. First of all there are the SESAR established ATM needs; these are reviewed in Sub-Section 5.1. 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. Sub-Section 5.2 reviews ATM relevant accident statistics. Sub-Section 5.3 presents the ICAO en-route TLS for mid-air collision risk, Sub-Section 5.4 addresses ESARR4 and EC common requirements relative to ICAO's TLS. Sub-Section 5.5 addresses Human Factors oriented studies. Sub-section 5.6 reviews SESAR safety observations regarding separation provision and collision avoidance. Sub-Section 5.7 shows which WP's are expected to make use of which identified ATM needs.

5.1 SESAR established ATM needs

The main conclusions and result are taken from [SESAR D2, 2006]. The proposed SESAR Vision is to achieve a performance based European ATM System, built in partnership, to best support the ever increasing societal and States', including military, expectations for air transport with respect to the growing mobility of both citizens and goods and all other aviation activities, in a safe, secure, environmentally sustainable and cost-effective manner. Central to achieving this Vision, is the business trajectory concept of placing the best overall outcome of individual flights at the heart of the ATM network. The SESAR Vision is to govern the future ATM system based on a framework existing of the following five key elements:

a. The "Performance Framework"
b. The "Business Management Framework"
c. The "Institutional and Regulatory Framework".
d. The "Business Trajectory Concept"
e. The "Role of the Human in ATM"

a. The Performance Framework

The Performance Framework will be used to drive management decisions towards achieving the Vision. The SESAR Consortium has started to address the definition of the 2020 performance by setting initial targets. These will be continuously refined within the lifetime of the ATM Master Plan. ATM Performance covers a broad spectrum of aspects, which are represented through eleven Key Performance Areas (KPAs) [ICAO Doc 9854]. The KPA targets represent initial indicative values (working assumptions), subject to further analysis and validation. All KPAs are interdependent and will be the basis for impact assessment and consequent trade-off analysis for decision-making in the subsequent SESAR Milestone Deliverables. Four KPAs, directly linked to the achievement of the proposed SESAR Vision are described below. The other seven KPAs (Efficiency, Flexibility,

Predictability, Security, Access and Equity, Participation, Interoperability) are addressed in [SESAR D2, 2006].

Capacity

In accordance with the political vision and goal, the ATM target concept should enable a 3-fold increase in capacity which will also reduce delays, both on the ground and in the air (en-route and airport network), so as to be able to handle traffic growth well beyond 2020.
The deployment of the ATM target concept should be progressive, so that only the required capacity is deployed at any time. The target for Capacity deployment is that the ATM System can accommodate by 2020 a 73% increase in traffic from the 2005 baseline, while meeting the targets for safety and quality of service KPAs (Efficiency, Flexibility, Predictability).

Safety

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.

Environment

The overall aim is that ATM will deliver its maximum contribution to the environment:

- Achieve the implicit emission improvements through the reduction of gate-to-gate excess fuel consumption addressed in the KPA Efficiency.
- Minimise noise emissions and their impacts for each flight to the greatest extent possible.
- Minimise other adverse atmospheric effects to the greatest extent possible. Suitable indicators are yet to be developed.

Cost-Effectiveness

The overall aim is to halve the total direct ATM costs. The working assumption for the Cost Effectiveness target is to progressively reduce the total direct European gate-to-gate ATM 2005 costs per flight [EUROCONTROL Performance Review Report 2005] to a value in 2020 that halves the costs per flight. Notwithstanding this 2020 target, continuing cost improvement should be sought after 2020. This “ATM Performance Framework” provides a common basis to ensure the effectiveness of the ATM System through a dynamic relationship between European States, institutions and regulations (“Institutional and Regulatory Framework”), and all aircraft operators, air navigation service providers and airports working in partnership to match the targets (“Business Management Framework”).

b. The ATM Business Framework

This should manage all phases of the European ATM System lifecycle:

- Establishes ATM Performance Partnership between all stakeholders including roles and targets based on a shared set of values, priorities, and network interactions.
- Improve from the present fragmented decision making process to the execution of a common and shared ATM strategic planning
- Implement the concept of “Business Trajectory”.

c. The Institutional and Regulatory Framework

The aim is to ensure that societal expectations are met:

- Consists of a simple and well-structured set of regulations and regulatory actions allocated at global, European or national level, whilst continuing to rely on Member States for enforcement.
- Needs to be flexible so it easily adapts to business and societal changes.

d. The Business Trajectory Concept

The Business Trajectory is the basis for all partners in the ATM System design, planning and operation to enable the optimal performance of the flight, resulting in optimisation of the whole European network performance.

The "Business Trajectory" is the representation of an airspace user's intention with respect to a given flight. It is aimed at guaranteeing the best outcome for the flight as seen from the airspace user's perspective. At the airspace user's discretion this outcome may be with respect to the minimum time for the flight, the minimum cost, or any other characteristic of the trajectory. Although perhaps not as obvious as for commercial airlines, business aviation, general aviation and the military also have their own "business" intention. The emphasis is on "intention" and naturally, all must be carried out in a manner which guarantees the safety of life and takes into account the need to meet environmental and security requirements.

e. The role of the human in ATM

- The human will remain the most flexible and creative element to direct the performance of the overall ATM System including the management of threats, errors and unpredictable events.
- Changes in the operation of the future ATM System will involve a change in the human roles which requires an extensive change management process throughout the entire process of system development, design and implementation.
- The European Civil Aviation Sectorial Social Dialogue Committee is considered as a first promising step to a European social dialogue.
- 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.

5.2 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%)

Table 3 The distribution of separation-related accidents (light), fatal accidents (grey) and fatalities (black) over various accident types.

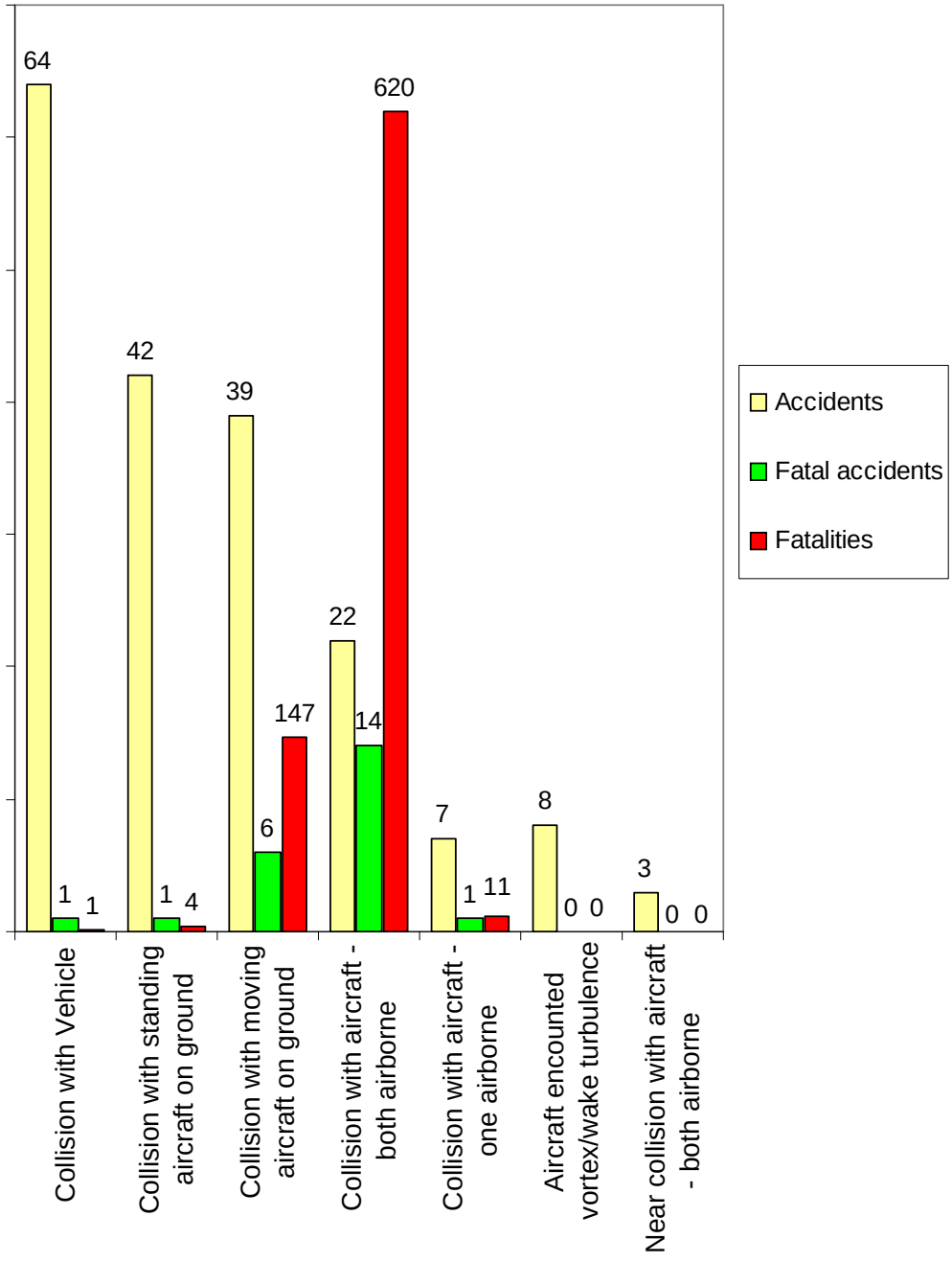

Table 3 shows that 11 out of 185 accidents, i.e. 6%, are not constituted by a collision but by last moment manoeuvring to avoid a collision or by hitting the wake vortex turbulence from another aircraft. Moreover, these non-collision accidents did not cause any fatality. The number of separation related 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 4 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 4 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

5.3 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.

5.4 ESARR4 and EC common requirements

[RESET D6.1, 2007] has reviewed ATM related safety requirements by ESARR, EC and SRC and compared this with ATM related 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 for ATM related safety requirements.

- 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 for ATM related safety requirements. 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.

5.5 Human Factors oriented studies

It is widely recognized, e.g. [Wise et al., 1993], that a key element of validation is addressing human factors aspects of a novel developed concept such as considered within iFly. As has been explained in [iFly D2.1, 2007], several EC funded programs have been working on different aspects of airborne self separation concept and considerable progress has been achieved. In the human factors domain NLR/NASA Free Flight, and two EC funded projects

– INTENT and Mediterranean Free Flight (MFF) – have contributed significantly to human factors issues in airborne self separation. Probably the best overview available about these issues is in the recent paper by Ruigrok, & Hoekstra (2007). Main findings of these studies confirm that:

(1) free flight crews is a viable concept,
(2) airborne primary separation responsibility offers several times higher traffic density compared to ground control primary responsibility,
(3) human-machine interfaces developed in the projects have been favourably rated by the flight crews.

[iFly D2.1, 2007] considers these as resolved issues from the human factors point of view. In addition, there are a number of unresolved issues that need further human factors studies. For example, how should information necessary for conflict detection and resolution be presented to pilots both in state-based (using ground speed, track and vertical speed of aircraft involved) and intent-based (using the flight plans of aircraft involved) mode and behaviour of flight crews in both information display modes has been evaluated. The results obtained leave open the question, which mode of information presentation is better and "the best of both worlds" – combination of state-based conflict detection and resolution with a limited amount of intent information needs further studies. Also an open question is how to use the rules of conflict resolution by aircrews: "The pilots in the MFF experiments were not in agreement on the use of priority rules versus co-operative conflict detection and resolution in the state-based conflict detection and resolution system. Some liked priority rules, some liked the co-operative approach. From an analytical point of view, this issue is also not clear yet. And because issues of information display are open, the favourable ratings of human-machine interfaces received in previous research have not solved all the interface issues yet. And still, pilot workload issues during self separation remain open – in conflict situations the demands of the situation may exceed the resources available to the pilot and in problem-free situations suboptimal workload may decrease the level of pilot activation.

5.6 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
  - 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 UAVs/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.

5.7 Which iFly WP addresses which ATM needs?

The ATM needs material that has been collected within the previous sub-Sections includes material that was not even known at the time the iFly work description was finalized. This may very well mean that some of these ATM needs are not yet explicitly mentioned within the existing iFly technical work descriptions. The table below provides a rough indication which iFly WP's are expected to take (part of) which ATM needs identified into account (based on the WP descriptions in the Technical Annex to the contract).

Table 5. Within which iFly WP's are the relevant ATM needs addressed?

ATM needs	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8	WP9	WP10
Performance frame	Yes	-	Yes	Yes	Yes	Yes	Yes	Yes	-	-
Business frame	-	-	-	-	-	Yes	-	-	-	-
Institutional	-	-	-	-	-	Yes	-	-	-	-
Business trajectory	Yes	-	-	-	Yes	-	-	Yes	-	-
Human role	Yes	Yes	-	Yes	-	-	Yes	Yes	-	-
Accident statistics	-	-	-	-	-	-	Yes	-	-	-
ICAO TLS	-	-	-	-	-	-	Yes	-	-	-
Common Requirm's	-	-	-	-	-	-	Yes	-	Yes	-
Human Factors	-	Yes	-	-	-	-	-	-	-	-
Safety Observations	-	-	-	-	-	-	-	-	-	-

This table shows that (based on the Technical Annex) currently the SESAR safety observations [SESAR D3-safety, 2007] are not foreseen to be covered by iFly. In order to improve on this, if appropriate scientific expertise can be made available amongst the iFly partners, then an initial liability study will be performed within WP10.1.

6 Concept development prior to E-OCVM Phase V1

Prior to starting E-OCVM Phase V1 (Scope) the concept to be evaluated need to be developed 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

Within the iFly project two advanced air traffic concepts will be developed:
- A^3 ConOps will be developed within WP1
- A^3 ConOps refinement will be developed within WP8.

In addition, airborne technology requirements will be developed within WP9.

These developments will be based on human responsibility studies that will be performed within WP2, prior to the subsequent WP1 and WP8 studies. Details of these studies are provided in Sub-Section 6.1, Sub-Section 6.2, Sub-Section 6.3 and Sub-Section 6.4 for WP2, WP1, WP8 and WP9 respectively.

6.1 Human responsibility studies within WP2

WP2 Objectives

The objective is to develop the anchor points for the A^3 ConOps development that can be defined from the human responsibility and goal setting, and later to verify how well these anchor points are used in the A^3 ConOps, and where needed to provide potential solutions.

Work package 2 is divided into two parts: “airborne responsibilities” and “bottlenecks and potential solutions”.

Part A: Airborne responsibilities

1. To identify current and new responsibilities of cockpit crew during en-route phase of flight
2. To analyse Situation Awareness, Information, Communication and cockpit crew tasks.

Part B: Bottlenecks and potential solutions

3. To identify bottlenecks in responsibility issues.
4. To define potential solutions.

Description of work

Changes in the air traffic management system irrevocably cause changes in the role of the human involved in that system as a result of technological changes. When the system becomes more and more automated, a shift in tasks and responsibilities of the human controlling the system occurs. The human operator – in case of an aircraft, the cockpit crew – is responsible for the actions and tasks he/she performs. This responsibility is a core issue in (aerospace) operations, because it determines who makes what decision and can take action if required without being required to request permission from another actor.

Important in this, is that many functions in autonomous aircraft operations will be supported by automation on the flight deck and there should be a balance between automation and responsibility. As long as the human remains responsible for the resulting actions of the human-machine system, he/she also needs to be able to control the system. When the system is fully automated and the human

is out of control, it is not possible to hold him/her responsible for the resulting outcomes. On the other hand, automating (parts of) a system can also support the human to maintain control over the situation, especially in complex systems like an aircraft.
Therefore, human responsibility is a key factor in determining to what extent a system can be automated. In an air traffic management environment this responsibility can be spread among the airborne and ground side of the system. Current developments in ATM show a shift towards a more decentralised system, with increasing tasks and likely more responsibilities for the airborne side, i.e. the cockpit crew. This side forms the starting point for the current project, therefore the question that arises is: "What responsibilities can be assigned to the airborne side of the system assuming a new task distribution implied by autonomous ATM?" Work package 2 considers these issues in more detail.

Part A: Airborne responsibilities

WP 2.1 To identify current and new responsibilities of the cockpit crew during the en-route phase of the flight
An analysis should be carried out to identify the responsibilities of the cockpit crew during the en-route phase of the flight. To be able to define a new air traffic management concept, first of all, current responsibilities of the cockpit crew have to be identified.
It also needs to be identified what tasks the crew currently has to perform during (the en-route phase of) the flight. A task analysis helps to provide this information. This analysis needs to be performed on an operational scenario of the en-route flight phase, to map out the tasks of the cockpit crew during this phase.
In addition to the description of tasks, also a description of the goals of the crew is valuable as input for the identification of responsibilities. These goals provide the framework within which the crew performs the actions. Important goals are, for example, to ensure a safe and efficient flight.
This provides a basic overview of the current situation. The already existing responsibilities can be adopted into the new concept. To achieve a highly automated air traffic management system, the possibility for assigning more responsibilities to the airborne crew than in the current situation, should also be investigated. This is a necessity for a more autonomous operation of the aircraft. The proposed concept departs from the view that as much as possible, responsibilities should be assigned to the airborne side, not to the ground side. Therefore, issues that are in current operations accounted for by the ground, are likely to be assigned to the airborne crew and become their responsibilities.
Responsibilities of a cockpit crew go beyond issues related to air traffic management only. For example, the cockpit crew is responsible for monitoring the functioning of the system (i.e. the aircraft). A shift in responsibility with respect to ATM issues should never result in conflicts with other responsibilities. Therefore, consequences of this responsibility shift should be reviewed and resulting bottlenecks – when consequences appear to be outside acceptable limits – need to be identified. All aircraft types that take part of en-route air traffic (e.g. civil aircraft, UAVs, military aircraft) are taken into account.

WP 2.2 Situation Awareness (SA), Information, Communication and Pilot Tasks
The aim of this WP is to identify the SA to be maintained by the crew, the information and communication needs and the tasks of the controller. This involves several questions to be taken into account.
While total situation awareness is prohibitively costly in terms of both financial and human workload costs, it is recognized that there will be some minimum prerequisites for satisfactory situation awareness for iFly crews. How does one create active and engaged iFly pilots who are sensitive not only to their own aircraft but also those around it. How does the system support iFly pilots so that they can make the appropriate delegation of tasks with the iFly automation, particularly when the pilots are not exactly sure what their neighbours will be doing? How will an iFly crewstation effective support recognition and projection of future automation actions? How will they be able to intuitively

predict how neighbouring iFly aircraft will perform?

How will an iFly crewstation support information abstraction and distillation to the appropriate level for effective iFly operation. How will iFly support salient mode transitions so the pilots will know how their own aircraft & those around them will be behaving so they know what to expect next?

What type of human cognitive support will be necessary for the flight crew to be an effective iFly participant? What will be the best way of presenting system uncertainty "information" to the flight crew? Considering the potential state-of-the-art of avionic technology and the supportable human-system interface 1) what will the flight crew information needs be & to what extent will it be possible to meet or support those needs. How does one make clear the level of responsibility and related roles as a function of time & place in the system? How does one assure that the information available matches with the responsibility at the moment? What does the crewstation need from system wide information management and what will crew contribute? What new roles will the flight crew take on & how will the needs of those tasks to be supported?

Part B: Bottlenecks and solutions

The results of WP2 part A are used as input for definition of the operational concept in WP1. WP1 uses this to develop the A^3 ConOps. Next WP2 part B assesses A^3 ConOps against human responsibilities identified in WP2 part A. WP2 part B tasks will reveal, where bottlenecks with respect to human responsibility issues arise. Finally, potential ways for solving these bottleneck issues have to be developed.

WP 2.3 To identify bottlenecks in responsibility issues

After having identified what responsibility issues arise in a highly automated ATM environment, bottlenecks can be identified where mitigating measures are required. The aim of WP2.3 is to identify such bottlenecks.

Issues like safety and capacity should be investigated to identify when these bottlenecks arise. As these should remain within acceptable limits, maybe changes in task allocation is needed when constraints resulting from human responsibilities are reached. Task analysis serves as input to the task allocation process. Within the task allocation, tasks are allocated to the airborne crew and to the supporting airborne or non-airborne systems.

As the initial options for allocating responsibility to the cockpit crew have been identified in WP1.3, WP2.3 will be searching for inconsistencies in these options and will question them, to prepare the second design cycle for improvement of the A^3 concept. This in contrast with the common way, in which first a concept is fully developed regarding the technical systems, and after this, responsibilities are assigned to the applicable actors.

WP2.4 To develop potential human factors improvements for A^3 ConOps

After WP2.3 has identified human factors responsibility bottlenecks where additional ground support is required (in the tasks and functions, where it is impossible to allocate all responsibility to the airborne side of the system), the goal of WP2.4 is to develop potential mitigating human factors related measures of these bottlenecks for the A^3 ConOps. These potential mitigating human factors measures are taken into account for the refinement of A^3 within WP8.1.

6.2 A³ ConOps development within WP1

WP1 Objectives

- This work-package will develop an autonomous aircraft advanced concept (A^3) including an airline strategy concept for autonomous aircraft operations, using state-of-the-art aeronautics research and Technology results. The airline strategy concept offers opportunities for airlines to harness the greater autonomy to improve on customer service.
- The A^3 concept developed here focuses on the en-route phase of flight, for a potential shift into autonomous en-route operations in airspace that is busy according current standards.

Description of work

The purpose of WP1 is to:

- Develop the overall A^3 concept of operations (ConOps).
- Describe the airline strategy concept for the A^3 environment.

WP1 takes advantage of state-of-the-art research results obtained in previous aeronautics research projects like Free Flight, Intent, CARE-ASAS, Freer, MFF, AFAS, M-AFAS. In addition it leans significantly on the pilot responsibility and cognition analysis performed within WP2.

The tasks performed in this WP will be consolidated around an A^3 concepts that is targeted to:

- Optimize the performance of airlines with autonomous aircraft.
- Maximise the safety level in the en-route phase at 3 times current busy levels.
- Ensure the interoperability of the various A^3 services.
- Improve on customer services by making effective use of the autonomy.

The WP is organised in three sub-WPs. WP1.1 called "High level ConOps" describes the available options towards autonomous en-route aircraft advanced operations. WP1.2 called "Airline Strategy Concept" will describe the strategy concept for airline operations in an autonomous aircraft environment. WP1.3 called "ConOps" will describe the overall concept of operations within the autonomous en-route ATM environment.
The activities performed in these sub-WPs are:

WP1.1 A^3 High-level ConOps

This sub-WP outlines the vision in terms of potential solutions towards a shift to autonomous aircraft operations en-route which might or might not lead to the required capacity breakthrough.
The activities outlined in the High-level ConOps are:

- Assessment and definition of a common basis, e.g.: terminology and functionality.
- Identification of candidate concepts or concept elements from previous state-of-the-art aeronautics Research & Technology projects.
- Operational environment description of autonomous aircraft operations en-route.

WP1.2 A^3 Airline Strategy Concept

Air traffic demand is highly dependent on customer demand. Customers want to fly directly to their destination within their preferred time constraints. Airlines try to accommodate these preferences mainly within hub-and-spoke strategies resulting in periodic peak demand levels. This kind of

behaviour needs to be accommodated within the autonomous aircraft environment. Any limitations of the autonomous aircraft operations can induce delays and reductions in connection probabilities. On the other hand, autonomous aircraft operations offers also new opportunities to improve on the effectiveness of hub-and-spoke strategies, for instance through improved arrival timing. So it needs to be identified how airlines will react with their movement strategies.

This sub-WP identifies

- Novel ways for airlines to make effective use of autonomous aircraft operations.
- Airline operational environment description for autonomous aircraft operations.
- Identifying a strategy concept for airline operations in an autonomous aircraft environment.
- Identifying the expected benefits and limitations for the proposed strategy concept.

WP1.3 A^3 ConOps

The ConOps obtained by integration of candidate concepts or concept elements into an overall concept of operations, aims at the safe accommodation for all types of autonomous aircraft operations en-route, including new or non conventional types of air traffic, and supported by ground CFM service and Airline Operational Centres (AOC) provision only.

The overall potential solution is then to be analysed as follows in order to assure completeness and proper understanding towards the mathematical modeling:

- Holistic view on the proposed concept, identifying interactions with other ATM flight cycles and concepts.
- Identification the providers of the potential solutions. It is expected that the on-board solutions will rely to a large extend on advanced automation of the cockpit.
- Identification of services for the different technologies such as ADS, GNSS and CPDLC.
- Critical self assessment by A^3 designers:
  - ❖ Identification and understanding of the assumptions made for the proposed concept.
  - ❖ Identification of the expected benefits to ATM areas such as safety, capacity limitations, actor workload and actor error tolerance, etc.
  - ❖ Identification of expected limitations of the proposed solutions.
  - ❖ Possible problems and weak-points created through the introduction of the proposed solution and their mitigation.
  - ❖ Identification of potential safety issues.

The outcomes of the WP7 pre-brainstorming are used to further improve the A^3 ConOps. In addition, on the first consolidated draft critical review comments are actively collected from WP3, WP5, WP6 and WP7. These comments are taken into account in the finalization of the A^3 concept.

6.3 A³ ConOps refinement within WP8

WP8 Objectives

The objective of WP8 is to refine the A^3 ConOps and to develop a vision how A^3 equipped aircraft can be integrated with SESAR concept. The key inputs to be used for the refinement are the innovative methods and architecture implications that are delivered by WP3, WP4 and WP5. In addition, use is made of feedback from WP2, WP6 and WP7. The WP will make use of results from global work performed by AP23 on ConOps (AP23 D3) and ASAS operational elements (AP23 D4) and integrate them. Because the requirements for the airborne and ground segments have to be developed following conventions and specific background from both domains, WP8 is performed in parallel with an airborne counterpart design WP9. The objective of WP8 thus also is to describe the non-airborne requirements in support of A^3 equipped aircraft, working in close collaboration with WP9. Together, WP8 and WP9 form the second design cycle.

The rationale to be followed within iFly is that with increasing traffic levels the advantage of effective ATM ground support will increase, and at a certain traffic demand level there even is an absolute need to receive the best possible ATM ground support. Half a year prior to the end of the iFly project, the safety and cost-efficiency assessment results from WP6 and WP7 shall provide the key information on the performance of A^3 operations as a function of traffic demand levels. From that moment on the A^3 ConOps refinement cycle shall scale its design and the corresponding requirements to this full spectrum of traffic demand levels. In order to safely accommodate even higher traffic demand levels, then there is a theoretical need to make use of ground ATM support.

In practice, however, and also in line with the SESAR deployment sequence (D4), a possible gradual implementation of ASAS self separation into SESAR en-route environment is needed. In support of this gradual implementation view, within WP8 also a vision is developed regarding the SESAR necessary elements that are in support of A^3 equipped aircraft. Again this leans significantly on the analysis of pilot responsibility, cognition and bottlenecks as will be performed within WP2. This is done in close cooperation with the airborne needs addressed within WP9, the strategic ground ATM options identified by SESAR, and the innovative methods developed in WP3, WP4 and WP5. Moreover, this includes the development of an integrated concept for air traffic flow management (ATFM). ATFM role may both increase and may go beyond the current centralized approach if this allows to take advantage of the opportunities autonomous aircraft operations will give in optimizing Gate-to-Gate operations for the airlines, but it focusses on en-route phase of flights. WP8 also takes SESAR ConOps and strategy into account as far as these have been developed at the start of WP8 tasks. Moreover, WP8 may deviate from SESAR ConOps or strategy if such deviation is properly justified.

Description of work

The sub-WPs performed in this WP will be consolidated around the A^3 concept that is targeted to:

- Ensure A^3 equipped aircraft within SESAR to accommodate the target safety levels at busy traffic levels up to 6 times current busy en-route traffic levels.
- Ensure the interoperability between the A^3 airborne and SESAR ground services.
- Improve on effective usage of available capacity within the A^3 environment.

The WP is organised in four sub-WPs. WP8.1 takes the lessons learned from the mathematical WPs and integrates them into the ConOps for the A^3 environment. WP8.2 called "Distributed Air Traffic Flow Management" will describe a concept for flow management which supports and emphasises the philosophy behind autonomous aircraft operations. WP8.3 develops a vision for fitting "A^3 equipped aircraft within SESAR". Finally, in WP8.4 called "Non-airborne requirements in support of A^3 environment" will identify the prerequisites for the non-airborne support to A^3 (e.g. FOC, ATFM, SWIM, COM, etc.). Finally, WP8.5 identifies options for the potential mitigation of any cost-benefit or safety bottlenecks identified within WP6 and WP7.

WP8.1 Integration of mathematical results

The options still open within the A^3 ConOps are now further analysed and consequentially reduced by taking advantage of the outcomes of the innovative methods under development by WP3, WP4 and WP5 for the:

- Methods for the timely prediction of complex conflict conditions. (WP3)
- Methods to systematically identify and analyse potential safety critical multi-agent situation awareness inconsistency conditions in distributed designs. (WP4)
- Advanced multiple conflict resolution methods which have the potential to be formally validated on their performance. (WP5)

Likewise, bottlenecks with respect to human responsibility identified in A^3 ConOps from WP2B how these can be solved have to be integrated. WP8.1 will be performed in parallel and in close collaboration with the OSED development within WP9. For the A^3 ConOps this means WP8.1 will produce an updated version, with innovative results from WP3, WP4, WP5 and feedback from WP2B and WP9.1.

WP8.2 Distributed Air Traffic Flow Management Concept

In the current day ATM system several layers of traffic management are incorporated. Each layer has the objective to avoid overloading the subsequent layers with too much traffic load. The layer ATFM in the current ATM system has the objective to not overload any airports and sectors with too much traffic by balancing capacity and demand. In the current day ATM system capacity is limited due to a number of factors like runway separation minima, airport weather conditions, and controller workload limitations. Demand is dependent on for instance airline hub strategies and customer preferred flying times.

Although controller workload is less of an issue, with autonomous aircraft operations a number of the current bottlenecks will not dissolve automatically. If these capacity limits are not addressed well, pilots may find themselves flying circles in a stack. So there will clearly be a need for a form of ATFM which works in conjunction with autonomous aircraft operations.

In an environment with autonomous aircraft operations new opportunities arise to reduce delays imposed by ATFM. Shorter feedback loops allows for better adjustment to uncertainties. Fewer bottlenecks make it easier to find solutions accommodating for real 4D ATM. Furthermore, ATFM can within limits assure through CDM and demand management that the traffic levels for autonomous aircraft operations do not exceed above set restrictions.

The objective of this sub-WP is to describe an air traffic flow management concept which builds upon the philosophy behind autonomous aircraft operations and breaks away from the centralised doctrine of current flow management.

In this sub-WP the following activities are foreseen:

- Identifying the interactions of autonomous aircraft operations and highly automated ATC with air traffic flow management
- Identify problems and weak-points from air traffic flow management interacting with autonomous aircraft operations together with their mitigations.
- Develop an air traffic flow management concept which emphasises the advantageous of autonomous aircraft operations.

WP8.3 A^3 equipped aircraft within SESAR

This sub-WP develops the vision in terms of A^3 equipped aircraft can operate within SESAR. At all times it is important for WP8.3 to keep all options open for which there does not exist yet a good rationale to make design decisions. Within WP8.3 the ConOps vision will be based on an analysis of how the A^3 ConOps impacts strategic ATM options identified by SESAR on issues such as:

- Mixed equipage
- 4D ATM including a systematic way of working with uncertainty
- Integrating ATFM (from WP8.2)
- CDM & demand management
- Human roles and responsibilities
- System Wide Information Management (SWIM)

Due to the nature of A^3 operation, the A^3 ConOps is purely focussed on the airborne-side and under the demanding condition that all aircraft are A^3 equipped. In practice, however, a gradual increase of equipped aircraft will be the case. Therefore the aim of WP8.3 is to develop a vision how the gradual increase of A^3 equipped aircraft within the SESAR settings should fit best. This way, WP8.3 aims to contribute to the SESAR Operational Evolution regarding ATM Service Level 5 conceptualizing the implementation of 4D Trajectory and the introduction of ASAS Self-Separation in a mixed mode environment. This will answer the question how well the A^3 thinking combines with the gradual implementation of autonomous aircraft operations, where IFR and AFR aircraft will coexist for a period of time.

WP8.4 Non-airborne Requirements in support of A^3 equipped aircraft

This sub-WP produces the final WP8 report on the A^3 from a non-airborne operations perspective. To accomplish this, the A^3 ConOps of WP8.1 is combined with the WP6 and WP7 results in assessing the A^3 operation. This allows to place the A^3 ConOps in the perspective of the traffic demand levels that are supported by the A^3 operation alone and within SESAR perspective respectively. And this has significant impact on the non-airborne requirements of A^3 operations (e.g. FOC, SWIM, ATFM, COM, etc). As before, the rationale of addressing the requirements from a non-airborne perspective will be documented, and these are developed in collaboration with the airborne perspective experts working in WP9. Some of the non-airborne requirements that will be looked at include:

- Communication requirements (voice, data-link)
- Data accuracy, integrity and availability
- Automated ground surveillance support requiements
- Network security
- Pre-flight requirements
- Arrival and Departure Management requirements
- Flow management requirements

Where applicable, the derivation of requirements will be ensuring traceability and consistency with

other WP (i.e. WP9).

WP8.5 Potential mitigating measures of bottlenecks

This task identifies options for the mitigation of any critical safety or economy bottlenecks on A^3 ConOps that have been revealed by:

- Cost-benefit analysis of the viability of the autonomous aircraft concept (WP6).
- Accident risk assessment of advanced autonomous aircraft operation from (WP7).

The results are mitigating measures, which are not solved by system requirements WPs (WP8.4 or WP9.4).

WP8.5 starts with a workshop where the main bottlenecks identified by WP6 and WP7 are presented to, and discussed with the WP8.5 design team and invited experts. This should lead to a proper understanding what exactly the bottlenecks are of the A^3 ConOps as developed. Subsequently it is again a role of operational concept experts, rather than safety capacity experts, to use expert-judgement type of process in order to identify the potential mitigating measure options, and subsequently select the preferred ones. For the identification of potential mitigating measures, structured brainstorms are being held with the design team and invited experts. As a follow up, the design team has the task to select the preferred options, and explain how this should improve the A^3 ConOps.

6.4 A³ Airborne system design requirements study within WP9

WP9 Objectives

The objectives of WP9 are summarised as follows:
1. To define the preliminary Safety and Performance Requirements (SPR) of the Autonomous Aircraft Operations Advanced Concept (the 'A³' concept) described in WP1; and
2. To use the results of the SPR process to define preliminary system design requirements for an airborne system to support the 'A³' concept.

The SPR process will be carried out in line with the methodology described in EUROCAE document ED-78A "Guidelines For Approval of The Provision and Use of Air Traffic Services Supported By Data Communications". The SPR process comprises preparation of an Operational Safety Assessment (OSA) and an Operational Performance Assessment (OPA) based on the 'A³' concept as described in an Operational Services and Environment Description (OSED). System design requirements can then be derived from the OSA and OPA results. The aim of WP9 is to perform a preliminary cycle through ED78A, with focus on strategic results and identifying the required technology pull.

For the purposes of exploitation, WP9 will produce a preliminary set of requirements. Follow on work will be required to increase the maturity level of the Safety and Performance Requirements and the System Design Requirements. The WP will identify, at the end of the work, areas that will need to be further analysed from a performance standpoint.

Description of work

WP9.1 – Operational Services and Environment Description (OSED)
This WP will develop an OSED describing the operational environment and the air traffic services required to support the 'A³' concept described in the A³ ConOps delivered by WP1 and refined by WP8.1. To accomplish this, use is made of the A³ ConOps from WP1, the output of WP2, and the innovative methods from WP3, WP4 and WP5.

The OSED will be written based on an operational services and environment information capture process that co-ordinates the information among stakeholders. The process captures elements related to a defined CNS/ATM system, and will be expected to include aspects such as aircraft equipage, ATS provider technical system, communication service provider systems, and procedural requirements. The work performed in AP23 on OSED building from ASAS operational elements and ASAS avionics support functions will be analysed and used if necessary.

The OSED will identify the operational services and their intended operational environments and includes the operational performance expectations, functions, and selected technologies of the related CNS/ATM system. During this process, a high-level Functional System Description will also be developed.

The OSED facilitates the formulation of technical and procedural requirements based on operational expectations and needs and will be updated as necessary throughout the co-ordinated requirements determination process.

WP9.2 – Operational Safety Assessment (OSA)
The OSA will be an assessment of the safety of the autonomous ATM concept described in the OSED produced in WP9.1, and will consist of two interrelated processes. First is an Operational Hazard Assessment (OHA) and second is an Allocation of Safety Objectives and Requirements (ASOR).

Operational Hazard Assessment (OHA)
The purpose and scope of the OHA will be to qualitatively assess operational hazards related to the advanced autonomous ATM concepts, and to establish safety objectives and candidate safety requirements related to each identified hazard.

Operational services will be examined to identify and classify hazards that could adversely effect those services. Hazards are classified according to a standardised classification scheme based on hazard severity, taking into account human factors. Overall safety objectives will be assigned to the identified hazards.

Allocation of safety objectives and requirements (ASOR)
Based on the results of the OHA, the ASOR will allocate safety objectives to organisations, develop risk mitigation strategies that are shared by multiple organisations, and allocate safety requirements to those organisations.

Requirements are allocated to the CNS/ATM system elements that provide the functional capability to perform the service and the stakeholders in control of or responsible for each of the elements. Understanding the interactions of the operational services, procedures, and airspace characteristics will assist in the identification of failures, errors, and/or combinations thereof that contribute significantly to the hazards identified in the OHA. It may be that the allocation requires updating based on feedback from other processes.

WP9.3 – Operational Performance Assessment (OPA)
The main objective of the OPA will be to provide the airborne performance requirements for A^3 operations. The definition and setting of the performance requirements are linked to the primary performance objectives (extracted from the OSED produced in WP9.1), as well as to safety analysis in WP9.2 and operational needs (WP1, WP8.1).

Performance requirements are the minimum operational requirements ensuring that end users can expect the same quality of services for the autonomous ATM concept in any airspace where the various elements of the CNS/ATM system meet these requirements.

WP9.4 – Airborne System Design Requirements
This sub-WP will use the results of the OPA and OSA processes to define the preliminary system design requirements for airborne systems to support the A^3 operations. In addition, interim results of the assessment cycle (WP6 and WP7) and the second design cycle (WP8) will be taken into account and a first estimation of their impact on airborne requirements will be provided. WP9.4 will as well collaborate with WP8 which will develop requirements from the non-airborne perspective.

7 E-OCVM Phase V1: Scope

E-OCVM Phase V1 (Scope) aims to evaluate which traffic demand levels can safely be accommodated by the proposed A^3 concept, and aims to gain 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.

7.1 Assessment feedback to design

The objective of iFly is to explore the boundaries of airborne self separation in en-route air-space including the preliminary assessment of the A3 ConOps. More specifically a safety risk assessment will be performed within WP7, and a cost-benefit assessment will be performed within WP6. The outcomes of these assessments feedback to the refined A^3 ConOps within WP8, and the A^3 airborne technology requirements analysis by WP9.

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.

In order to evaluate the initial feasibility of the A^3 ConOps, a qualitative human factors assessment will be performed by WP2.3, and an overall safety assessment will be performed using the TOPAZ safety risk assessment methodology (see Appendix B3) within WP7. The TOPAZ methodology supports both a qualitative first round as well as a Monte Carlo (MC) simulation second round. For the iFly project the MC simulation approach is particularly of relevance. The outcomes of this study are used as inputs to the ED78A assessment that will be performed within WP9. This way the MC simulation results form a powerful source towards getting the technical requirements right from an overall safety perspective. The outcomes of the human factors and safety assessments also form input to the cost-effectiveness study that will be performed within WP6.

7.2 Safety study within WP7

WP7 Objectives

The aim of this WP is to assess 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. In order to accomplish this assessment through Monte Carlo simulation, the complementary aim of this WP is to further develop the innovative HYBRIDGE speed up approaches in rare event Monte Carlo simulation.

Description of work

The work is organised in the following four sub-WPs:

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. 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.

WP7.2: Monte Carlo speed up methods

Within HYBRIDGE novel Monte Carlo simulation speed up techniques have successfully been developed and applied. 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.

WP7.3 Perform Monte Carlo simulations

Monte Carlo simulations are performed to assess flight efficiency and collision risk of the A^3 operation. Because the Monte Carlo simulation speed up will not yet be at its maximum, at this stage of the work, the results will be of point estimation type. On the basis of these point estimation results, an intermediate report is produced which shows the assessment results obtained for A^3 operation.

WP7.4 Final report

This is the finalization of the report. The safety results now include sensitivity analysis and bias and uncertainty assessment. In the final report it is also shown which are the main safety bottlenecks of the A^3 operation evaluated.

7.3 Cost-benefit study within WP6

WP6 Objectives

The objective of this work package is to assess the cost-benefit of en-route A^3 operations. The operational benefits and costs associated with the introduction of A^3 the concept will be identified and the conditions under which the proposed concept is viable will be determined. The WP will assess the cost related to the avionics baseline used by early ADS-B implementations in Europe and USA,(regulated respectively by EC surveillance implementing rule and FAA ADS-B mandate)

Description of work

A necessary prerequisite for the practical implementation of any new Air Traffic Management (ATM) concept is the estimation of its potential positive (benefits) and negative (costs) impacts. Given the fact that the introduction of a new ATM concept may generate positive and negative impacts to all stakeholders, e.g. airlines, air traffic management organizations, air traffic controllers, etc., it is important to be able to consider in the evaluation process the goals and priorities of all affected parties. Furthermore, it is important to stress here the fact that the estimation of the various types of impacts, e.g. capacity, work load, delays, etc., due to the introduction of the autonomous aircraft concept should be quantified on the basis of alternative scenarios. Given, the organizational complexities arising from the participation of multiple stakeholders in the Air Traffic Management System, it is important to study the institutional and organizational issues associated with the implementation of the autonomous aircraft concept as well as to identify a strategy for the optimum implementation of the proposed concept. The WP will estimate the avionics package cost as part of the analysis, using avionics industry experience, and by making comparison against the baseline set by regulations for ADS-B driving the ADS-B equipage both in Europe and in the USA.

For methodological purposes the proposed work will be divided into the following sub-WPs:
WP6.1: Development of a methodological framework for cost-benefit analysis.
WP6.2: Institutional and organizational analysis for the implementation of the autonomous aircraft operations.
WP6.3: Data collection for cost-benefit analysis
WP6.4: Cost-benefit analysis and results assessment

WP6.1: Development of a methodological framework for cost-benefit analysis

This sub-WP will develop the overall methodological framework for assessing the cost-benefit of the proposed A^3 concept. The objectives and priorities of all involved stakeholders will be identified and indicators measuring the objectives of all stakeholders will be determined. Alternative scenarios, representing different achievement levels of the performance of the autonomous aircraft concept will be developed in cooperation with the involved stakeholders. The cost-benefit analysis will be based on the established scenarios through the quantification of the expected financial and operational impacts.

WP6.2: Institutional and Organizational issues

The objective of this sub-WP is to identify institutional and organizational barriers and enablers for the effective implementation of the autonomous aircraft concept. The relationship among the various ATM participants will be analyzed and the organizational and institutional changes needed for the successful implementation of the autonomous aircraft concept will be identified.

WP6.3: Data collection for cost-benefit analysis

The objective of this sub-WP is to collect the data needed for the implementation of the cost-benefit analysis. The collection of data will relate to : i) traffic projections for the horizon of analysis, ii) conversion of operational impacts into monetary benefits and costs, and iii) financial analysis data, i.e. interest rates , inflation rates etc.

WP6.4: Cost- benefit analysis and results assessment

In this sub-WP the data collected in WP6.3 will be analyzed using the cost-benefit technique identified in WP6.1. The results of the cost-benefit analysis will be assessed and the viability of the autonomous aircraft concept will be determined, on the basis of the analyzed scenarios. The interim results of this analysis will provide input to WP8.4

7.4 Planning of V1 activities within iFly WP7 and WP6

In order to ensure that E-OCVM is well applied during each of the phase V1 relevant WPs of iFly, within each of these WP's the structured planning framework (section 3.3) will be followed. Within WP7 this will be done as part of the WP7 scoping report D7.1a. Within WP6 this will be done as part of the report D6.1 on the methodology framework for cost-effectiveness analysis. As much as is possible, this will be done in line with the state of the art of the E-OCVM extensions that are currently under development within EC projects RESET and CAATSII.

8 Concluding remarks

This report has placed the iFly project into the E-OCVM validation framework. In order to accomplish this, first a high level description of the iFly project has been given in Section 2. Next, in Section 3, an overview of the E-OCVM framework has been given. Because the current E-OCVM framework does not describe the relation with the safety case building process well, in Section 4, the safety validation and safety case development elements are placed in the E-OCVM phases. Subsequently, in Section 5, the E-OCVM phase V0 (ATM needs) has been performed through collecting material from various complementary sources. Next, Section 6 shows the development of iFly specific operational concepts, one of which will be evaluated during E-OCVM phase V1. Finally, in Section 7 it is shown which foreseen WPs fit within the E-OCVM phase V1 (scope).

By the end of the iFly project an E-OCVM based validation plan will be produced which makes explicit which aspects need to be addressed in the follow up work.

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. 2005]	H.A.P. Blom, K.M. Corker, S.H. Stroeve, On the integration of human performance and collision risk simulation models of runway operation, Proc. 6th USA/Europe Air Traffic Management R&D Seminar, Baltimore, USA, 27-30 June 2005.
[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.
[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.

LIST OF REFERENCE DOCUMENTS	
Short Reference	**Author / Organisation, Title, Edition, Date and Reference**
[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.
[EATMP SAM, 2006]	Air Navigation System Safety Assessment Methodology, SAF.ET1.ST03.1000-MAN-01, Edition 2.1, November 2006. 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. Blom 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**
[Everdij et al., 2007]	M.H.C. Everdij, H.A.P. Blom, and G.J. Bakker, Modelling lateral spacing and separation for airborne separation assurance using Petri nets, In: Transactions of The Society for Modeling and Simulation International, Volume 83, Number 5, May 2007, pp. 401-414.
[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.

LIST OF REFERENCE DOCUMENTS	
Short Reference	**Author / Organisation, Title, Edition, Date and Reference**
[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.
[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.
[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.
[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. Safety validation quality indicators

Safety validation is the process aimed to validate[2] 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

[2] 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 B. Main Safety Assessment Methodologies

This annex, based on [CAATS D1.4-II, 2006], gives a brief description of the main safety assessment methodologies currently in use by the ANSPs considered in this report. These methodologies are:

- EATMP SAM
- ED-78A
- SEE Framework, in combination with TOPAZ accident risk assessment methodology

B.1. EATMP SAM

[EATMP SAM, 2004] presents a general overview of an Air Navigation Systems safety assessment from an engineering perspective. The safety assessment activities are sub-divided into:

- Risk Assessment activities, to identify hazards, and evaluate the associated risk tolerability,
- Safety engineering activities, to select, validate and implement counter measures to mitigate these risks, and
- Safety assurance activities, which involve specific planned and systematic actions that together provide confidence that all relevant hazards and hazard effects have been identified, and that all significant issues that could cause or contribute to those hazards and their effects have been considered.

The objective of the methodology is to define a means for providing assurance that an Air Navigation System is safe for operational use. It is an iterative process conducted throughout the system development life cycle, from initial system definition, through design, implementation, integration, transfer to operations, to operations and maintenance. The iterative process consists of a Functional Hazard Assessment (FHA), a Preliminary System Safety Assessment (PSSA) and a System Safety Assessment (SSA), see figure below.

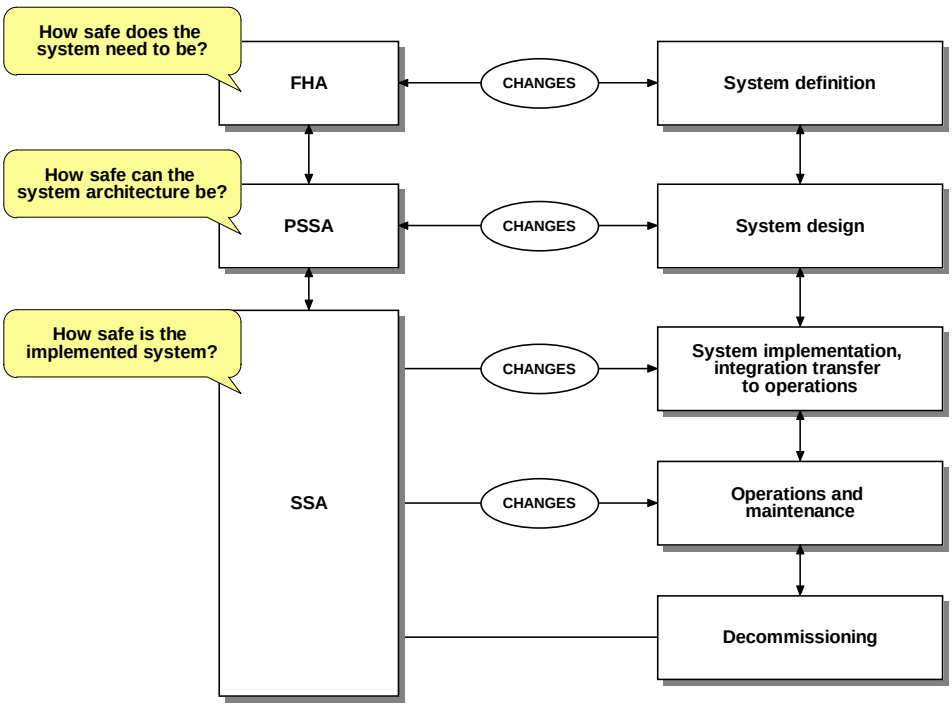

Figure 6: Relationships between the safety assessment process and the overall system life cycle

The objectives of the FHA, the PSSA and the SSA are:

- Functional Hazard Assessment (FHA) analyses the potential consequences on safety resulting from the loss or degradation of system functions. Using service experience, engineering and operational judgement, the severity of each hazard effect is determined qualitatively and is placed in a class 1, 2, 3, 4 or 5 (with class 1 referring the most severe effect, and class 5 referring to no effect). *Safety Objectives* determine the maximum tolerable probability of occurrence of a hazard, in order to achieve a tolerable risk level.
- Preliminary System Safety Assessment (PSSA) determines that the proposed system architecture is expected to achieve the safety objectives. PSSA examines the proposed system architecture and determines how faults of system elements and/or external events could cause or contribute to the hazards and their effects identified in the FHA. Next, it supports the selection and validation of mitigation means that can be devised to eliminate, reduce or control the hazards and their end effects. System *Safety Requirements* are derived from Safety Objectives; they specify the potential means identified to prevent or to reduce hazards and their end effects to an acceptable level in combination with specific possible constraints or measures.
- System Safety Assessment (SSA) collects arguments, evidence and assurance to ensure that each system element as implemented meets its safety requirements and that the system as implemented meets its safety objectives throughout its operational lifetime (till decommissioning), i.e. the *Safety Assurance & Evidence Collection* step. It demonstrates that all risks have been eliminated or minimised as far as reasonably practicable in order to be acceptable, and subsequently monitors the safety performance of the system in service. The safety objectives are compared with the current performances to confirm that they continue to be achieved by the system.

The FHA (edition 2.0) and PSSA (edition 2.0) are described in significantly more detail in [EATMP SAM, 2004]. A first edition for SSA is described in [EATMP SAM, 2004], although currently no guidance material is publicly available for the SSA safety assurance and evidence collection step (this is under development).
Next, the activities to be followed for FHA, PSSA and SSA are detailed.

Functional Hazard Assessment (FHA)

The FHA part of reference [EATMP SAM, 2004] gives more details on the FHA steps and provides guidelines on how to perform each step. It lists for each FHA step the objectives, the input necessary, the major tasks and the output provided, see the table below.

Table 6: EATMP SAM FHA objectives and major tasks

FHA STEP	OBJECTIVES	MAJOR TASKS
F1. FHA Initiation	• Develop a level of understanding of the system, its operational environment and, if appropriate, its regulatory framework, sufficient to enable the safety assessment activities to be satisfactorily carried out.	F1.1. Gather all necessary information describing the system.
		F1.2. Review this information to establish that it is sufficient to carry out the FHA.
		F1.3. If not available, describe the operational environment of the system.
		F1.4. Identify and record assumptions made.
		F1.5. Formally place the input information under configuration management.
F2. FHA	• Define the objectives and scope of the FHA, the activities to be carried out, their deliverables, their schedule	F2.1. Identify and describe the more specific activities for each FHA step.
		F2.2. Submit the FHA plan to peer review to provide assurance of its suitability.

FHA STEP	OBJECTIVES	MAJOR TASKS
Planning	and the required resources.	F2.3. Submit the FHA plan for comment or approval to interested parties (including regulatory authorities), as appropriate.
		F2.4. Formally place the FHA plan under configuration management.
		F2.5. Disseminate the plan to all interested parties.
F3. Safety Objectives Specification	• To identify all potential hazards associated with the system; • To identify hazard effects on operations, including the effect on aircraft operations; • To assess the severity of each hazard effect; • To specify Safety Objectives, i.e. to determine the maximum frequency of hazard's occurrence; • To assess the overall foreseen (future) risk associated to introducing the change or new system.	F3.1. For each system function and combination of functions, identify potential hazards
		F3.2. For each system function and combination of functions, identify hazard effects
		F3.3. For each system function and combination of functions, assess the severity of hazard effects.
		F3.4. For each system function and combination of functions, specify Safety Objectives.
		F3.5. For each system function and combination of functions, assess intended aggregated risk.
F4. FHA Evaluation		
F4a. FHA Verification	• To demonstrate that the set of Safety Objectives meet the Organisation Safety Target, i.e. the overall acceptable level of risk.	F4a.1. Review and analyse the results of the FHA process.
F4b. FHA Validation	• To ensure that the Safety Objectives are (and remain) correct and complete; • To ensure that all safety-related assumptions are credible, appropriately justified and documented.	F4b.1. Review and analyse the Safety Objectives to ensure their completeness and correctness;
		F4b.2. Review and analyse the description of the operational environment to ensure its completeness and correctness;
		F4b.3. Review, analyse, justify and document safety-related assumptions about the system, its operational environment and its regulatory framework to ensure their completeness and correctness.
		F4b.4. Review and analyse traceability between functions, failures, hazards, hazard's effects and Safety Objectives.
		F4b.5. Review and analyse the credibility and sensitivity of derived Safety Objectives to assumptions and risk.
F4c. FHA Assurance Process	• To provide assurance and evidence that all FHA activities (including FHA Verification and FHA Validation) have been conducted according to the plan; • To ensure that the FHA process as described in the FHA Plan is correct and complete.	F4c.1. Ensure that FHA steps are applied;
		F4c.2. Ensure that assessment approaches are applied;
		F4c.3.Ensure that all outputs of the FHA steps, including FHA Verification, FHA Validation and FHA Process Assurance are formally placed under configuration management;
		F4c.4. Ensure that any deficiencies detected during FHA Verification or FHA Validation activities have been resolved;

FHA STEP	OBJECTIVES	MAJOR TASKS
		F4c.5. Ensure that the FHA process would be repeatable by personnel other than the original analyst(s);
		F4c.6. Ensure that the findings have been disseminated to interested parties;
		F4c.7. Ensure that the outputs of the FHA process are not incorrect and/or incomplete due to deficiencies in the FHA process itself.
F5. FHA Completion	• To record the results of the complete FHA process; • To disseminate these results to all interested parties	F5.1. Document the results of the FHA process (including the results of FHA Verification, FHA Validation and FHA Process Assurance activities);
		F5.2. Formally place the FHA documentation under configuration management;
		F5.3. Disseminate the FHA documentation to all interested parties.

Preliminary System Safety Assessment (PSSA)

The PSSA part of reference [EATMP SAM, 2004] gives more details on the PSSA steps and provides guidelines on how to perform each step. It lists for each PSSA step the objectives, the input necessary, the major tasks and the output provided, see the table below.

Table 7: EATMP SAM PSSA objectives and major tasks

PSSA STEP	OBJECTIVES	MAJOR TASKS
P1. PSSA Initiation	• Develop a level of understanding of the system design framework, its operational environment and, if appropriate, its regulatory framework, sufficient to enable the safety assessment activities to be satisfactorily carried out.	P1.1. Gather all necessary information describing the system design;
		P1.2. Review this information to establish that it is sufficient to carry out the PSSA;
		P1.3. Update the Operational Environment Description (OED) of the system (add PSSA-related data to FHA-related data);
		P1.4. Identify and record assumptions made;
		P1.5. Formally place all information under a documentation control scheme.
P2. PSSA Planning	• Define the objectives and scope of the PSSA, the activities to be carried out, their deliverables, their schedule and the required resources	P2.1. Identify and describe the more specific activities for each PSSA step in a PSSA Plan;
		P2.2. Submit the PSSA plan to peer review to provide assurance of its suitability;
		P2.3. Submit the PSSA plan for comment or approval to interested parties (including regulatory authorities), as appropriate;
		P2.4. Formally place the PSSA plan under a documentation control scheme;
		P2.5. Disseminate the PSSA plan to all interested parties.
P3. Safety Requirements Specification	• Derive Safety Requirements for each individual system element (People, Procedure and Equipment)	P3.1. For each function and combination of functions, refine the functional breakdown;
		P3.2. For each function and combination of functions, evaluate system architecture(s);
		P3.3. For each function and combination of functions, apply risk mitigation strategies;
		P3.4. For each function and combination of functions, apportion Safety Objectives in to Safety Requirements;
		P3.5. For each function and combination of

PSSA STEP	OBJECTIVES	MAJOR TASKS
		functions, balance/Reconcile Safety Requirements.
P4. PSSA Evaluation		
P4a. PSSA Verification	• To ensure that Safety Requirements meet Safety Objectives.	P4a.1. Review and analyse the results of the PSSA process.
P4b. PSSA Validation	• To ensure that the Safety Requirements are (and remain) correct and complete; • To ensure that safety-related assumptions are (and remain) correct and complete.	P4b.1. Review and analyse Safety Requirements to ensure their completeness and correctness;
		P4b.2. Review and analyse the description of the operational environment to ensure its completeness and correctness;
		P4b.3. Review, analyse, justify and document critical assumptions about the system design, its operational environment and its regulatory framework to ensure their completeness and correctness;
		P4b.4. Review and analyse traceability between Safety Objectives and Safety Requirements;
		P4b.5. Review and analyse the credibility and sensitivity of Safety Requirements with respect to the Safety Objectives and the assumptions.
P4c. PSSA Process Assurance	• To provide assurance and evidence that all PSSA activities (including PSSA Verification and PSSA Validation tasks) have been conducted according to the PSSA plan; • To ensure that the PSSA process as described in the PSSA plan is correct and complete.	S4c.1. Ensure that (in accordance with the PSSA plan) the PSSA steps are applied;
		P4c.2. Ensure that (in accordance with the PSSA plan) assessment approaches (e.g. success approach, failure approach, use of safety methods and techniques such as Fault-Tree, FMEA, CCA, …) are applied;
		P4c.3. Ensure that (in accordance with the PSSA plan) all outputs of the PSSA steps (including PSSA Validation and Verification output) are formally placed under a configuration management scheme;
		P4c.4. Ensure that (in accordance with the PSSA plan) any deficiencies detected during PSSA Verification or Validation activities have been resolved;
		P4c.5. Ensure that (in accordance with the PSSA plan) the PSSA process would be repeatable by personnel other than the original analyst(s);
		P4c.6. Ensure that (in accordance with the PSSA plan) the findings have been disseminated to interested parties;
		P4c.7. Ensure that (in accordance with the PSSA plan) outputs of the PSSA process are not incorrect and/or incomplete due to deficiencies in the PSSA process itself.
P5. PSSA Completion	• To document and formally place the results of the whole PSSA process under a configuration management scheme; • To disseminate these results to all	P5.1. Document the results of the PSSA process (including the results of PSSA Validation, Verification and Process Assurance activities);
		P5.2. Formally place the PSSA results under a configuration management scheme;

PSSA STEP	OBJECTIVES	MAJOR TASKS
	interested parties.	P5.3. Disseminate the PSSA documentation to all interested parties.

System Safety Assessment (SSA)

The SSA part of reference [EATMP SAM, 2004] gives more details on the SSA steps and provides guidelines on how to perform each step. It lists for each SSA step the objectives, the input necessary, the major tasks and the output provided, see the table below.

Table 8: EATMP SAM SSA objectives and major tasks

SSA STEP	OBJECTIVES	MAJOR TASKS
S1. SSA Initiation	• Develop a level of understanding of the system design framework, its operational environment and, if appropriate, its regulatory framework, sufficient to enable the safety assessment activities to be satisfactorily carried out.	S1.1. Gather all necessary information describing the system implementation, transfer into operation, operation, maintenance and decommissioning;
		S1.2. Review this information to establish that it is sufficient to carry out the SSA;
		S1.3. Update the operational environment description (OED) of the system (add SSA-related OED data to FHA & PSSA-related data);
		S1.4. Identify and record assumptions made;
		S1.5. Formally place all input information under a documentation control scheme.
S2. SSA Planning	• Define the objectives and scope of the SSA, the activities to be carried out, their deliverables, their schedule and the required resources.	S2.1. Identify and describe the more specific activities for each SSA step in a SSA Plan;
		S2.2. Submit the SSA plan to peer review to provide assurance of its suitability;
		S2.3. Submit the SSA plan for comment or approval to interested parties (including regulatory authorities), as appropriate;
		S2.4. Formally place the SSA plan under appropriate documentation control scheme;
		S2.5. Disseminate the SSA plan to all interested parties.
S3. Safety Assurance & Evidence Collection		
S3a. Safety Assurance & Evidence Collection *during Implementation & Integration (including Training)*	To collect evidences and to provide assurance that: • each system (people, procedure, equipment) element as implemented meets its Safety Requirements; • the system as implemented satisfies its Safety Objectives throughout its operational lifetime (till decommissioning); • the system satisfies users expectations with respect to safety; • the risk is acceptable;	S3a.1. Re-assess FHA & PSSA output (process and assumptions);
		S3a.2. Verification that system elements (People, Procedures, Equipment) as implemented meet their SRs;
		S3a.3. Verification that system as implemented can meet its Safety Objectives;
		S3a.4. Verification that risk is acceptable.
S3b. Safety Assurance & Evidence Collection *during*	To collect evidences and to provide assurance that: • each system (people, procedure, equipment) element as implemented meets its Safety Requirements;	S3b.1. Safety assessment of the transfer into operations phase;
		S3b.2. Verification that system elements meet their SRs and that system as transferred into operations meets its Safety

SSA STEP	OBJECTIVES	MAJOR TASKS
Transfer into Operations	• the system as implemented satisfies its Safety Objectives throughout its operational lifetime (till decommissioning); • the system satisfies users expectations with respect to safety; • the risk is acceptable;	Objectives; S3b.3. Validation of the system as transferred to operations with respect to users' Safety expectations; S3b.4. Validation that risk is acceptable.
S3c. Safety Assurance & Evidence Collection *during Operations & Maintenance*	To collect evidences and to provide assurance that: • each system (people, procedure, equipment) element as implemented meets its Safety Requirements; • the system as implemented satisfies its Safety Objectives throughout its operational lifetime (till decommissioning); • the system satisfies users expectations with respect to safety; • the risk is acceptable;	S3c.1. Continuous data collection and monitoring of safety performances with respect to SRs, SOs, assumptions and risk; S3c.2. Safety assessment of maintenance and/or planned interventions.
S3d. Safety Assurance & Evidence Collection *during System Changes (people, procedures, equipment)*	To collect evidences and to provide assurance that: • each system (people, procedure, equipment) element as implemented meets its Safety Requirements; • the system as implemented satisfies its Safety Objectives throughout its operational lifetime (till decommissioning); • the system satisfies users expectations with respect to safety; • the risk is acceptable;	S3d.1. Re-iterate the overall safety assessment process through FHA, PSSA and SSA.
S3e. Safety Assurance & Evidence Collection *during Decommis-sioning*	To collect evidences and to provide assurance that: • each system (people, procedure, equipment) element as implemented meets its Safety Requirements; • the system as implemented satisfies its Safety Objectives throughout its operational lifetime (till decommissioning); • the system satisfies users expectations with respect to safety; • the risk is acceptable;	S3e.1. Assessment of the safety impact on global ANS operations of the system withdrawing; S3e.2. Safety assessment of the decommissioning process.
S4. SSA Evaluation		
S4a. SSA Verification	• To demonstrate that the process followed in collecting the Safety Assurance & Evidence is technically correct.	S4a.1. Review and analyse the results of the SSA process.
S4b. SSA Validation	• To ensure that the Safety Assurance & Evidence are (and remain) correct and complete; • To ensure that all critical assumptions are credible, appropriately justified and documented.	S4b.1. Review and analyse Safety Assurance & Evidence to ensure their completeness and correctness; S4b.2. Review and analyse the description of the operational environment to ensure its completeness and correctness; S4b.3. Review, analyse, justify and document critical assumptions about the system design,

SSA STEP	OBJECTIVES	MAJOR TASKS
		its operational environment and its regulatory framework to ensure their completeness and correctness;
		S4b.4. Review and analyse traceability between SOs/SRs/assumptions/risk and Safety Assurance & Evidence;
		S4b.5. Review and analyse the credibility and sensitivity of Safety Assurance & Evidence wrt to SOs/SRs/assumptions/risk.
S4c. SSA Process Assurance	• To provide evidence that all SSA activities (including Safety Verification and Safety Validation) have been conducted according to the plan; • To ensure that the results – and the assumptions on which they depend - are properly recorded and disseminated for use by those involved in later stages of the development/assessment cycle, and to future system users.	S4c.1. Ensure that (in accordance with the SSA plan) the SSA steps are applied;
		S4c.2. Ensure that (in accordance with the SSA plan) assessment approaches (e.g. success approach, failure approach, use of safety methods and techniques) are applied;
		S4c.3. Ensure that (in accordance with the SSA plan) all outputs of the SSA steps are formally placed under a configuration management scheme;
		S4c.4. Ensure that (in accordance with the SSA plan) outcomes of SSA Validation and Verification activities are formally placed under configuration management;
		S4c.5. Ensure that (in accordance with the SSA plan) any deficiencies detected during SSA Verification or Validation activities have been resolved;
		S4c.6. Ensure that (in accordance with the SSA plan) the SSA process would be repeatable by personnel other than the original analyst(s);
		S4c.7. Ensure that (in accordance with the SSA plan) the findings have been disseminated;
		S4c.8. Ensure that (in accordance with the SSA plan) outputs of the SSA process are not incorrect and/or incomplete due to deficiencies in the SSA process itself.
S5. SSA Completion	• To record the results of the whole SSA process; • To disseminate these results to all interested parties.	S5.1. Document the results of the SSA process (including the results of SSA Validation, Verification and Process Assurance activities);
		S5.2. Formally place the SSA results under a configuration management scheme;
		S5.3. Disseminate the SSA result to all interested parties.

B.2. ED-78A

The EUROCAE ED-78A document [ED-78A, 2000] (identical to the RTCA DO-624), entitled "Guidelines for approval of the provision and use of Air Traffic Services supported by data communications" provides means to establish the operational, safety, performance, and interoperability requirements for ATS supported by data communications, to assess their validity, and to qualify the related CNS/ATM system. It is a single source document that provides guidance for approval of the CNS/ATM system and its operation where coordination is necessary across organizations. The guidance material considers the allocations of the operational, safety, performance, and interoperability requirements to the elements of the

CNS/ATM system. These include ground-based elements, operational procedures, including the human, and aircraft equipage.
The process considered in ED-78A consists of

- approval planning,
- coordination of requirements determination across organizations,
- development and qualification of CNS/ATM systems at the organizational level,
- entry into service, and
- operations using ATS supported by data communications.

The *Coordinated Requirements Determination* process includes the interrelated processes that are coordinated by the stakeholders. These are:

- Operational Services and Environment Information Capture (OSEIC) process delivers an Operational Services and Environment Description (OSED).
- Operational Safety Assessment (OSA), including an Operational Hazard Assessment (OHA) and an Allocation of Safety Objectives and Requirements (ASOR); the output of this process is reported in an Operational Safety and Performance Requirements (SPR) standard
- Operational Performance Assessment (OPA), including Required Communication Performance (RCP) type determination or evaluation (when directly provided in the OSED), Required Communication Technical Performances (RCTP) and human performance determination, and RCTP system elements allocation; the output of this process is reported in an Operational Safety and Performance Requirements (SPR) standard.
- Interoperability Assessment (IA); The output of this process is an Interoperability requirements (INTEROP) standard.

The processes are shown in Figure 7, which also shows the relationships among the guidance material, the OSED, the SPR standard, the INTEROP standard, and other evidence under control of an applicant responsible for one of the approval types. The processes are shown in logical sequence. Recognizing that there may be considerable overlap of processes, the logical sequence is also the recommended sequence.

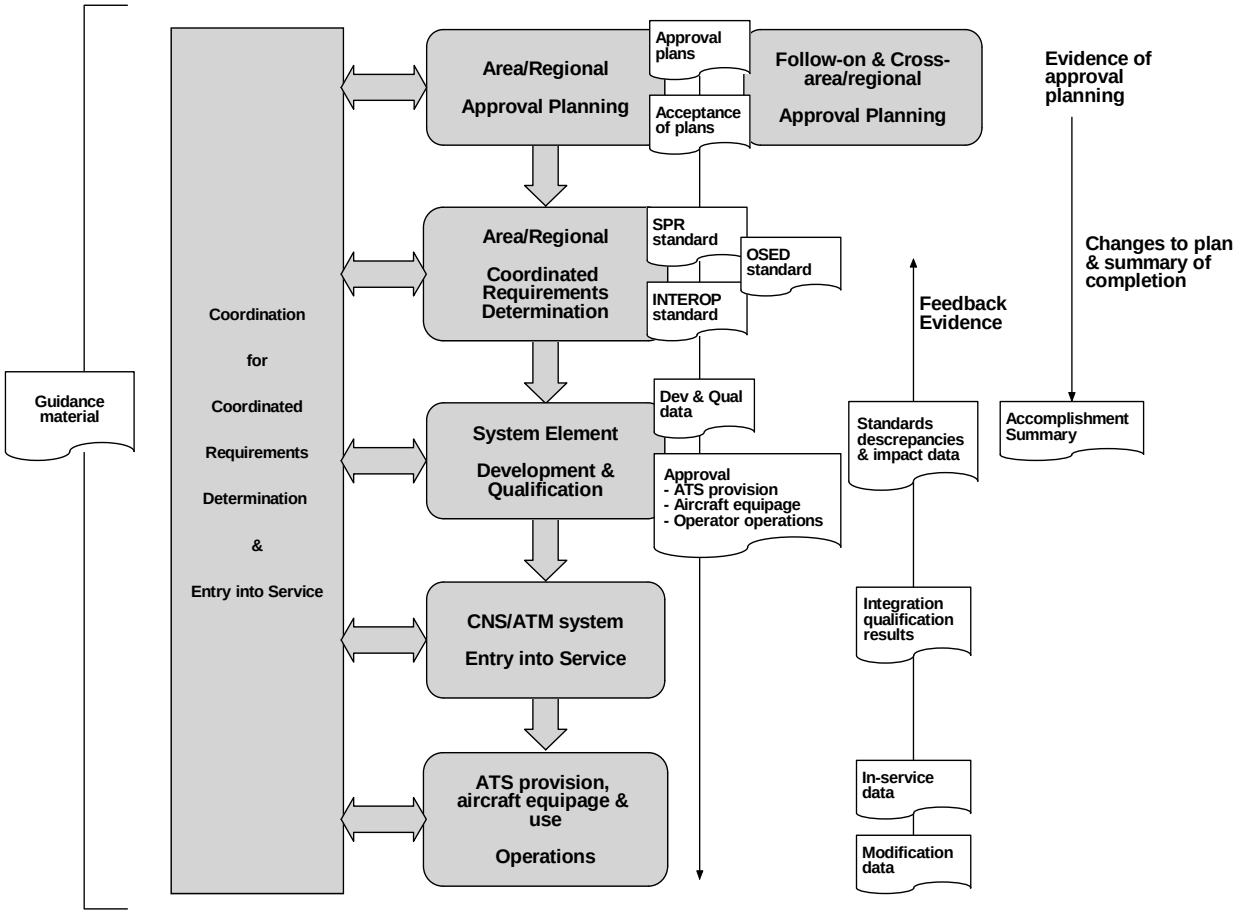

Figure 7: Process for ATS supported by data communications

In the subsequent phases, it needs to be verified and ensured whether all requirements are satisfied. If not, this requires updates and feedback into the Coordinated Requirements Determination. Note that e.g. Development and Qualification are considered iterative processes themselves: including requirements capture, design, integration, validation, verification et cetera.

Operational Safety Assessment (OSA)

The OSA includes an operational hazard assessment (OHA) and an allocation of safety objectives and requirements (ASOR) among the multiple organisations, and is based on the operational services and environment definition (OSED). Their relationship is illustrated in the following figure.

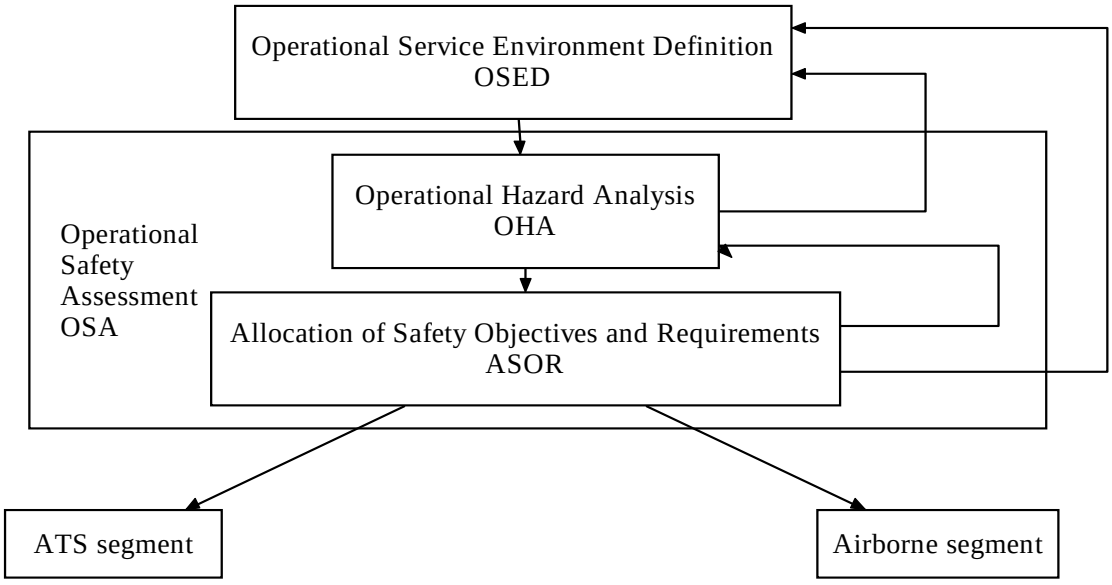

Figure 8: Relationship between ED-78A's OSED, OHA and ASOR processes

In the context of the OSA methodology, the objective of the OSED is to obtain the relevant information for the safety assessment of the CNS/ATM system under consideration. In a wider context, as considered in the RTCA/EUROCAE guidance, the OSED is also used as a basis for assessing and establishing the performance and interoperability requirements.

The purpose of the OHA step is to develop an end-to-end qualitative assessment of potential operational hazards. The next step is the ASOR, i.e. the establishment and allocation of safety objectives and requirements to stakeholders and elements of the CNS/ATM system. These stakeholders include ATS providers, ATS equipment manufacturers, supporting service providers, such as those that provide communication and weather services, aircraft and equipment manufacturers, and operators. The OHA and ASOR are interrelated and iterative processes.

The OHA is a qualitative assessment of the operational hazards associated with the OSED. For the OHA, operational functions are examined to identify and classify hazards that could adversely affect those functions. Based on a high level description of the operational procedures and airborne/ground functional characteristics, the identification of operational hazards should be supported by considerations including:

- functional failure;
- human failure to respond appropriately to functional failure;
- human error or omission during normal use;
- transitional hazards (those that may result by changing over from an existing to new operations);
- external factors (e.g. outages, weather).

Hazards are classified according to a standardised classification scheme based on hazard severity and taking into account effects at the aircraft, air traffic services and operations. The severity classification is independent of the hazard likelihood. Overall safety objectives are assigned to the identified hazards according to a risk classification matrix. The more severe the hazards are, the less frequently they are tolerated. Based on the OHA results, the ASOR allocates safety objectives to domains, develops and validates risk mitigation strategies that are shared by multiple domains, and allocates safety requirements to those domains.

B.3. TOPAZ accident risk assessment methodology

TOPAZ (Traffic Organization and Perturbation AnalyZer) 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[3]. The main aim of TOPAZ is to model accident risks that are related to advances in air traffic management 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 designers 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.

As the development of appropriate Monte Carlo simulation support may be demanding, it is important to notice that the TOPAZ accident risk assessment methodology can also be applied if such Monte Carlo simulation support is not yet developed for the operation considered. In that case expert judgement plays a larger role and uncertainty level may be relatively large. When the dynamic and stochastic effects are significant and the uncertainty in the assessed risk level is too large, than it is recommended to use Monte Carlo simulation support for the safety risk assessment.

Monte Carlo simulation based TOPAZ applications have been developed for several areas, such as:
1. En-route opposite traffic [Blom et al., 2003]
2. Double Missed Approach [BlomKlompstra&Bakker. 2003]
3. Wake vortex induced riks assessment [VanBaren et al., 2002]
4. Active runway crossing [Stroeve et al., 2006]
5. ASAS within route structure [Everdij et al., 2007]
6. ASAS without route structure [Blom et al., 2006]

The following table shows which specific mathematical techniques have been used within each of these six TOPAZ applications.

TOPAZ application #	1	2	3	4	5	6
Mathematical technique						
Petri net	Y	Y	-	Y	Y	Y
Stochastic differential equations	Y	Y	Y	Y	Y	Y
Stochastic analysis	Y	Y	Y	Y	Y	Y
Advanced human performance model	Y	-	-	Y	-	Y
Bias and uncertainty assessment	Y	Y	-	Y	Y	-

This table shows that for all TOPAZ applications stochastic differential equations and stochastic analysis has been used. For all six, except wake vortex induced risk assessment, use has been made of Petri Net modelling.

An overview of the steps following the TOPAZ accident risk assessment methodology is given in Figure 9.

[3] It is noted that the Dynamic Risk Modelling and Monte Carlo simulations used in TOPAZ can also be applied as a technique in supporting other safety assessment methodologies.

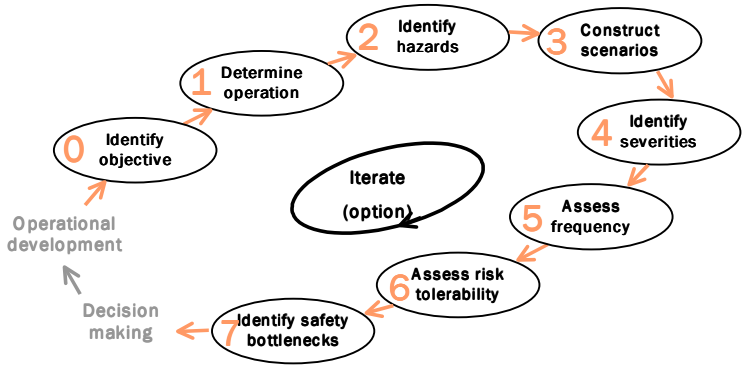

Figure 9: Steps in TOPAZ accident risk assessment

In step 0 the objective of the study 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). Using severity and frequency assessments (steps 4 and 5), the risk associated with each conflict scenario is classified (step 6). For each conflict scenario with a (possibly) unacceptable risk, 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.

Step 0: Identify objective

Before starting the actual safety assessment, the objective and scope of the assessment are set. This should be done in close co-operation with the stakeholder(s). Also, the safety context must be made clear, such that the assessment is performed in line with the safety management framework of the stakeholder(s).

Objective and scope

Generally, the objective of the safety assessment is to obtain an indication how safe the developed operation is, in order to decide about implementation of the operation, or redevelopment. The scope of the assessment concerns for instance the boundaries of the operation under consideration. These can be physical boundaries as well as boundaries of the procedures or systems under consideration.

Safety criteria

An important issue for the safety context is the choice of safety criteria with respect to which the assessment is performed. Example criteria are by ICAO, Eurocontrol ([ESARR 4, 2001]), JAA ([JAR 25.1309, 1994]) or others (e.g. LVNL, DFS). Such criteria are defined for particular flight condition categories (this may vary from flight phases to detailed conflict scenarios and anything in between) and for particular severity categories (e.g. accident, serious incident). Typically, within the chosen context, these criteria define which flight

condition / severity categories have to be evaluated and which frequency level forms the threshold between tolerable and unacceptable risk per flight condition / severity category. In line with ICAO terminology, we refer to such a threshold value as a TLS (Target Level of Safety).

Step 1: Determine operation

Step 1 just serves for the safety assessors to obtain a complete and concise overview of the operation, and to freeze this description during each safety assessment cycle.

Main input to step 1 is a description of the operation from concept developers, while the output is a sufficiently complete, structured, consistent and concise description of the operation considered. The operational context of the operation should be described in generic terms if possible in order to promote universality of application. On the other hand, the description should provide any particular operational assumption to be used in the safety assessment, and the description has to be verified by the operational concept experts/designer(s). Note that it is no part of the safety assessment to develop the operation; this is a task outside the scope of the assessment, which definitely should be performed by operational concept designers.

Important aspects that need to be covered in the operational concept description are:

- The *objective* of the operation and the *traffic flows* to be accommodated;
- The *operational context* of the operation, describing e.g. the geometry of the airport or the air route structure, the timeframe, and the traffic characteristics;
- The roles and responsibilities of the *humans* involved in the operation, especially air traffic controllers and pilots;
- The operational *procedures*, both from an ATC and from a pilot point of view; and
- The *technical systems* used in the operation. These systems are usually divided according to communication, navigation and surveillance functions. Questions like how the systems serve the human, what is their performance, and how are they used need to be answered.

Step 2: Identify hazards

Similar to [ESARR 4, 2001] the term hazard is used in the wide sense; i.e. an event or situation with possibly harmful effects. Such a non-nominal event or situation may evolve into danger, or may hamper the resolution of the danger, possibly in combination with other hazards or under certain conditions. Goal of step 2 is to identify as diverse and many hazards as possible.

Hazard identification brainstorming sessions are used as primary means to identify novel hazards. Necessary participants in these sessions are an air traffic controller, a pilot, a moderator, somebody taking notes, and preferably an expert on the operational concept. The participants should all have a sufficient level of understanding of the operation under consideration. The moderator should prepare by explaining the operation and by identifying some hazards to trigger the brainstorm when necessary, and by making an initial list of conflict types that should be covered. Emphasis is on shifting the boundary between imaginable and unimaginable hazards [De Jong, 2004]. These hazard identification brainstorming sessions should be used to identify potential hazards only, and not to analyse them. Hazards seemingly unimportant during the brainstorming may turn out to be very important in the later steps, and may also trigger the identification of other hazards.

Another important source is formed by hazards identified in previous studies on similar subjects. For this purpose, hazards identified in previous studies are maintained in a TOPAZ hazard database.

Step 3: Construct scenarios

When the list of hazards is as complete as reasonably practicable, it is processed to deal with duplicate, overlapping, similar and ambiguously described hazards. First, per flight condition selected in Step 0, the relevant conflict types which may result from the hazards are to be identified using a full list of potential conflict types, such as for instance 'conflict between two aircraft merging onto one route' or 'aircraft encounters wake vortex of parallel departure'. Per flight condition, each conflict type is subsequently used as crystallisation point upon which all applicable hazards and their combined effects are fitted. The output of such crystallisation process is a bundle of events and condition sequences and effects per crystallisation point, and these are referred to as a *conflict scenario.* This way of constructing conflict scenarios aims to bring into account all relevant ways in which a hazard can play a role in each flight condition / severity category. In order to cope with the complexity of the various possible causes and results to be considered, *clusters* of generic hazards are formed. Such a cluster may cause, or may result from, the same generic hazardous situation. A cluster of events could for instance be the set of 'events causing a missed approach to deviate from the normal path'. An example is given in the figure below. It should also be noticed that one cluster of hazards may play a role in one or more *conflict scenarios*. Often, a conflict is caused by a hazard in combination with a specific condition. Each of the identified hazards can be of the following types:

- a root hazard, which may cause a conflict; or
- a resolution hazard, which may complicate the resolution of a conflict.

Usually, both clusters with root hazards and with resolution hazards play a role in conflict scenario resolution.

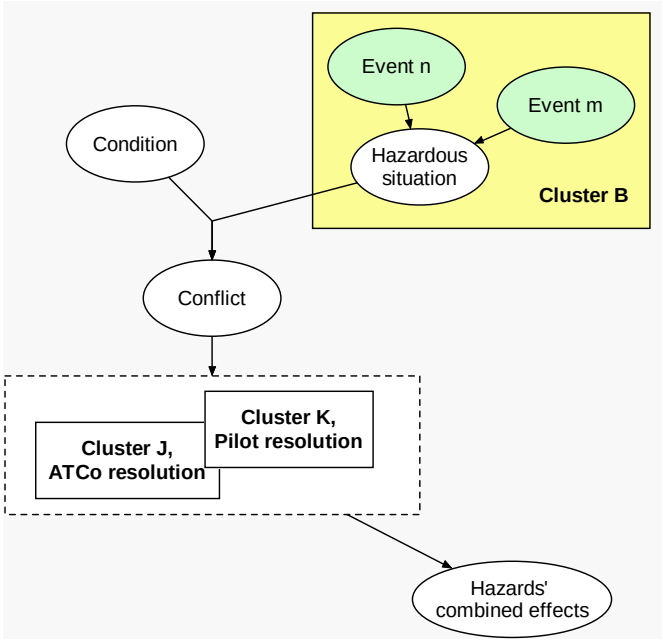

Figure 10: Example conflict scenario

Step 4: Severities of hazards' combined effects

For each of the in Step 3 identified conflict scenarios it is determined which of the severity categories selected in step 0 are applicable to the hazards' combined effects. Safety experts should assess which of the severities are applicable for each conflict scenario, by consultation of and review by operational experts. For each conflict scenario the hazards' combined effects and their severities depend on many factors, such as the conditions under which the conflict occurs, the geometry of the conflict, and on whether (timely) resolution of the conflict takes place. Therefore, a range of severities may apply to a conflict scenario. If necessary, the

structuring of the events in the conflict scenarios of step 3 are updated such that each applicable severity category is linked to the occurrence of specific event sequences.

Step 5: Assess frequency per severity category

Next, for each possible severity outcome of each conflict scenario the occurrence frequency is evaluated by making use of appropriate trees per scenario. The probability of the top event in the tree is expressed as a sum of a product of probabilities of applicable conditional events. For assessing the factors in these trees, primary sources of data are formed by available statistical databases, such as data collected through the Aviation Safety Reporting System (ASRS), NLR's Air Safety Database, local controller reporting system(s), etc. For an appropriate use of such data dedicated operational expertise is taken into account. Of those particular areas of the tree for which a dedicated TOPAZ simulation tool exists, such tool will be used for risk estimation including bias and uncertainty assessment. Important additional data for the frequency assessments is formed by interviews with operational experts, who are familiar with the local ATM systems and procedures of the operation under consideration. Qualitative expressions are to be translated in quantitative numbers when the selected safety criteria of Step 0 also are expressed in numbers. Complicating factors in assessing the frequency of a conflict ending in a given severity at once can be that there is often little or no experience with the new operation, and that the situation may involve several variables. This holds especially for the more severe outcomes of the conflict, since these situations occur rarely, and accordingly less information is at hands about the behaviour of air traffic controllers and pilots in such situations. Using a suitable TOPAZ simulation tool for such assessments has then significant advantages: 1) the risk estimate quality improves, and 2) it is possible to estimate a 95% uncertainty area. Whenever a suitable TOPAZ simulation tool is not available for the application considered, then it is a realistic option to extend an existing or to develop a TOPAZ simulation toolset for this.

Methodology to extend or develop a TOPAZ simulation tool set

The underlying idea of the TOPAZ methodology is to run Monte Carlo simulations of the operation to count the number of risk related events over very large periods of time, e.g. 10^{10} flight hours or more. Although the idea is simple, making this work in practice is not. The key problems and how each is managed within the TOPAZ methodology are described next:

a) In order to simulate 10^{10} or more flight hours in a straightforward manner, even with a supercomputer, one needs a lifetime to accomplish this. Within TOPAZ, use is made of various techniques to speed up the Monte Carlo simulations. Basically, these techniques allow to "factorise" the accident risk in a suitable form. Subsequently, for each factor in this product, a conditional Monte Carlo simulation is performed and at the end all factors are combined into the desired result, e.g. [Blom&al, 2003].
b) How to compare the Monte Carlo simulation model and results with reality? A systematic approach in identifying differences between the Monte Carlo simulations model and reality and in assessing the effects of these differences in terms of bias and uncertainty. The operational concept designers are actively involved with the evaluation of these differences. [Everdij et al., 2006].
c) How to model human behaviour and interactions with other humans and systems? The psychological knowledge and submodels that are used for this have a lot in common with those used in Air-MIDAS and IPME [Laughery&Corker, 1997]. The main difference is that more attention goes to modelling the non-nominal [Blom&al, 1998/2001], [Stroeve&al, 2003], [Blom&Corker&al, 2003].
d) How to build in a controlled way a Monte Carlo simulator for a complex operation in ATM? For building a Monte Carlo simulator use is made of formal mathematical specification methods such as Petri Nets, stochastic differential equations, Markov

processes and similarity transformations. Once such a formal specification is completed, it is used to generate the Monte Carlo simulation code in a semi-automated way [Everdij&Blom, 2003],

Step 6: Assess risk tolerability per severity category

The aim of this step is to assess the tolerability of the risk for each of the flight condition / severity categories selected in step 0. First the total risk per flight condition / severity category is determined by summing over the assessed risk contributions per conflict scenario for that flight condition / severity category. This summation takes into account both the expected value and the 95% area of the risk summation. Next for each severity category the total risk expected value and the 95% area are compared against the in Step 0 selected TLS. If either the expected value arises above the TLS, or the 95% area peaks over the 10xTLS, then the operation is qualified as being UNACCEPTABLE regarding the safety of this severity category. Otherwise the safety of the severity category is qualified as being TOLERABLE.

The figure below presents an example of such a comparison

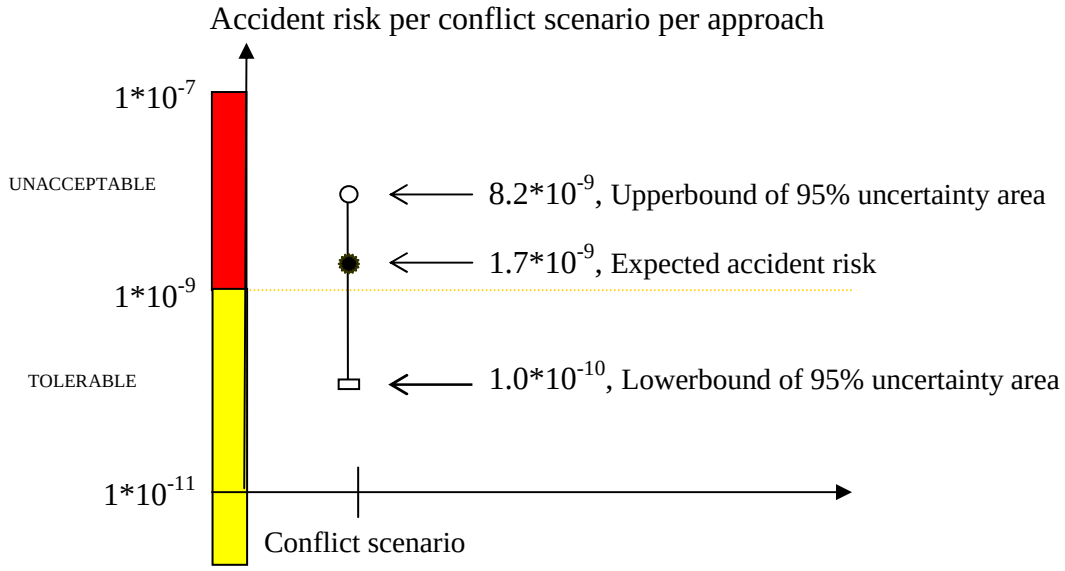

Figure 11: Accident risk per approach for one particular conflict scenario. The * denotes expected accident risk, the area between the small square and small circle is the 95% uncertainty area

During step 0 in [Scholte&al, 2004] each conflict scenario is selected as a flight condition category and four severity categories have been adopted (ACCIDENT, SERIOUS INCIDENT, MAJOR INCIDENT, SIGNIFICANT INCIDENT). For ACCIDENT a TLS of 10^{-9} per conflict scenario has been adopted. During step 5, for one of the conflict scenarios (at least one aircraft is turning to intercept its localizer) the ACCIDENT risk level has been assessed in terms of expected value and 95% uncertainty area. In this example, the 95% uncertainty area stays below 10xTLS, however the expected risk level falls above the TLS. Hence the ACCIDENT risk due to an aircraft turning to intercept its localizer for the operation considered within this Sourdine example has been qualified as being UNACCEPTABLE.

Step 7: Identify safety bottlenecks

From the risk tolerability assessment, it follows which conflict scenario(s) contribute(s) most to the expected value and the 95% area of the risks that has been qualified as being UNACCEPTABLE. For these conflict scenarios the hazards or conditions that contribute most to these high risk level or uncertainty are identified and localised during step 7. If desired, this may also be done for TOLERABLE risks levels that are near the TLS level. Knowledge about these bottlenecks can be used to support further development of the operation.

A systematic way to identify and localise hazard or uncertainty safety bottlenecks for a conflict scenario with UNACCEPTABLE risk is through a sensitivity study. For each hazard/condition one evaluates how much the total risk would improve if its estimated frequency (or uncertainty) is reduced by a factor ten. For some of the hazards and conditions the risk such a factor ten improvement may even reduce the total risk to a TOLERABLE level. These hazards and conditions apparently play a large role in causing the large risk of the conflict scenario, and hence are referred to as safety bottlenecks. The identification and localisation of safety bottlenecks is important as it gives operational concept designers

directions in searching for potential risk mitigating measures for the operation, and for the safety assessment experts to be aware of the hazards/conditions for which the reduction of uncertainty has high priority.

Optional Step: Development of mitigating measures

Following the above assessment steps, decision-makers can consider whether the operation will be implemented as such, or that the operation will not be implemented at all, or that the operation has to be adapted first with mitigating measures. Sometimes sufficient mitigating measures can be achieved at the technical level, where the development of mitigating measures comes down to a rather straightforward engineering process of posing higher requirements on the dependability parameters of the systems, such as is done in [ED-78A, 2000]. More often however, the development of adequate mitigating measures has to be done at the operational level by concept designers and operational experts. Within the TOPAZ methodology the latter process is supported by a mitigation measure brainstorm with concept designers and operational experts as participants and a safety analyst as moderator. The safety analyst moderator can structure the brainstorm on the basis of the outcomes of the safety analysis steps 1 through 6.

Iteration of safety assessment cycle

In case adaptation or redevelopment of the operation takes place, a new safety assessment should be performed that adopts the same wide view as the first cycle, not limiting to the adapted operational details. The reason for this is that adaptations of the air traffic operation may improve safety in one respect, but may imply additional hazards also. And in combination with earlier hazards the additional hazards may deteriorate safety even more than the aimed safety improvement.

Complementary step: Verification

After implementation of the operation the process of monitoring the operation can be initiated. Monitoring yields all kinds of data generated by the operation, e.g. incident or accident reports, realised number of aircraft movements for specific runway combinations in peak hours, flight profiles. These data can be used to verify assumptions which were made in the risk assessment of the operation before implementation. These assumptions are related to the scope of the assessment, the (mathematical) model of the operation, the estimates of operational experts. Verification of these assumptions with operational data provides valuable information about the performed risk assessment and the level of safety.

It may not be necessary to verify all assumptions of the risk assessment. It can be decided to focus on those conflict scenarios that contribute most to the top level risk, or that have an estimated risk above a certain “verification level”. Also, the bias and uncertainty assessment may show that assumptions have a neutral or insignificant effect on risk. Furthermore, operational data may not be available (yet) or sufficient to verify assumptions. These considerations result in a selection of assumptions to be verified. To ease the verification, a list of questions will be formulated in a specific and measurable way, if possible in terms of statistical hypotheses to enable the application of statistical analysis.

Operational data are then used to answer the questions. As soon as these questions have been answered, it has to be decided if there is an indication that assumptions were made unjust. If so, it has to be assessed what this means for the results of the performed risk assessment.

Annex C. Acronyms

A^3	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