EUROPEAN ORGANISATION FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

Enhanced Flexible Use of Airspace Process

Outline Safety Case: Enhanced Real Time Civil-Military Co-ordination (OI-1B)

Edition	:	1.0
Edition Date	:	05/10/04
Status	:	Draft
Class	:	Restricted

EUROPEAN AIR TRAFFIC MANAGEMENT PROGRAMME

PAGE INTENTIONALLY LEFT BLANK

DOCUMENT CHARACTERISTICS

TITLE			
Enhanced Flexible Use of Airspace Process: Outline Safety Case Enhanced Real Time Civil-Military Co-ordination (OI-1B)			
	EATMP Infocentre Reference:		TBD
Document Identifier	**Edition Number:**		1.0
TBD	**Edition Date:**		05/10/04

Abstract

This document contains the Outline Safety Case for the Enhanced Flexible Use of Airspace Process Operational Improvement 1B (OI-1B) which concerns enhanced real time civil/ military co-ordination. It presents the argument why e-FUA OI-1B is acceptably safe in principle to implement in ECAC States together with supporting evidence. All ECAC States should verify that the assumptions, safety assessment scope and conclusions of this Outline Safety Case are applicable to their specific national circumstances prior to implementing OI-1B in their State. Alternatively States may determine that changes are acceptably safe through their own documented safety assessment work.

Keywords

Flexible Use of Airspace	Safety
Enhanced Flexible Use of Airspace Process	Outline Safety Case
Real time civil-military co-ordination	OI-1B

Contact Person(s)	Tel	Unit
T F Suffolk	93383	AFN BD

STATUS, AUDIENCE AND ACCESSIBILITY					
Status		**Intended for**		**Accessible via**	
Working Draft	□	General Public	□	Intranet	□
Draft	☑	EATM Stakeholders	☑	Extranet https://extranet.eurocontrol.int	☑
Proposed Issue	□	Restricted Audience	□	Internet	□
Released Issue	□	*Printed & electronic copies of the document can be obtained from the EATM Infocentre (see page v)*			

ELECTRONIC SOURCE		
Path:	P:/AOM/Library/FUA/Enhanced FUA Documents/	
Host System	Software	Size
Windows XP	Microsoft Word 2002	

THIS PAGE INTENTIONALLY LEFT BLANK

EATM Infocentre
EUROCONTROL Headquarters
96 Rue de la Fusée
B-1130 BRUSSELS

Tel: +32 (0)2 729 51 51
Fax: +32 (0)2 729 99 84
E-mail: eatmp.infocentre@eurocontrol.int

Open on 08:00 - 15:00 UTC from Monday to Thursday, incl.

DOCUMENT APPROVAL

The following table identifies all management authorities who have successively approved the present issue of this document.

AUTHORITY	NAME AND SIGNATURE	DATE
Enhanced FUA Safety Manager	Mr. T. F. SUFFOLK	
FUA Task Manager	Mr. J-P LEMAIRE	
Safety Management DAS/SSM	Dr. B. TIEMEYER	
Head of EATM DAP/SAF	Dr. E MERCKX	
Airspace Management Sub-Group Chairman	Mr. J. DOS SANTOS	
Airspace and Navigation Team Chairman	Mr. A. HENDRIKS	
Director ATM Strategies	Mr. B. REDEBORN	

THIS PAGE INTENTIONALLY LEFT BLANK

DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of and amendments to the present document.

EDITION. AMENDEMENT	DATE	REASON FOR CHANGE	SECTIONS PAGES AFFECTED
Edition 0.1	19/03/04	Draft for comment by ANT and ASM SG	All
Edition 0.2	08/06/04	Comments received from ANT, ASM SG and DAP/SAF	All
Edition 0.3	27/08/04	Comments received from DAP/SAF	All
Edition 1.0	05/10/04	Issue for submission to SRC	All

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This is the Outline Safety Case for Operational Improvement 1B (OI-1B) of the Enhanced Flexible Use of Airspace (e-FUA) process. OI-1B concerns enhanced real-time civil-military co-ordination. This involves 3 main changes:

- The introduction of passive flight data exchange protocols from the military controller to the civil controller;
- The introduction of silent flight data exchange protocols to support the airspace crossing function between civil and military controllers; and
- The introduction of airspace-use data exchange protocols (the Airspace Data Repository).

The purpose of this Outline Safety Case is to demonstrate that OI-1B is acceptably safe in principle for implementation in ECAC States. This is achieved by assessment of the changes required by OI-1B from a generic perspective (that is, using clearly stated assumptions but not taking account of State specific issues) and demonstrating that it will meet the relevant safety criteria derived from the e-FUA Safety Policy.

This Outline Safety Case demonstrates:

- How the overall safety argument has been structured (Section 2).
- Why OI-1B is capable of being acceptably safe in principle (Section 3).
- That all necessary risk reduction measures have been specified as safety requirements or recorded as assumptions (Section 4).
- That EUROCONTROL has taken sufficient measures to enable consistent implementation of safety requirements by ECAC States (Section 5).
- That the evidence from the safety assessment process performed for OI-1B is trustworthy (Section 6).
- That the assumptions made during the safety assessment have been documented and responsibility for their validation has been assigned (Section 7).

This Outline Safety Case for e-FUA OI-1B concludes that it is acceptably safe in principle to implement OI-1B in ECAC States provided that the specified safety requirements are satisfied and subject to verification of the assumptions and resolution of open issues identified in the Recommendations section of this document.

PAGE INTENTIONALLY LEFT BLANK

1. INTRODUCTION

1.1 Background and Justification

The Flexible Use of Airspace (FUA) Concept is intended to provide the maximum flexibility to all airspace users in a seamless fashion across all ECAC States.

The basis of the FUA Concept is that airspace should no longer be designated as either military or civil airspace but instead should be considered as one continuum and used flexibly by all airspace users on a day-to-day basis. Thus any required segregation of Operational Air Traffic (OAT – mostly military aircraft) and General Air Traffic (GAT) should be achieved by the temporary allocation of airspace.

The general airspace management (ASM) functions and procedures needed to fully exploit the FUA Concept are specified in the EUROCONTROL Handbook for Airspace Management [1]. The planning elements and methods of application for a common airspace design and change process in the ECAC Region are contained in the EUROCONTROL Manual for Airspace Planning [2].

Basic FUA (b-FUA) was introduced in early 1996. A list of minimum requirements has been established to define the main criteria and the essential organisational structures and procedures that shall be completed by the State in order to comply with the b-FUA implementation. By the end of 1998 b-FUA was implemented in 13 ECAC States and is currently implemented in almost all ECAC States [3]. b-FUA is a prerequisite for all OIs under Enhanced FUA (e-FUA), including OI-1B.

EUROCONTROL's Airspace Strategy document [4] identifies a coherent set of actions, grouped into 7 Directions for Change (DfC), with the objective of contributing to a single European Sky sometime after 2015. Within the Airspace Strategy DfC B is entitled "Airspace Management & Civil/Military Co-ordination".

Within DfC B, the following 6 Operational Improvements (OI-1B to OI-6B) have been identified along with the stated target implementation timeframe:

OI-1B Enhance real-time civil/ military co-ordination.
OI-2B National collaborative/ integrated airspace planning, to be complete by Q3 2004.
OI-3B Extend FUA to lower airspace, to be complete by Q4 2005.
OI-4B Enhance FUA with dynamic airspace allocation and harmonise OAT/ GAT handling throughout Europe, to be complete by Q4 2006.
OI-5B Collaborative European airspace planning, to be complete by 2008.
OI-6B Integrated European airspace, to be complete by 2012.

These Operational Improvements are collectively called the Enhanced FUA Process.

Within FUA, airspace use is planned with reference to 3 organisational levels:

- Level 1 concerns strategic planning months or years in advance of use;
- Level 2 concerns pre-tactical planning up to 1 day in advance of use; and
- Level 3 concerns tactical planning and co-ordination on the day of operations.

This Outline Safety Case (OSC) concerns enhanced real time civil military co-ordination (OI-1B) which relates exclusively to Level 3.

The main objective of the Operational Improvements under e-FUA is to increase airspace capacity whilst maintaining, or improving where practicable, the safety levels accepted under b-FUA.

1.2 Description of Operational Improvement 1B

Operational Improvement 1B under Enhanced FUA consists of 3 main changes as follows:

- Change 1 – The passive exchange of flight data (basic flight plan data and current flight plan data) from the military controller to the civil controller.
- Change 2 – The silent exchange of flight data between civil and military controllers to support the airspace crossing function.
- Change 3 – The provision of airspace structure status information via the Airspace Data Repository.

OI-1B is described in more detail in Section 2 of the safety assessment report [5].

It should be noted that OI-1B does not change the civil-military co-ordination process. It only changes the means by which that co-ordination process is accomplished.

1.3 Definitions

Some terms used in this report have specific meanings as follows:

- In order for an OI under e-FUA to be “Acceptably Safe” it needs to be at least as safe as b-FUA and, in addition, risks need to be reduced further as far as reasonably practicable. These are the criteria used in the FHA/ PSSA report (DNV, 2004a).

- The term “Acceptably Safe in Principle” means that the OI has been assessed generically and has been shown to be acceptably safe, but that State specific factors that might affect risk levels have not yet been assessed.

- The term “Acceptably Safe to Implement”, means that the OI has been shown to be acceptably safe taking account of all State specific factors.

This Outline Safety Case demonstrates that e-FUA OI-1B is acceptably safe in principle. ECAC States are required to show that a specific implementation of OI-1B is acceptably safe in their State environment and to document this in their National Safety Case (see Section 1.6).

1.4 Aim

The aim of this document, the Outline Safety Case for e-FUA OI-1B, is to show, through argument and supporting evidence, why OI-1B is acceptably safe in principle. It has been prepared by EUROCONTROL to facilitate the implementation of OI-1B by ECAC States within their national boundaries.

1.5 Scope

This Outline Safety Case for e-FUA OI-1B concerns ATM issues that arise from OAT and GAT interactions in controlled airspace above FL 195 that are supervised by civil-military co-ordination procedures at the tactical level (Level 3), consistent with the definition of OI-1B. It is assumed that this involves Class C airspace, with negligible amount of VFR, and that only within state co-ordination is considered.

1.6 The Use of the Outline Safety Case by States

EUROCONTROL has shown, as far as it is able, against clearly defined generic assumptions and definitions that e-FUA OI-1B is acceptably safe in principle for implementation in ECAC States. This assurance is documented in this Outline Safety Case.

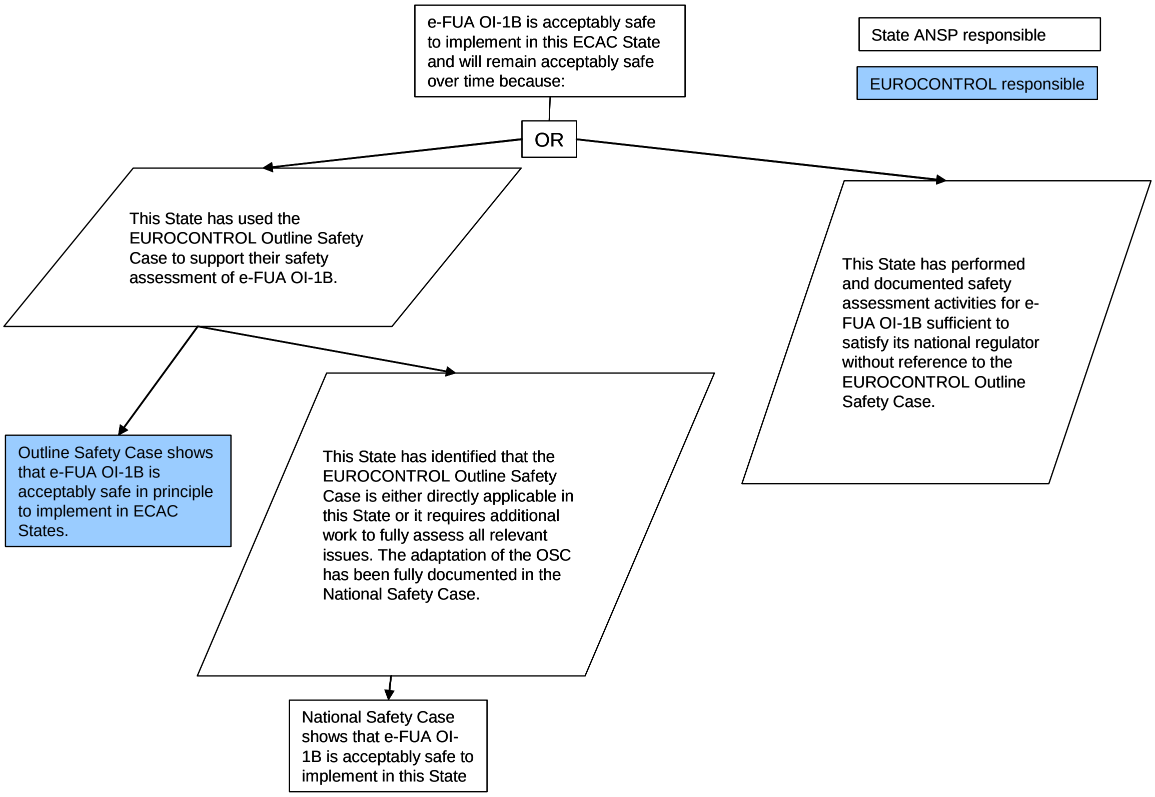
Each individual ECAC State intending to implement e-FUA OI-1B is responsible for:

- Reviewing the Outline Safety Case for e-FUA OI-1B produced by EUROCONTROL; and
- Either determining that the Outline Safety Case is wholly transferable to circumstances in their own State, or identifying additional safety assessment activities that need to be performed to make the Outline Safety Case transferable to their own State and executing these tasks satisfactorily. In both cases the process followed and the results obtained by the implementing States must be documented in their National Safety Case.

Alternatively, a State may perform their own safety assessment of e-FUA OI-1B independent of the EUROCONTROL Outline Safety Case.

These alternative strategies to demonstrate that OI-1B is acceptably safe within a specific ECAC State are summarised in Figure 1.1.

Figure 1.1 The Use of the Outline Safety Case by States



e-FUA OI-1B is acceptably safe to implement in this ECAC State and will remain acceptably safe over time because:

State ANSP responsible

EUROCONTROL responsible

OR

This State has used the EUROCONTROL Outline Safety Case to support their safety assessment of e-FUA OI-1B.

This State has performed and documented safety assessment activities for e-FUA OI-1B sufficient to satisfy its national regulator without reference to the EUROCONTROL Outline Safety Case.

Outline Safety Case shows that e-FUA OI-1B is acceptably safe in principle to implement in ECAC States.

This State has identified that the EUROCONTROL Outline Safety Case is either directly applicable in this State or it requires additional work to fully assess all relevant issues. The adaptation of the OSC has been fully documented in the National Safety Case.

National Safety Case shows that e-FUA OI-1B is acceptably safe to implement in this State

Figure 1.1 also emphasises the party that is responsible for safety at each stage.

1.7 Structure of this Safety Case

This Outline Safety Case for e-FUA OI-1B makes use of a methodology known as Goal Structured Notation (GSN) [6]. This approach begins with the claim that e-FUA OI-1B is acceptably safe in principle to implement in ECAC States. This claim is then broken down into 5 main safety arguments. Each of these is more fully developed in Sections 3-7 of this Outline Safety Case. The full safety argument in GSN format is presented in Appendix A.

Section 2 provides an overview of the safety objectives and safety criteria stated in the e-FUA Safety Policy and how these were applied to e-FUA OI-1B. It also presents the overall structure of the safety argument contained in this Outline Safety Case.

Sections 3 demonstrates why OI-1B is capable of being acceptably safe in principle (proof of concept).

Section 4 demonstrates that all necessary risk reduction measures have been identified as Safety Requirements or recorded as Assumptions.

Section 5 demonstrates that sufficient measures have been taken by EUROCONTROL to enable consistent implementation of safety requirements across ECAC States. This section also details the respective responsibilities of EUROCONTROL and the ECAC States for safety assessment and safe operations of e-FUA OI-1B.

Section 6 demonstrates that the evidence from the safety assessment and analysis is trustworthy.

Section 7 demonstrates that all the assumptions made in the safety assessment and Outline Safety Case have been documented and responsibility for their validation has been assigned.

Section 8 summarises the conclusions of this Outline Safety Case.

Section 9 provides the recommendations of this work programme.

Section 10 lists references cited and defines the acronyms and abbreviations used.

Appendix A shows the argument and evidence structure in GSN format.

2. SAFETY STRATEGY FOR ENHANCED FUA PROCESS OI-1B

2.1 Enhanced FUA Safety Policy and Application to OI-1B

The Enhanced FUA Safety Policy [7] defines 4 Safety Policy Statements to be applied to all the e-FUA Operational Improvements. These are:

1. To maintain safety levels by ensuring that the number of ATM induced accidents and serious or risk bearing incidents do not increase and, where possible, decrease;

2. To periodically review safety targets and requirements (both qualitative and quantitative criteria) for their relevance and applicability to the Enhanced FUA Process over the implementation time period;

3. To demonstrate that safety targets and requirements will be, or have been met; and

4. To ensure that all involved parties are aware of their responsibilities for safety.

These statements are designed to ensure that OIs under e-FUA are acceptably safe upon implementation and remain safe over time.

The e-FUA Safety Policy also elaborates how each Safety Policy is to be satisfied through 4 corresponding High Level Safety Objectives.

In order to meet Policy statement 1:

- The parties responsible for the implementation of the Enhanced FUA Process (EUROCONTROL, States and national ATSPs) will facilitate the orderly implementation of the identified OIs such that there is a net safety benefit, no additional net risk and such that appropriate ESARR4 requirements are met.

In order to meet Policy statement 2:

- EUROCONTROL will periodically review all relevant safety criteria and revise the safety criteria applied to the Enhanced FUA Process if necessary by updating this Safety Policy Document.

In order to meet Policy statement 3:

- EUROCONTROL will conduct safety assessment and safety assurance activities (simulations, trials, operational evaluations, etc. as required) to demonstrate that the Enhanced FUA Process will meet the determined safety criteria (prior to implementation) and to verify that individual States have indeed met those criteria (post-implementation).

In order to meet Policy Statement 4:

- The ATM service-providers, both civil and military, involved in the Enhanced FUA Process shall have in place, in accordance with ESARR3 requirements, a safety management system which ensures, amongst other things, that everyone involved in the safety aspects of ATM service provision has an individual responsibility for their own actions, and that managers are responsible for the safety performance of their own organisation.

This Outline Safety Case addresses these policy statements and objectives in the following manner:

A. It presents the outputs from the safety assessment process. The safety assessment was based on the following two criteria:

   1. Risks should be no higher than under b-FUA; and

   2. Risks should be further reduced as far as reasonably practicable.

   Safety requirements were derived to ensure that these criteria would be met. This part of the safety case is contained primarily in Sections 3 and 4 of this document and partly addresses Statements and Objectives 1 and 3.

B. The safety case also presents the respective safety responsibilities of EUROCONTROL and the States in Section 5 and Section 7. These address the remaining parts of the Statements and Objectives.

2.2 Overall Safety Argument for Enhanced FUA OI-1B

The overall argument presented in this safety case is that:

"*e-FUA OI-1B is acceptably safe in principle to implement in ECAC States*" (***Arg 0***)

The two main strategies employed in supporting this overall argument are to present:

1. *Direct* evidence based on analysis of the results of the safety assessment processes and specification of the necessary risk-reduction measures (***St 001***); and

2. *Backing* evidence based on the adequacy of the safety assessment processes and competence of the project team (***St 002***).

Underlying Strategy St 001 are three arguments:

1. e-FUA OI-1B is capable of being acceptably safe in principle (proof of concept, ***Arg 1***). This argument is primarily based on the outputs from the safety assessment process and is presented in Section 3 of this document together with relevant evidence.

2. All necessary risk-reduction (NRR) measures related directly to the system have been specified as Safety Requirements or recorded as Assumptions (***Arg 2***). Again this argument derives from the safety assessment process and it is further developed in Section 4 of this safety case.

3. Sufficient measures have been taken by EUROCONTROL to enable consistent implementation of Safety Requirements by States (***Arg 3***). This argument is based on a clear definition of EUROCONTROL's responsibilities towards the safety of OI-1B and the interfaces with the ECAC States; this is presented in Section 5 of this report.

Underlying Strategy St 002 is just one argument, namely:

4. Evidence from the safety assessment and analysis is trustworthy (***Arg 4***). This argument is supported by consideration of the safety assessment processes employed and of the personnel involved. These issues are presented in Section 6.

In addition to the two main strategies outlined above, the central argument concerning OI-1B's acceptable safety is supported by an argument concerning comprehensive handling of the assumptions, i.e.

5. All assumptions made in the safety assessment and OSC have been explicitly documented and responsibility for their validation has been assigned (***Arg 5***). These issues are addressed in Section 7.

Following these strategies and ensuring that assumptions are documented and followed up, a robust argument for OI-1B's safety can be developed.

3. OI-1B IS CAPABLE OF BEING ACCEPTABLY SAFE IN PRINCIPLE – PROOF OF CONCEPT (ARG 1)

3.1 Strategy

The strategy (***St 003***) used to support this key argument contains the following three elements:

1. Use the FHA to show that no new hazards are introduced by e-FUA OI-1B and that the probability of more severe existing hazard outcomes is likely to be reduced. This part of the strategy is developed further through Arguments 1.1, 1.2 and 1.3, discussed below.

2. Use the PSSA to show that under e-FUA OI-1B some causes of existing hazards have been removed and that hazard frequencies are in all cases either equal to or lower than for b-FUA. This part of the strategy is developed further through Arguments 1.4 and 1.5, discussed below.

3. Show that no operational factors or issues exist which might prevent e-FUA OI-1B from being implemented to an acceptably safe level (developed further in Argument 1.6, see below).

The direct evidence that underlies arguments 1.1 to 1.5 is presented in Section 3.2.

3.2 Direct Evidence

The FHA/ PSSA report [5] demonstrates that OI-1B is capable of being acceptable safe in principle, i.e.

1. The risks should be no higher than under b-FUA; and

2. Risks can be further reduced as far as reasonably practicable.

It does this through providing evidence for the following series of arguments, 1.1 to 1.6.

Argument 1.1 - No new hazards have been introduced by e-FUA OI-1B

In order to identify hazards associated with OI-1B three activities were conducted:

1. A functional model of OI-1B and the associated changes was developed by EUROCONTROL and its contracted safety specialists;

2. A “dry run” hazard identification brain storming session was conducted with EUROCONTROL personnel to check, amongst other issues, the changes introduced by OI-1B and potential hazards arising; and

3. A full hazard identification FHA session was carried out involving a multi-disciplinary team of ATM and safety specialists drawn from EUROCONTROL and ECAC States in which the changes were systematically analysed and hazardous conditions identified.

The outputs from these activities were then rationalised within a model (known as a bow tie model) consisting of event trees and fault trees. The key hazards identified of relevance to the changes introduced by OI-1B were:

- Failure of controllers to provide a timely clearance; and
- Incorrect clearance by controllers.

These hazards are referred to collectively as “clearance errors” and already exist under b-FUA. No new hazards were identified during the activities described above. Fuller documentary evidence exists within the FHA/ PSSA report, which includes complete records of the FHA session and details of the functional model.

Argument 1.2 - Consequential mitigations for some existing hazards are made more effective & Argument 1.3 - No consequential mitigations for existing hazards made less effective

The consequences of the hazards above were considered with the assistance of an Event Tree. This structured a list of the key factors that would determine the severity of the hazard outcome. These key factors were then analysed to see whether OI-1B would have any effect, whether beneficial or detrimental. This analysis is shown in Table 3.1 taken from the FHA/PSSA report.

Table 3.1 Analysis of Effect of e-FUA on Hazard Mitigation for Civil Controllers

Event Tree Node	Effect of e-FUA OI-1B
Pilot questions clearance leading to its correction.	Implementation of OI-1B will not affect this event tree node as the mode of controller-controller communication has no effect on the pilot’s ability to detect an incorrect clearance.
c-ATCO detects and corrects error.	Under e-FUA OI-1B the civil controller has a more complete picture of the traffic situation. Probabilities of successful clearance correction potentially improved.
m-ATCO sees error and contacts c-ATCO.	Military controllers’ picture of the traffic situation may be unchanged by e-FUA OI-1B or slightly improved by access to GAT intention data. Probabilities of successful clearance correction either unchanged or potentially improved.
m-ATCO sees error and contacts OAT.	Military controllers’ picture of the traffic situation may be unchanged by e-FUA OI-1B or only slightly improved by access to GAT intention data,. Probabilities of successful clearance correction either unchanged or potentially improved.
STCA[1] leads to resolution.	Under e-FUA OI-1B the civil controller has a more complete picture of the traffic situation and STCA should have a better picture of civil-military conflicts. Probabilities of successful clearance correction potentially improved.
ACAS leads to resolution.	Implementation of OI-1B will not affect this event tree node.
See and avoid.	Implementation of OI-1B will not affect this event tree node.

The overall conclusions from Table 3.1, are that:

- Certain mitigations are potentially improved through the changes associated with OI-1B, primarily as the civil controllers will have a more complete traffic picture and would be in a better position to react and resolve any impending losses of separation.

- No mitigations are made less effective.

[1] Note that while STCA is considered for completeness, no reliance is placed on it in the demonstration that OI-1B is acceptably safe. The same applies to ACAS.

It should be noted that in developing safety requirements for OI-1B to satisfy the defined risk criteria, no credit has been taken for any potential improvement in risk mitigation within the event trees.

Argument 1.4 – Safety Objectives have been specified to meet the Safety Criteria

Safety Objectives were derived from the safety criteria in relation to the hazards identified above (see ***Argument 1.1***).

1 The likelihood of clearance errors under OI-1B shall be no higher than under b-FUA; and
2 The risk of an accident under OI-1B shall be reduced further as far as reasonably practicable (AFARP).

Argument 1.5 – Safety Objectives are satisfied by the High-level Safety Requirements specified for e-FUA

The strategy (***St 004***) was to address the Safety Objectives by means of high-level Safety Requirements which relate directly to the 3 Changes introduced by e-FUA, and to show how the content of those Changes (known as the Necessary Risk Reduction (NRR[2]) measures) satisfied the high-level Safety Requirements. This is demonstrated by decomposing the Argument into 4 lower-level Arguments, as follows[3]:

Argument 1.5.1- High-level Safety Requirements have been specified for e-FUA

In relation to Change 1 (passive data exchange affecting the controller's traffic picture):

*1 The frequency of clearance errors due to **traffic picture error** shall be no greater than under b-FUA and it shall be reduced further as far as is reasonably practicable.*

In relation to Change 2 (silent data exchange affecting airspace crossing):

*2 The frequency of clearance errors due to **airspace crossing co-ordination error** shall be no greater than under b-FUA and it shall be reduced further as far as is reasonably practicable.*

In relation to Change 3 (airspace data repository affecting airspace status awareness):

*3 The frequency of clearance errors due to **airspace status error** shall be no greater than under b-FUA and it shall be reduced further as far as is reasonably practicable.*

Argument 1.5.2- Some causes of existing hazards have been removed

Causes of hazards were identified within the FHA/ PSSA brainstorming sessions and then rationalised using Fault Tree Analysis (FTA). This process demonstrated that, for the NRR measures in Changes 2 and 3, the spoken and listening failures would be removed and the mis-remembering failures either removed or significantly reduced.

Argument 1.5.3 - All hazard frequencies are equal to or lower than those under b-FUA

The FHA/PSSA showed that, whilst some causes will be removed, they will generally (but not in all cases) be replaced with different types of causes. Thus, the FTA was used to facilitate

[2] Section 4 below shows how the NRR measures are captured as the Safety Requirements for e-FUA
[3] Satisfaction of Safety Objective #2 is addressed in section 4 below.

a pairwise comparison of e-FUA versus b-FUA hazard frequency for each of the three changes.

1. For Change 1, involving passive exchange of flight data (basic flight plan data and current flight plan data) from the military controller to the civil controller, the civil controller will have a more complete traffic picture. This will mitigate against initiating errors by the military controller or the OAT pilot. Therefore, provided adequate safety requirements associated with the data exchange are put in place, the hazard frequency should be reduced by this change.

2. For Change 2, involving silent exchange of flight data to support the airspace crossing function, although spoken and listening failures would be removed and mis-remembering failures either removed or significantly reduced, data entry and read failures will be introduced. From existing data on these respective error modes it would appear that the frequency of initiating errors are comparable. However, human factors analysis presented in the FHA/PSSA report (Appendix III), indicates that the probability of recovering from an initial error under e-FUA should be at least as good as b-FUA and, on balance across all possible scenarios, probably better under e-FUA. Therefore, provided adequate safety requirements associated with the data entry, reading and transfer are put in place, the hazard frequency should not be increased, and would probably be reduced by this change.

3. For Change 3, involving the provision of airspace structure status information via the Airspace Data Repository (ADR), the issues concerning replacement causes stated above under Change 2 also apply. In addition, the ADR should increase the likelihood that all controllers have a consistent picture of airspace status. Thus, provided adequate safety requirements associated with the data entry, checking, storage, transfer and reading are put in place, the hazard frequency should not be increased, and would probably be reduced by this change.

The fault trees were used to ensure that adequate safety requirements were identified for each change covering human performance, procedures and equipment and addressing both function and integrity. This process is presented in Section 4 of this document.

Argument 1.5.4 - No operational factors or issues which might prevent e-FUA OI-1B from being implemented to an acceptably safe level have been identified

As noted above, a comprehensive hazard identification and evaluation process was conducted with the assistance of specialists with considerable relevant operational experience. Their inputs were then further processed using ETA, FTA and human factors analysis (using the TRACEr technique). During none of these stages were factors or issues identified which might prevent e-FUA OI-1B from being implemented to an acceptably safe level.

3.3 Open Issues and Recommendations

There appears to be a lack of publicly available data on comparative error frequencies of verbal and electronic communication in the ATM sector. It would improve the confidence in the safety assessment if such data could be collected. Therefore it is recommended that further evidence on the error frequencies of verbal and electronic (keyed and menu driven selected data using mouse or tracker ball etc) communication in the ATM sector should be collected and used to validate Argument 1.5.3.

It should be noted that currently there is little detail concerning procedures for the Airspace Data Repository, Change 3. It is recommended that when more detail does become available, the safety assessment is revisited to check on its impact.

3.4 Conclusions

It has been shown in this section that:

- OI-1B will not introduce any new hazards;
- Consequential mitigations will be improved with OI-1B. However, the effect on risk may be small and hence no credit has been taken for potential improvements in consequential mitigations;
- Some causes of clearance error will be removed under OI-1B, primarily spoken and listening failures although replaced by other causes; and
- A pairwise comparison of e-FUA versus b-FUA for each of the three changes shows that, with adequate safety requirements, the hazard frequency under e-FUA should be equal to or lower than under b-FUA. The main benefit is likely to arise from the more complete traffic picture afforded to the civil controller.

4. ALL NECESSARY RISK REDUCTION MEASURES HAVE BEEN SPECIFIED AS SAFETY REQUIREMENTS OR RECORDED AS ASSUMPTIONS (ARG 2)

4.1 Strategy

The strategy (***St 005***) to support this argument is to show that all the necessary risk reduction (NRR) measures for each change, including all mitigations identified in the safety assessments, that are necessary to meet the safety criteria have been specified as Safety Requirements or captured as Assumptions, as appropriate.

This strategy leads to five sub-arguments, 2.1 to 2.5. The direct evidence that underlies these arguments is presented in Section 4.2.

4.2 Direct Evidence

In order to satisfy the risk criteria noted in Section 3.2, the safety assessment [5] derived a set of safety requirements for the changes proposed under OI-1B. These requirements were derived in a systematic manner through the use of the functional model, from recommendations made during the brainstorming sessions and during the ETA, FTA and human factors analysis. They are driven by the need to be at least as safe a b-FUA and to have reduced risk further as far as reasonably practicable.

Argument 2.1 - All NRR measures related to Change 1 (passive data exchange affecting the controller's traffic picture) have been specified as Safety Requirements

As discussed in section **Error! Reference source not found.**, the high level requirement for this change is that:

The frequency of clearance errors due to ***traffic picture error*** *shall be no greater than under b-FUA and it shall be reduced further as far as is reasonably practicable.*

In order to meet this high level requirement a set of more detailed requirements was derived. These requirements addressed the relevant branches of the fault tree that modelled the causes of traffic picture error. They are taken from the FHA/PSSA report and shown in full in Table 4.1.

Argument 2.2 - All NRR measures related to Change 2 (silent data exchange affecting airspace crossing) have been specified as Safety Requirements

The high level requirement for this change is that:

The frequency of clearance errors due to ***airspace crossing co-ordination error*** *shall be no greater than under b-FUA and it shall be reduced further as far as is reasonably practicable.*

As above, in order to meet this high level requirement a set of more detailed requirements was derived. These requirements addressed the relevant branches of the fault tree that modelled the causes of airspace crossing error. They are taken from the FHA/PSSA report and shown in full in Table 4.2.

Table 4.1 Safety Requirements for Change 1 – Passive Data Exchange

Safety Requirements Related to Data Entry and Reading
1.1. Information exchanged by the passive mode shall be labelled as new until accepted by the receiving ATCO. 1.2. To reduce data entry errors appropriate use shall be made of automatic syntax and spelling checkers for passive data exchange.
Safety Requirements Related to Transfer and Use of Data
1.3. Passively exchanged data shall be used as a feed into STCA where this provides safety benefits. 1.4. Before the use of passive data exchange leads to removal of a requirement for co-ordination between civil and military controllers, a site-specific safety assessment shall be carried out to ensure that risk will not increase through this change. 1.5. Systems for passive data exchange shall have integrity levels no lower than those for b-FUA systems (verbal via telephone). This level of integrity shall be achieved irrespective of equipment inter-operability issues.

Table 4.2 Safety Requirements for Change 2 – Silent Data Exchange

Safety Requirements Related to Data Entry and Reading
2.1. Each stage of the silent mode co-ordination process shall be coded visually so that the ATCO is immediately aware of the transaction status. 2.2. Standard phraseology shall be used in the silent data exchange. 2.3. To reduce data entry errors appropriate use shall be made of automatic syntax and spelling checkers for silent data exchange.
Safety Requirements Related to Transfer and Use of Data
2.4. Procedures shall be in place to identify which controller should be contacted during co-ordination. (While these should already be in place under b-FUA, it is especially important under e-FUA as there might not be immediate recognition if data is sent to the wrong person). 2.5. Silent mode messages after the initial clearance request shall be automatically routed to the correct controller (similar to “Reply” using email). 2.6. Silent mode communications shall include sufficient contextual and supporting information to enable the identification of mis-addressed messages. 2.7. The voice communication telephone systems used for co-ordination under b-FUA shall be maintained (both the hardware and through regular ATC practice). 2.8. Systems for silent data exchange shall have integrity levels no lower than those for b-FUA systems (verbal telephone). This level of integrity shall be achieved irrespective of equipment inter-operability issues.

Argument 2.3 - All NRR measures related to Change 3 (airspace data repository affecting airspace status awareness) have been specified as Safety Requirements

The high level requirement for this change is that:

The frequency of clearance errors due to ***airspace status error*** *shall be no greater than under b-FUA and it shall be reduced further as far as is reasonably practicable.*

In order to meet this high level requirement a set of more detailed requirements was derived. These requirements addressed the relevant branches of the fault tree that modelled the causes of airspace status error. They are taken from the FHA/PSSA report and shown in full in Table 4.3.

Table 4.3 Safety Requirements for Change 3 – Airspace Status and Airspace Data Repository

Safety Requirements Related to Data Entry and Reading	
3.1.	Authorisation levels shall be set for writing to and reading from the ADR.
3.2.	Procedures shall be in place for preparing, entering, checking and retrieving data from the ADR.
3.3.	To reduce data entry errors appropriate use shall be made of automatic syntax and spelling checkers for writing to the ADR.
Safety Requirements Related to Storage, Transfer and Use of Data	
3.4.	Procedures for use of the Airspace Data Repository shall ensure that all controllers check the current status of the airspace structure they use from the Airspace Data Repository, prior to clearing aircraft to use the structure.
3.5.	The Airspace Data Repository systems shall have integrity levels no lower than those for b-FUA (fax or verbal via telephone). This level of integrity shall be achieved irrespective of equipment inter-operability issues.

Argument 2.4 - All other NRR measures have been captured as Safety Requirements or Assumptions

In addition to the requirements above which are specific to each change a set of requirements was derived that is applicable to all the changes under OI-1B. These requirements are presented in Table 4.4.

Table 4.4 Safety Requirements for All Changes

Additional Technical Requirements Related to Data Transfer
4.1. Time delays for passive exchange of data shall be no greater than those under b-FUA (verbal via telephone). 4.2. Data compatibility and system interoperability shall be assured through the design process. 4.3. The availability of new systems under OI-1B shall be at least as high as equivalent systems under b-FUA. 4.4. The potential for common cause failure modes and other installation specific issues which could degrade system availability and integrity unacceptably shall be assessed. 4.5. All new systems to support OI-1B shall fail safe (that is, shall not appear to be working when they are not, consistent with verbal co-ordination processes performed under b-FUA). 4.6. Consideration shall be given to whether equipment to support OI-1B should be subject to third party testing and certification. Inter-operability would be a key part of such third party testing.
Additional Human Factors, Procedures and Safety Management Requirements
4.7. Consideration shall be given to human factors including human machine interface issues during the design phase of equipment and procedures to support changes required by OI-1B. 4.8. A system performance and incident evaluation programme shall be implemented during switch-over to OI-1B so that any unexpected operational factors are identified, understood and, if necessary, resolved promptly. 4.9. Controller workload shall be monitored during and following switch-over to OI-1B to determine whether the potential safety benefits discussed in the FHA/PSSA report are being realised. 4.10. Contingency planning and drills shall include the scenario where passive and silent data exchange systems and/ or the ADR fail. 4.11. As traffic levels increase under e-FUA, it shall be regularly checked that emergency procedures (e.g. in event of surveillance and/ or communications failure) are still adequate. 4.12. Appropriate training shall be provided for all new systems.

Argument 2.5 – The Safety Requirements represent a reduction in risk that is As Far As Reasonably Practicable

It was inherent in the FHA / PSSA process, and reflected in the derivation of the above detailed Safety Requirements that:

- All potential functional improvements that are both practicable and significantly beneficial to safety were identified and captured as Safety Requirements; and
- The required integrity was set at a level at least as high as currently achieved by the systems supporting b-FUA.

4.3 Open Issues and Recommendations

Through the use of formal safety assessment processes safety requirements have been defined for this Outline Safety Case (OSC). Inevitably these processes are somewhat generic when applied in an OSC and do not take account of State-specific factors. Thus the requirements above are not necessarily a complete set. Specific States may need additional requirements and their own studies may reveal this. It is recommended that EUROCONTROL maintain an open dialogue with ECAC States so that States may identify additional safety requirements that may be applicable more widely, or identify requirements that are unnecessary or impracticable. In this way the set of Safety Requirements will be optimised.

4.4 Conclusions

It has been shown in this section that:

- A systematic process, using the fault trees to focus on key hazard causes, has been used to derive the detailed Safety Requirements;
- The Safety Requirements cover human performance, procedures and equipment and address function and integrity;
- The Safety Requirements satisfy the necessary risk-reduction measures (NRRs) derived in section 3.

5. SUFFICIENT MEASURES HAVE BEEN TAKEN BY EUROCONTROL TO ENABLE CONSISTENT IMPLEMENTATION OF SAFETY REQUIREMENTS (ARG 3)

5.1 Strategy

The strategy (***St 006***) to support this argument is to show that:

- Respective responsibilities of EUROCONTROL and States have been clearly delineated; and that

- States have been given sufficient guidance on discharging their responsibilities.

The arguments and evidence developed to meet this strategy are described below in Section 5.2.

5.2 Direct Evidence

Argument 3.1 – Respective safety responsibilities of EUROCONTROL and the States have been clearly, correctly and completely specified

The respective responsibilities are set out below to ensure that all the Policy Statements and Objectives contained in the e-FUA Safety Policy are satisfied.

EUROCONTROL – is responsible for the following:

- Preparing a Safety Policy [7] and Plan [8] for e-FUA;
- Preparing a safety assessment and OSC for OI-1B;
- Promulgating the OSC and the derived Safety Requirements;
- Ensuring that States understand how the OSC and safety assessment should be used;
- Supporting States in the consistent implementation of Safety Requirements – see Section 4.3;
- Periodically reviewing safety targets to check whether any changes impact the safety assessment and safety Requirements; and
- Supporting States post Implementation via open dialogue and forums such as Airspace & Navigation Team (ANT).

The EUROCONTROL Airspace Management Sub-Group (ASM SG) supports the ANT in the development, planning and implementation of Europe-wide airspace management. Regular ASM SG meetings consider status reports on FUA and e-FUA Implementation in the ECAC States and Task Force B of the ASM SG supports the development of FUA and e-FUA in the ECAC States. EUROCONTROL staff provide ad-hoc support for FUA and e-FUA implementation on request to all ECAC States. More details of internal EUROCONTROL responsibilities are contained in the Safety Plan.

States – are responsible for:

- Reading and understanding the OSC, referring any queries to EUROCONTROL;
- Checking the applicability of safety assessment scope, assumptions, conclusions and safety requirements;

- Validating relevant assumptions (see Tables 7.1 to 7.3);
- Preparing National Safety Cases for OI-1B that either use the OSC or their own safety assessment activities (see Figure 1.1) to demonstrate that safety objectives will be met;
- Implementing OI-1B safely following approval procedures for that State;
- Conducting post-implementation monitoring activities to show that OI-1B continues to be acceptably safe, by reference to the OSC or otherwise; and
- Ensuring that all parties within the State are aware of their responsibilities for safety through a formal SMS.

Argument 3.2 – States have been provided with all necessary guidance to enable them to discharge their responsibilities completely and correctly

The main safety documents specifically related to OI-1B have been noted above already, namely:

- The Enhanced FUA Safety Policy [7];
- The Enhanced FUA Safety Plan [8];
- FHA/ PSSA Report on OI-1B [5]; and
- This OSC document.

The EUROCONTROL, Enhanced FUA Process Safety Policy defines the Safety Policy Statements and high level safety objectives for the implementation of the e-FUA process within ECAC States. The Safety Policy details the e-FUA Safety Policy that applies to e-FUA Operational Improvements OI-1B to OI-6B inclusive.

EUROCONTROL, Enhanced FUA Process Safety Plan defines the safety assessment activities that must be performed by EUROCONTROL and the ECAC States to demonstrate that e-FUA is acceptably safe. The Safety Plan outlines the activities to be performed, identifies the Safety Criteria and details the EUROCONTROL Safety Assessment Methodology. The Safety Plan details the Roles and responsibilities within EUROCONTROL and each ECAC State. The Safety Plan provides a route map to guide ECAC States' safety assessment activities to ensure that each OI within the e-FUA Process will be acceptably safe upon implementation in each ECAC State and will remain acceptably safe over time.

The **FHA/ PSSA Report on OI-1B** documents in full the safety assessment process and outputs associated with the proposed changes. Relevant parts are summarised in this document.

In addition, the ESARRs (2 to 6) are all relevant to the safe implementation of any change together with the EATMP Safety Policy [9].

In the course of the introduction of the FUA Concept and its further development Enhanced FUA (e-FUA) EUROCONTROL has developed a comprehensive range of basic FUA and e-FUA reference material to support ECAC States' implementation of FUA and e-FUA:

- EUROCONTROL Report on Organisational Structures and Procedures Required for the Application of the Concept of the Flexible Use of Airspace, Doc. 94.70.08, March 1994. [10]
- EUROCONTROL Functional Specifications for System Support to Airspace Data Distribution and Civil/Military Co-ordination, DPS.ET1.ST10.2000-FS-01-00, Edition 1.0, 15/05/96. [11]
- EUROCONTROL Airspace Strategy for ECAC States, ASM.ET1.ST03.4000-EAS-01-00, Edition 1.0, 18/01/01. [4]
- EUROCONTROL Guidance Document for the Implementation of the Concept of the Flexible Use of Airspace, ASM.ET1.ST08.5000-GUI-02-00, Edition 2.0, 18/08/03. [3]

- EUROCONTROL Handbook for Airspace Management, ASM.ET1.ST08.5000-HBK-02-00, Edition 2.0, 22/10/03 [1]
- EUROCONTROL Manual for Airspace Planning, ASM.ET1.ST08.5000-EAPM-02-02, Edition 2.0, 22/10/03 [2]

The e-FUA Safety Process documents, developed by EUROCONTROL during 2004, have been approved by the Airspace Management Sub-Group (ASM SG), endorsed by the Airspace & Navigation Team (ANT) and will be considered in detail by the Safety Review Commission (SRC).

5.3 Open Issues and Recommendations

It was recommended in Section 4.3 that EUROCONTROL maintains an open dialogue with States concerning the applicability of the Safety Requirements. It is recommended that this open dialogue is broadened to cover the identification of all significant implementation and post-implementation issues that arise from States. Where these issues have significance outside one specific State, EUROCONTROL should promulgate this information together with any lessons learnt.

5.4 Conclusions

It has been shown in this section that:

- The safety responsibilities of EUROCONTROL and the States have been fully specified in order to meet the e-FUA Safety Policy and to ensure safe implementation. In particular, the way in which this OSC should be used has been defined; and

- Available guidance material has been prepared that will enable States to discharge their responsibilities.

6. EVIDENCE FROM SAFETY ASSESSMENT IS TRUSTWORTHY (ARG 4)

6.1 Strategy

The strategy (***St 007***) to support this argument is to show that:

- Key outputs of the FHA and PSSA processes are complete and correct;
- The FHA and PSSA processes were suitable for the task and adhered to; and
- The people performing the safety assessment were suitably qualified and experienced.

This strategy is developed within Arguments 4.1 to 4.5 described below in Section 6.2. These provide backing evidence to the overall safety argument.

6.2 Backing Evidence

Argument 4.1 – All hazards from e-FUA OI-1B have been identified and correctly analysed & Argument 4.2 – Probable causes of the e-FUA OI-1B hazards have been identified and correctly analysed

Hazard identification involved the development of a functional model, a dry run hazard identification session and a full FHA/ PSSA brainstorming session. These demonstrated that the relevant hazards for OI-1B were unchanged from b-FUA. Recognised techniques were then used to analyse the hazards and their causes, namely Event Tree Analysis, Fault Tree Analysis and a Human Factors technique called TRACEr. These techniques allowed relevant causes to be identified and analysed so that a comparison between b-FUA and e-FUA could take place.

Argument 4.3 – FHA / PSSA processes were appropriate, adequate and completely and correctly followed

The FHA/ PSSA processes were designed by EUROCONTROL's FUA project team, DAP/SAF and EUROCONTROL's contracted safety specialist. They were based on EUROCONTROL's Safety Assessment Methodology (SAM) and used techniques documented in the SAM as appropriate for use in ATM [12]. The techniques were combined to ensure that they were adequate to demonstrate that OI-1B was acceptably safe in principle. They were followed using the guidance provided in the SAM and the processes were checked by DAP/SAF reviewers.

Table 6.1 shows how the safety assessment and safety case complies with the requirements specified in ESARR 4 [13].

Table 6.1 Comparison of ESARR 4 Safety Requirements with e-FUA OI-1B Safety Assessment and Safety Case

ESARR 4 Requirement	Compliance Description
5.1	Hazard identification as well as risk assessment and mitigation have been systematically conducted as detailed in Sections 3 and 4 of the OSC.
5.1a	The life-cycle has been addressed primarily up to specification of safety requirements. Responsibilities have been specified covering implementation and some post implementation activities.
5.1b	Airborne (pilot) and ground components of system have been addressed.
5.1c	Human, procedures and equipment and their interactions have all been addressed.
5.2a	Scope, boundaries and interfaces plus functions and operational environment have been specified through a functional model and material presented to and edited by participants at FHA/PSSA session.
5.2b	Safety objective for system was developed through identification of ATM hazards and failures. Severity classification scheme was not used explicitly because a safety objective relative to basic-FUA could be developed as hazard outcomes were no worse under e-FUA than b-FUA.
5.2c	A risk mitigation strategy has been derived aimed at the identified hazards and failures, including safety requirements which are practicable and will be effective at mitigating risk (Section 4 of OSC).
5.2d	Verification that safety objectives and requirements have been met will need to be conducted by States as set out in Section 5 of the OSC.
5.3a	Correct and complete arguments with supporting evidence are documented in this OSC to demonstrate that OI-1B should be safe.
5.3b	Safety requirements are traceable to the functions via the Fault Tree Analysis.

Argument 4.4 – The outputs of the FHA / PSSA processes were subjected to independent review

The outputs have been reviewed by ANT and a DAP/SAF specialist (independent of the initial design work). Their comments have been fully incorporated in the final documentation.

Argument 4.5 – All active participants in the FHA / Process were competent to carry out their roles

Safety assessment tasks were conducted by qualified and experienced FUA specialists and safety assessment professionals. The multi-disciplinary team of professionals used in the FHA/ PSSA session had extensive experience which is summarised in Table 6.2 below.

6.3 Open Issues and Recommendations

There are no open issues or recommendations associated with this argument.

6.4 Conclusions

It has been shown in this section that:

- The safety assessment processes have followed established guidelines;
- The process and outputs have been independently reviewed; and
- The conduct of safety assessment tasks and their review have been carried out by suitably qualified and experienced personnel.

Table 6.2 FHA/ PSSA Session Participants

Person	Affiliation and Experience
Tom Suffolk	EUROCONTROL AFN BD, served for 30 years in the RAF as a pilot, air traffic controller, instructor, supervisor, manager and staff officer. Mr Suffolk retired from the RAF as Wing Commander and joined EUROCONTROL in 1994 as an expert in ASM and civil/military coordination he has been directly involved in the development of the Concept for the Flexible Use of Airspace.
Jean-Paul Lemaire	EUROCONTROL AFN BD, joined the French Air Force Academy as a flying officer in 1966. As navigator he has 3,000 hours flying experience including many as navigator-in-command. In 1977 he graduated as a Civil Aviation Engineer and joined DIRCAM. He has considerable experience in ASM and civil/military coordination. He retired after 27 years service with the FAF in the rank of Colonel and joined EUROCONTROL in 1993 to develop the Concept of Flexible Use of Airspace and, subsequently, the Eurocontrol Airspace Strategy.
Major Per Coulet	EUROCONTROL (attended part time) has 28 years experience in the RDAF as an air traffic and air defence controller, fighter allocator and sector controller. He has also served as an instructor and supervisor. He has considerable experience as a staff officer at national and international level and the flight safety inspections of ATC and Air Defence units. He joined EUROCONTROL MIL BD in April 2003.
Lt. Col. Eric Chatelus	Dircam has 24 years service with the FAF as an air traffic control officer chief controller at airports and centres in France. From 1998-2002 he was chief of the ATC section in HQ FAF with responsibility for air traffic controllers. Since 2002 he has been the head of the ASM section at the French military air traffic services directorate responsible for the regulation of military air traffic for French MOD.
Wing Commander Mike Strong	EUROCONTROL MIL BD, has 37 years experience as an air traffic controller, supervisor, instructor, examiner, manager and staff officer. He has served at RAF airfields in the UK and abroad and at joint civil/military ACCs, and has broad experience in a variety of ATM management posts in military and civilian organisations. As a staff officer, he has held responsibility for RAF ATC equipment programmes, UK NATS business planning, safety management, and policy for all airspace activities in the UK outside controlled airspace.
Zlatko Meic	EUROCONTROL, AFN BD is an ASM expert who joined EUROCONTROL from Croatia in 2001. He is a fully qualified ATCO and instructor with experience in the Zagreb ACC, Ljubljana (Slovenia) ACC/APP, Prague ATC Training Centre, as the ATC Operations Manager in Federal ATS Authority of former Yugoslavia and in MOT - CAA of Croatia responsible for international affairs, liaising with ICAO, EUROCONTROL, UN and NATO peace-keeping forces.
Benoit Fonck	CFMU/URB, EUROCONTROL. Served for 15 years in the Belgian Air Force as an air traffic controller, supervisor, manager, staff officer and Head of base ATS. He joined EUROCONTROL in September 2001 as an ASM expert working in the AMN unit on the ASM Handbook and the development of the EUROCONTROL Airspace Strategy Operational Improvements. He joined the CFMU in October 2002 and currently works mainly on the development of the ATFCM Strategy and Evolutions and the improvement of the ASM/ATFCM interface.
Mervyn Oliver	EUROCONTROL. Safety Instructor, has served for over 15 years as an Air Traffic Control Engineer for National Air Traffic Services and spent 2 years in the HQ safety Department. Mr Oliver joined EUROCONTROL in 2000 and is responsible for the System Safety Assessment Courses at the Institute of Air Navigation Services.
Holger Ahrens	DFS is a German civil air traffic controller with considerable experience of flying, ATC and safety matters. He has 1100 hours experience as a German Army helicopter pilot. He was licensed as an ATCO at Bremen ACC from 1989. In 1999 he moved to management duties at Berlin ACC/UAC where he investigated incidents/losses of separation and participated in the safety assessment of the Berlin ACC move to Bremen. He is currently involved on safety assessments for new airspace concepts, new airways and ACC contingency planning.
Wing Commander Stu Wain	RAF has 19 years service with the RAF as a navigator. He has a wide experience of military fast jet flying and has a total of 2000 flying hours on Tornado, Hawk and Jet Provost aircraft in the UK and Germany. He has been a primary and advanced navigation instructor and has experience of staff appointments in the UK. He is

Person	Affiliation and Experience
	currently the UK Delegation to NATO SO ASM.
Squadron Leader David Raine	29 years experience as an air traffic controller, supervisor, instructor, airport manager and staff officer and has served at RAF airfields in the UK, Germany, Cyprus, the Middle East and the Falkland Islands. He has considerable experience at joint civil/military ACCs, and has broad experience in a variety of ATM staff and management posts in military and civilian organisations including responsibility for airspace changes and airspace policy matters.
Lt Col Mike Steinfurth	EUROCONTROL SD/MIL has 29 years experience as a pilot in the German Air Force flying in Germany and the USA. He has 2800 hours in fighter & reconnaissance aircraft and considerable experience in staff appointments including responsibility for Military Aviation Operations, Aviation Regulation and Operational Requirements and Capabilities. He has considerable experience in the management and command of operations, operational flying and training squadrons.
Tim Fowler (facilitator)	Det Norske Veritas. Tim has worked for DNV for 12 years as a risk management consultant and has nearly 25 years post-graduation experience. He has participated in and managed numerous risk assessment projects and is an experienced hazard identification facilitator.
Helen Jones (recorder)	Det Norske Veritas. Helen is an experienced human factors consultant who has worked for DNV for nearly 3 years. Previously she worked for the Royal Navy and has done project work with NATS on the use of electronic paper strips.

7. ALL ASSUMPTIONS HAVE BEEN DOCUMENTED AND VALIDATION ASSIGNED (ARG 5)

The safety assessment of OI-1B has made a number of assumptions. These assumptions are presented in this section and the approach to, and responsibility for, their validation is discussed and assigned.

Assumptions have been grouped as follows:

- Related to the scope of the safety assessment, see Table 7.1 below. States should check that these scope restrictions are consistent with their implementation.

- How b-FUA and OI-1B operate, see Table 7.2 below. This is necessary because the majority of ECAC States are at different stages of FUA implementation. (It is possible that no ECAC States operate b-FUA or OI-1B exactly in the manner assumed in this safety assessment.) Again, States should check that these assumptions are relevant to them. If they are not, they will need to consider what impact this has on the safety assessment conclusions.

- The safety argument that demonstrates that OI-1B is acceptably safe in principle, see Table 7.3 below. The responsibility for ensuring that these assumptions are validated is shared between EUROCONTROL and States.

Table 7.1 Assumptions Related to Scope of Safety Assessment

ID	Assumption	Comment
A1	It is assumed that OI-1B will be applied only to controlled airspace above FL 195	OI-3B will cover airspace below FL 195
A2	It is assumed that OI-1B will be applied only to Class C airspace above FL 195 where VFR GAT activity is negligible.	VFR require clearance to enter Class C airspace
A3	It is assumed that OI-1B will be applied only to within State co-ordination	OI-5B1 will cover Cross Border Areas

Table 7.2 Assumptions Related to Operation of b-FUA and OI-1B

ID	Assumption	Comment
B1	Civil and military controllers are separate entities and are not co-located	Some ECAC States already co-locate their controllers, or provide integrated ATC. The assumption is a worst case. Co-location or full integration is expected to result in safety benefits, though these have not been evaluated.
B2	CNS/ ATM capabilities: • Primary radar assumed to detect both OAT and GAT. • Secondary radar surveillance of OAT by military-controller and GAT by civil-ATC assumed respectively. • GAT detected directly by military secondary radar. • OAT detected directly by civil secondary radar. • VHF voice communication assumed between civil-ATC and GAT and between military-ATC and OAT.	All aspects of CNS and ATM are likely to vary between States.
B3	Silent mode requires additional electronic data entry from both civil and military controllers. Passive mode requires additional electronic data entry from the military controller.	
B4	Civil controllers are responsible for separation between GAT. Military controllers are responsible for separation of OAT-GAT and OAT-OAT	

Table 7.3 Assumptions Related to the Safety Argument for OI-1B

ID	Assumption	Comment	Validation Approach and Responsibility
C1	b-FUA is acceptably safe.	This key assumption of the safety argument is discussed in the e-FUA Safety Plan (Section 3.1.1).	ECAC States are responsible for validating this assumption, probably by reference to operational experience data.
C2	Human error rates for electronic communication (passive and silent modes) are similar to or less than verbal communication error rates.	The assumption here is that this is generally true, whereas there is only limited and/ or generic quantitative data.	EUROCONTROL should support ECAC States by seeking direct evidence via simulations and collation of operational data.[4] See Section 3.3 of OSC.
C3	It has been assumed that the Airspace Data Repository (Change 3) of OI-1B is safer than b-FUA (multiple bi-lateral communication of airspace status).	The Airspace Data Repository has clear safety advantages over b-FUA, but it is currently insufficiently defined to enable a full safety assessment.	EUROCONTROL should perform further safety assessment of Change 3 when it is better defined. See Section 3.3 of OSC.
C4	Safety assessment of OI-1B is assumed to be possible independent of which other OIs under DfC B have been implemented		ECAC States should carefully compare their pre-OI-1B situation with the b-FUA situation assumed in this Outline Safety Assessment and assess the significance of any differences identified.
C5	If e-FUA operations revert to b-FUA (verbal telephone communication) for any reason it is assumed that the risks are identical to current b-FUA risks.	The implementation of OI-1B must not degrade the performance of b-FUA co-ordination methods	ECAC States should confirm this through post implementation operational evaluations.
C6	Controller workloads after implementation of OI-1B are assumed to be similar to those under b-FUA.		ECAC States should confirm this through post implementation operational evaluations.

[4] This issue is applicable to other EATM programmes and hence extra data would have wider benefits.

8. CONCLUSIONS

8.1 Aim

The aim of the OI-1B Outline Safety Case is to show by means of argument and supporting evidence that OI-1B is acceptably safe in principle to implement in ECAC States.

8.2 Overall Safety Argument Structure

The five main arguments employed in supporting this aim are:

1. e-FUA OI-1B is capable of being acceptably safe in principle (proof of concept, ***Arg 1***). This argument is primarily based on the outputs from the safety assessment process and is presented in Section 3 of this document together with relevant evidence.

2. All necessary risk-reduction (NRR) measures related directly to the system have been specified as Safety Requirements or recorded as Assumptions (***Arg 2***). Again this argument derives from the safety assessment process and it is further developed in Section 4 of this outline safety case.

3. Sufficient measures have been taken by EUROCONTROL to enable consistent implementation of Safety Requirements by States (***Arg 3***). This argument is based on a clear definition of EUROCONTROL's responsibilities towards the safety of OI-1B and the interfaces with the ECAC States; this is presented in Section 5 of this report.

4. Evidence from the safety assessment and analysis is trustworthy (***Arg 4***). This argument is supported by consideration of the safety assessment processes employed and of the personnel involved. These issues are presented in Section 6.

5. All assumptions made in the safety assessment and OSC have been explicitly documented and responsibility for their validation has been assigned (***Arg 5***). These issues are addressed in Section 7.

8.3 Capable of Being Acceptably Safe in Principle (Arg 1)

It has been shown in Section 3 that:

- OI-1B will not introduce any new hazards;
- Consequential mitigations will be improved with OI-1B. However, the effect on risk may be small and hence no credit has been taken for potential improvements in consequential mitigations;
- Some causes of clearance error will be removed under OI-1B, primarily spoken and listening failures although replaced by other causes; and
- A pairwise comparison of e-FUA versus b-FUA for each of the three changes shows that, with adequate safety requirements, the hazard frequency under e-FUA should be equal to or lower than under b-FUA. The main benefit is likely to arise from the more complete traffic picture afforded to the civil controller.

8.4 All Necessary Safety Requirements Specified (Arg 2)

It has been shown in Section 4 that:

- A systematic process, using the fault trees to focus on key hazard causes, has been used to derive the detailed Safety Requirements;
- The Safety Requirements cover human performance, procedures and equipment and address function and integrity;
- The Safety Requirements satisfy the necessary risk-reduction measures (NRRs) derived in section 3.

8.5 All Necessary Measures Taken by EUROCONTROL (Arg 3)

It has been shown in Section 5 that:

- The safety responsibilities of EUROCONTROL and the States have been fully specified in order to meet the e-FUA Safety Policy and to ensure safe implementation. In particular, the way in which this OSC should be used has been defined; and
- Available guidance material has been prepared that will enable States to discharge their responsibilities.

8.6 Evidence from Safety Assessment is Trustworthy (Arg 4)

It has been shown in Section 6 that:

- The safety assessment processes have followed established guidelines;
- The process and outputs have been independently reviewed; and
- The conduct of safety assessment tasks and their review have been carried out by suitably qualified and experienced personnel.

8.7 Assumptions (Arg 5)

In Section 7 all the assumptions are documented and the approach and responsibility for their validation has been stated.

9. RECOMMENDATIONS

Based on the identification of open items and further work the following recommendations are made:

1. EUROCONTROL should co-ordinate a work programme to collect more direct evidence on the relative error frequencies of verbal and electronic (keyed and menu driven selected data using mouse or tracker ball etc) communication in the ATM sector. Such work should be used to validate relevant conclusions in this OSC and would be valuable to other ATM work programmes.

2. EUROCONTROL or ECAC States should perform further safety assessment of the Airspace Data Repository (Change 3) when sufficient details of its operation are available.

3. EUROCONTROL should maintain an open dialogue with ECAC States so that States may identify additional safety requirements that may be applicable more widely, or identify requirements that are unnecessary or impracticable. In this way the set of Safety Requirements will be optimised.

4. This open dialogue should also include the identification of all significant implementation and post-implementation issues that arise from States. Where these issues have significance outside one specific State, EUROCONTROL should promulgate this information together with any lessons learnt.

10. REFERENCES, ACRONYMS AND ABBREVIATIONS

10.1 References

1 EUROCONTROL, 2003: “EUROCONTROL Handbook for Airspace Management”, ASM.ET1.ST08.5000-HBK-02-00, Edition 2.0, 22/10/03

2 EUROCONTROL, 2003: “EUROCONTROL Manual for Airspace Planning”, ASM.ET1.ST08.5000-EAPM-02-02, Edition 2.0, 22/10/03

3 EUROCONTROL, 2003: “Guidance Document for the Implementation of the Concept of the Flexible Use of Airspace”, ASM.ET1.ST08.5000-GUI-02-00, Edition 2.0, 18/08/03

4 EUROCONTROL , 2001: “EUROCONTROL Airspace Strategy for ECAC States”, ASM.ET1.ST03.4000-EAS-01-00, Edition 1.0, 18/01/01

5 DNV, 2004: “Enhanced FUA Process: Functional Hazard Assessment/ Preliminary System Safety Assessment Report of OI-1B”, v3, Contract 20127100, 05/10/04

6 EUROCONTROL, 2003: “Safety Case Development Manual”, Edition 1.3, 07.07.03

7 EUROCONTROL, 2004: “Enhanced FUA Process Safety Policy”, Proposed Issue, Edition 1.0, 22/03/04

8 EUROCONTROL, 2004: “Enhanced FUA Process Safety Plan”, Proposed Issue, Edition 1.0, 22/03/04

9 EUROCONTROL, 2001: “EATMP Safety Policy”, Edition 2.0

10 EUROCONTROL, 1994: “Report on Organisational Structures and Procedures Required for the Application of the Concept of the Flexible Use of Airspace”, Doc. 94.70.08, March 1994

11 EUROCONTROL, 1996: “Functional Specifications for System Support to Airspace Data Distribution and Civil/Military Co-ordination”, DPS.ET1.ST10.2000-FS-01-00, Edition 1.0, 15/05/96

12 EUROCONTROL, 2003: “Review of Techniques to Support the EATMP SAM”, 11 April, 2003

13 EUROCONTROL, 2001: "Risk Assessment and Mitigation in ATM", EUROCONTROL Safety Regulatory Requirement (ESARR) 4, Edition 1.0

10.2 Acronyms and Abbreviations

ACAS	Airborne Collision Avoidance System
ADR	Airspace Data Repository
AFN	Airspace/ Flow Management and Navigation Business Division
AMC	Air Management Cell
ANSP	Air Navigation Service Provider
ANT	Airspace and Navigation Team
ARG	Argument

ASM	Airspace Management
ATCO	Air Traffic Controller
ATM	Air Traffic Management
ATS	Air Traffic Service
ATSP	Air Traffic Service Provider
DAP/ SAF	EUROCONTROL Directorate of ATM Programmes/ Safety Enhancement
DAS	EUROCONTROL Directorate of ATM Strategies
DfC	Direction for Change
EATMP	European Air Traffic Management Programme
ECAC	European Civil Aviation Conference
ESARR	EUROCONTROL Safety Regulatory Requirement
ETA	Event Tree Analysis
FHA	Functional Hazard Assessment
FTA	Fault Tree Analysis
FUA	Enhanced/ Basic Flexible Use of Airspace
GAT	General Air Traffic
GSN	Goal Structured Notation
ICAO	International Civil Aviation Organisation
JAA	Joint Aviation Authorities
LoA	Letters of Agreement
NRR	Necessary Risk Reduction
OAT	Operational Air Traffic
OI	Operational Improvement
OSC	Outline Safety Case
PSSA	Preliminary System Safety Assessment
SAM	Safety Assessment Methodology
SG	Sub-Group
SMS	Safety Management System
SOP	Standard Operating Procedures
SRC	Safety Regulatory Commission
SRU	Safety Regulatory Unit
St	Strategy
STCA	Short Term Conflict Alert
TAA	Temporary Airspace Allocation
TLS	Target Level Safety
TRACEr	Technique for the Retrospective Analysis of Cognitive Error
VFR	Visual Flight Rules

Prefixes

b-	basic
c-	civil
e-	enhanced
m-	military
p-	pre

APPENDIX A - Safety Argument for e-FUA OI-1B and Evidence Structure

A.1 Introduction and Methodology

The figures presented below show the safety argument for e-FUA OI-1B and the evidence structure using Goal Structured Notation (GSN).

A key to the *GSN* symbology is shown in **Figure 0**.

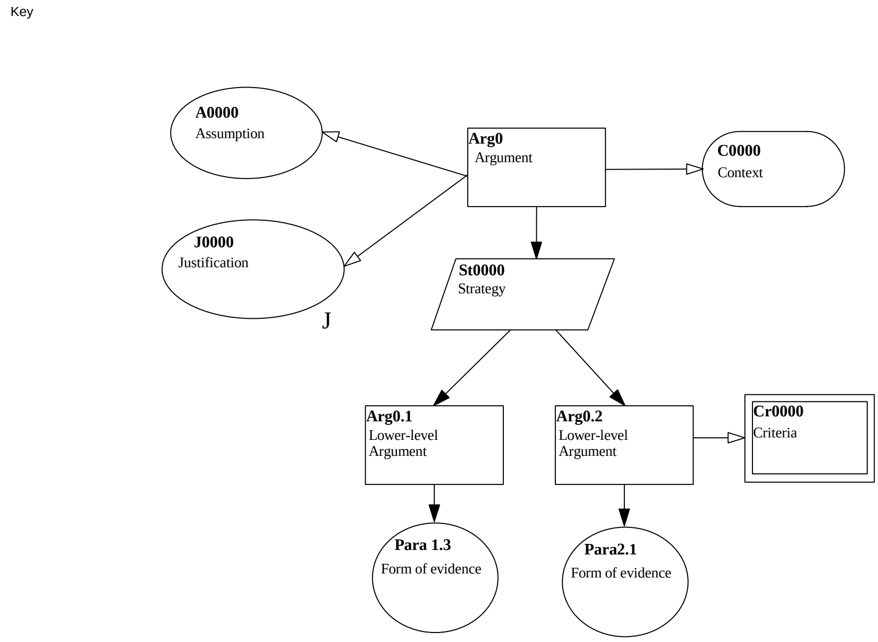


Figure 0 – GSN Key

An *Argument* always takes the form of a predicate - i.e. a statement that is either true or false. As the name suggests, *GSN* provides for the structured decomposition of *Arguments* into smaller, *sub-Arguments*; logically, an *Argument* is true (has been satisfied) if, and only if, its all *sub-Arguments* are true. For the structure to be considered complete, every branch must be terminated in an item of *Evidence* that supports the *Argument* structure to which it is attached.

Other, symbology may be used in order to provide supporting information, as follows.

Strategies are a useful means of adding comment to the structure to explain, for example, how the decomposition will develop. They are not predicates and do not form part of the logical decomposition; rather, they are there purely for explanation of the decomposition, and their use is optional.

Contextual symbology - including the *Assumptions*, *Context*, *Justification* and *Criteria* symbols- is also used to add completeness to the structure.

A.2 Application to OI-1B

Figure 1 starts with the claim that:

> "*e-FUA OI-1B is acceptably safe in principle to implement in ECAC States*" (***Arg 0***)

The two main strategies employed in supporting this overall argument are to present:

1. *Direct* evidence based on analysis of the results of the safety assessment processes and specification of the necessary risk-reduction measures (***St 001***); and

2. *Backing* evidence based on the adequacy of the safety assessment processes and competence of the project team (***St 002***).

Underlying Strategy St 001 are three arguments:

3. e-FUA OI-1B is capable of being acceptably safe in principle (proof of concept, **Arg 1**). This argument is primarily based on the outputs from the safety assessment process and is presented in **Figures 2a &b** of this appendix.

4. All necessary risk-reduction (NRR) measures related directly to the system have been specified as Safety Requirements or recorded as Assumptions (**Arg 2**). Again this argument derives from the safety assessment process and it is further developed in **Figure 3** of this appendix.

5. Sufficient measures have been taken by EUROCONTROL to enable consistent implementation of Safety Requirements by States (**Arg 3**). This argument is based on a clear definition of EUROCONTROL's responsibilities towards the safety of OI-1B and the interfaces with the ECAC States; this is presented in **Figure 4** of this appendix.

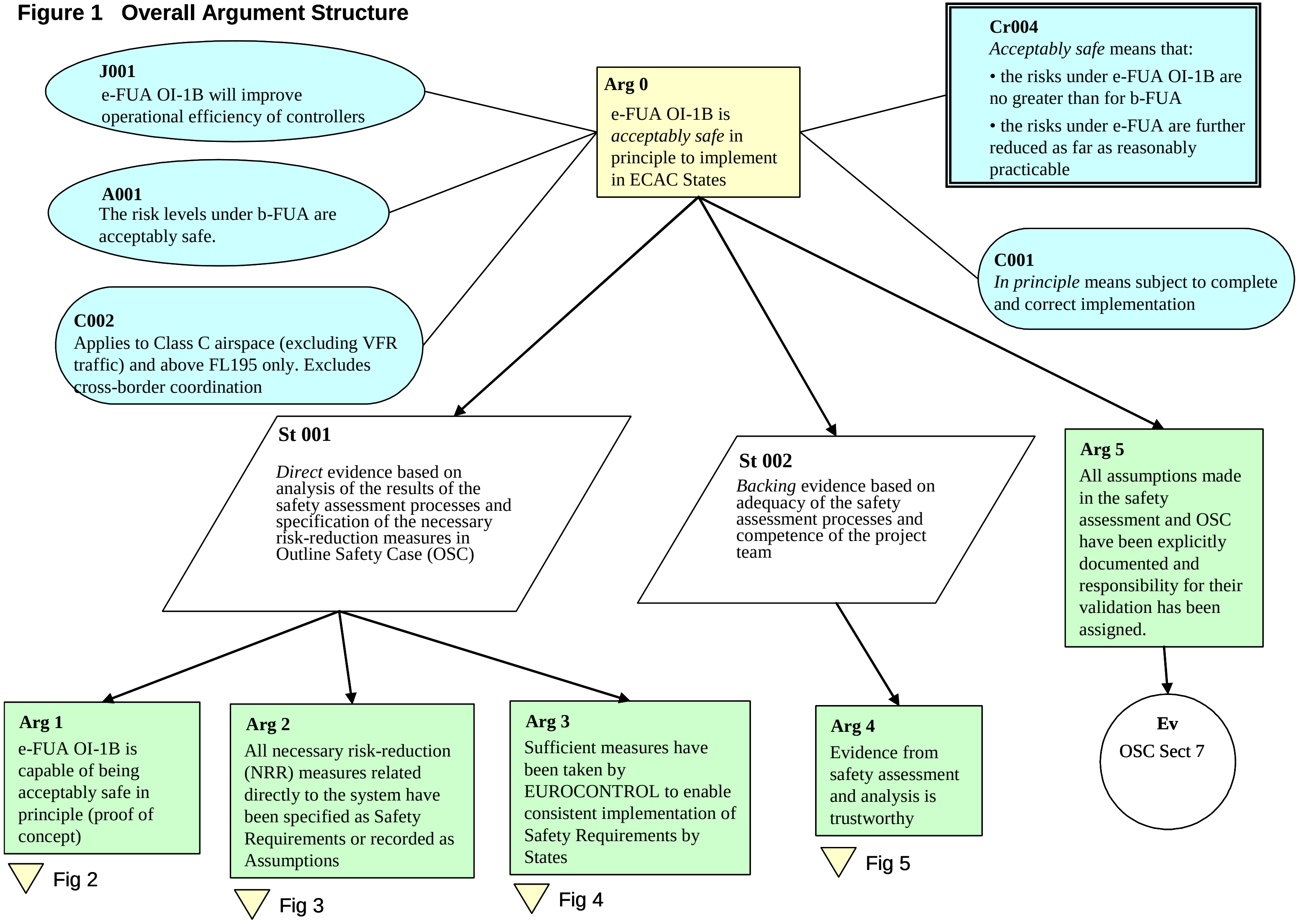
Underlying Strategy St 002 is just one argument, namely:

6. Evidence from the safety assessment and analysis is trustworthy (**Arg 4**). This argument is supported by consideration of the safety assessment processes employed and of the personnel involved. These issues are presented in **Figure 5** of this appendix.

In addition to the two main strategies outlined above, the central argument concerning OI-1B's acceptable safety is supported by an argument concerning comprehensive handling of the assumptions, i.e.

7. All assumptions made in the safety assessment and OSC have been explicitly documented and responsibility for their validation has been assigned (**Arg 5**).

Figure 1 Overall Argument Structure



J001
e-FUA OI-1B will improve operational efficiency of controllers
A001
The risk levels under b-FUA are acceptably safe.
C002
Applies to Class C airspace (excluding VFR traffic) and above FL195 only. Excludes cross-border coordination
Arg 0
e-FUA OI-1B is *acceptably safe* in principle to implement in ECAC States
Cr004
Acceptably safe means that:
• the risks under e-FUA OI-1B are no greater than for b-FUA
• the risks under e-FUA are further reduced as far as reasonably practicable
C001
In principle means subject to complete and correct implementation
St 001
Direct evidence based on analysis of the results of the safety assessment processes and specification of the necessary risk-reduction measures in Outline Safety Case (OSC)
St 002
Backing evidence based on adequacy of the safety assessment processes and competence of the project team
Arg 5
All assumptions made in the safety assessment and OSC have been explicitly documented and responsibility for their validation has been assigned.
Arg 1
e-FUA OI-1B is capable of being acceptably safe in principle (proof of concept)
Fig 2
Arg 2
All necessary risk-reduction (NRR) measures related directly to the system have been specified as Safety Requirements or recorded as Assumptions
Fig 3
Arg 3
Sufficient measures have been taken by EUROCONTROL to enable consistent implementation of Safety Requirements by States
Fig 4
Arg 4
Evidence from safety assessment and analysis is trustworthy
Fig 5
Ev
OSC Sect 7

Figure 2a Strategies for Using FHA/ PSSA

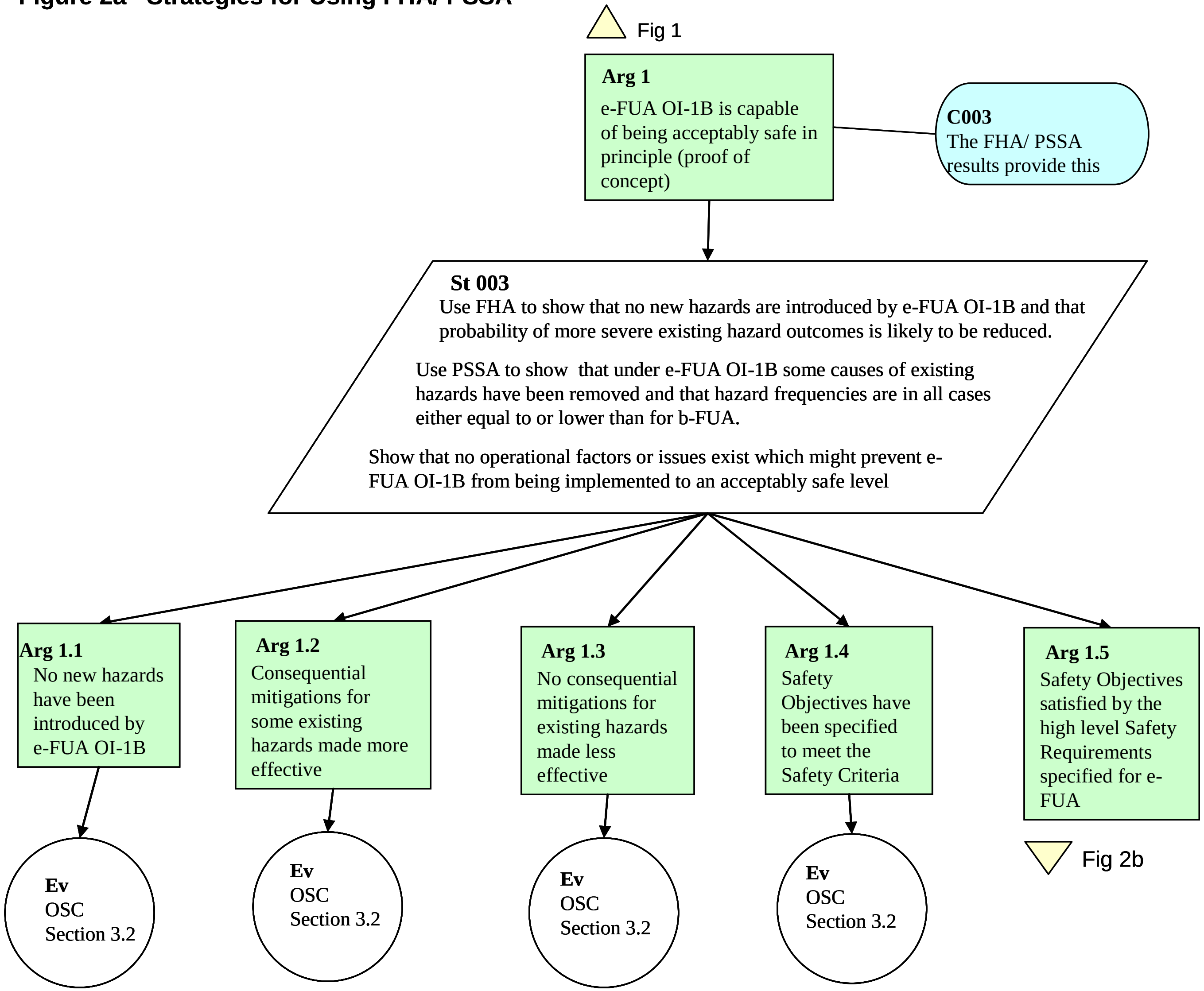


Fig 1
Arg 1
e-FUA OI-1B is capable of being acceptably safe in principle (proof of concept)
C003
The FHA/ PSSA results provide this
St 003
Use FHA to show that no new hazards are introduced by e-FUA OI-1B and that probability of more severe existing hazard outcomes is likely to be reduced.
Use PSSA to show that under e-FUA OI-1B some causes of existing hazards have been removed and that hazard frequencies are in all cases either equal to or lower than for b-FUA.
Show that no operational factors or issues exist which might prevent e-FUA OI-1B from being implemented to an acceptably safe level
Arg 1.1
No new hazards have been introduced by e-FUA OI-1B
Arg 1.2
Consequential mitigations for some existing hazards made more effective
Arg 1.3
No consequential mitigations for existing hazards made less effective
Arg 1.4
Safety Objectives have been specified to meet the Safety Criteria
Arg 1.5
Safety Objectives satisfied by the high level Safety Requirements specified for e-FUA
Ev
OSC
Section 3.2
Ev
OSC
Section 3.2
Ev
OSC
Section 3.2
Ev
OSC
Section 3.2
Fig 2b

Figure 2b Strategies for Using FHA/ PSSA

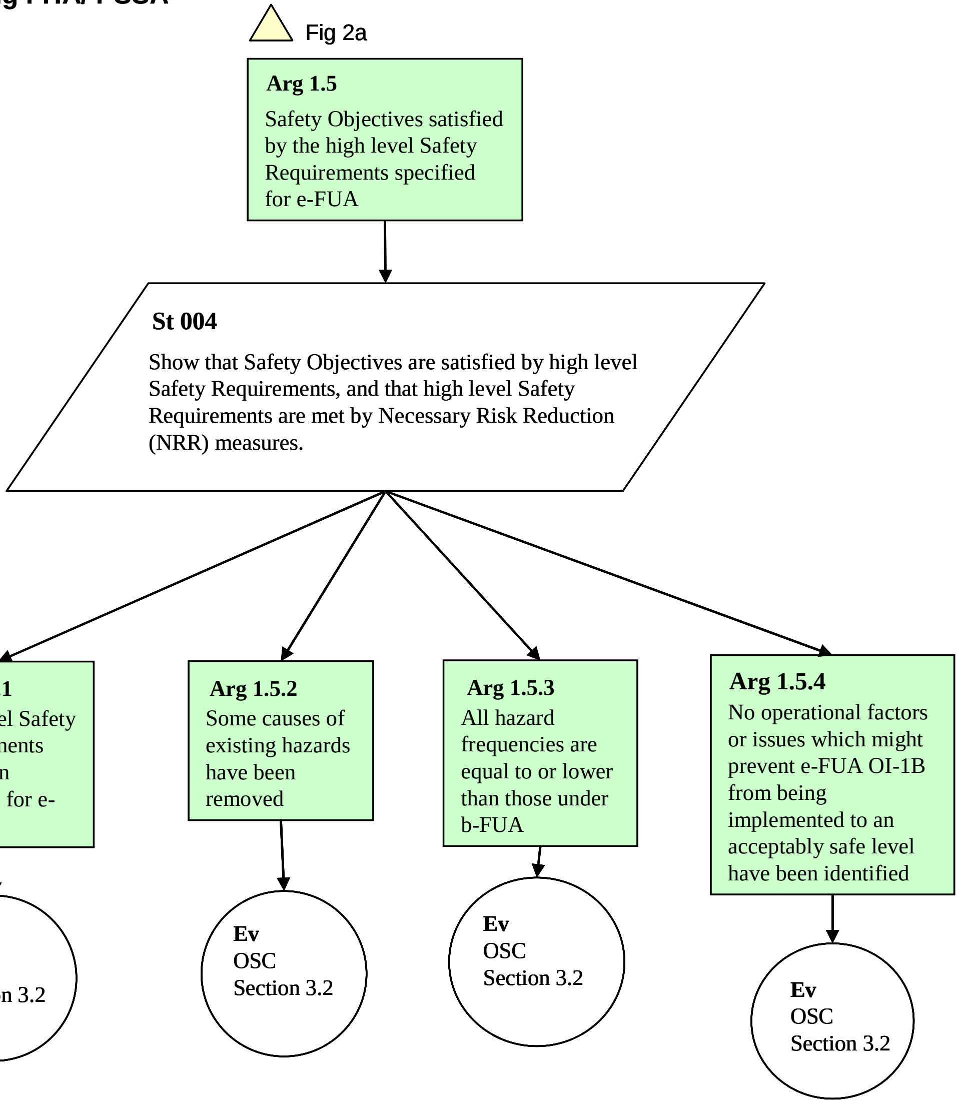


Fig 2a
Arg 1.5
Safety Objectives satisfied by the high level Safety Requirements specified for e-FUA
St 004
Show that Safety Objectives are satisfied by high level Safety Requirements, and that high level Safety Requirements are met by Necessary Risk Reduction (NRR) measures.
Arg 1.5.1
High level Safety Requirements have been specified for e-FUA
Arg 1.5.2
Some causes of existing hazards have been removed
Arg 1.5.3
All hazard frequencies are equal to or lower than those under b-FUA
Arg 1.5.4
No operational factors or issues which might prevent e-FUA OI-1B from being implemented to an acceptably safe level have been identified
Ev
OSC
Section 3.2
Ev
OSC
Section 3.2
Ev
OSC
Section 3.2
Ev
OSC
Section 3.2

Figure 3 Safety Requirements

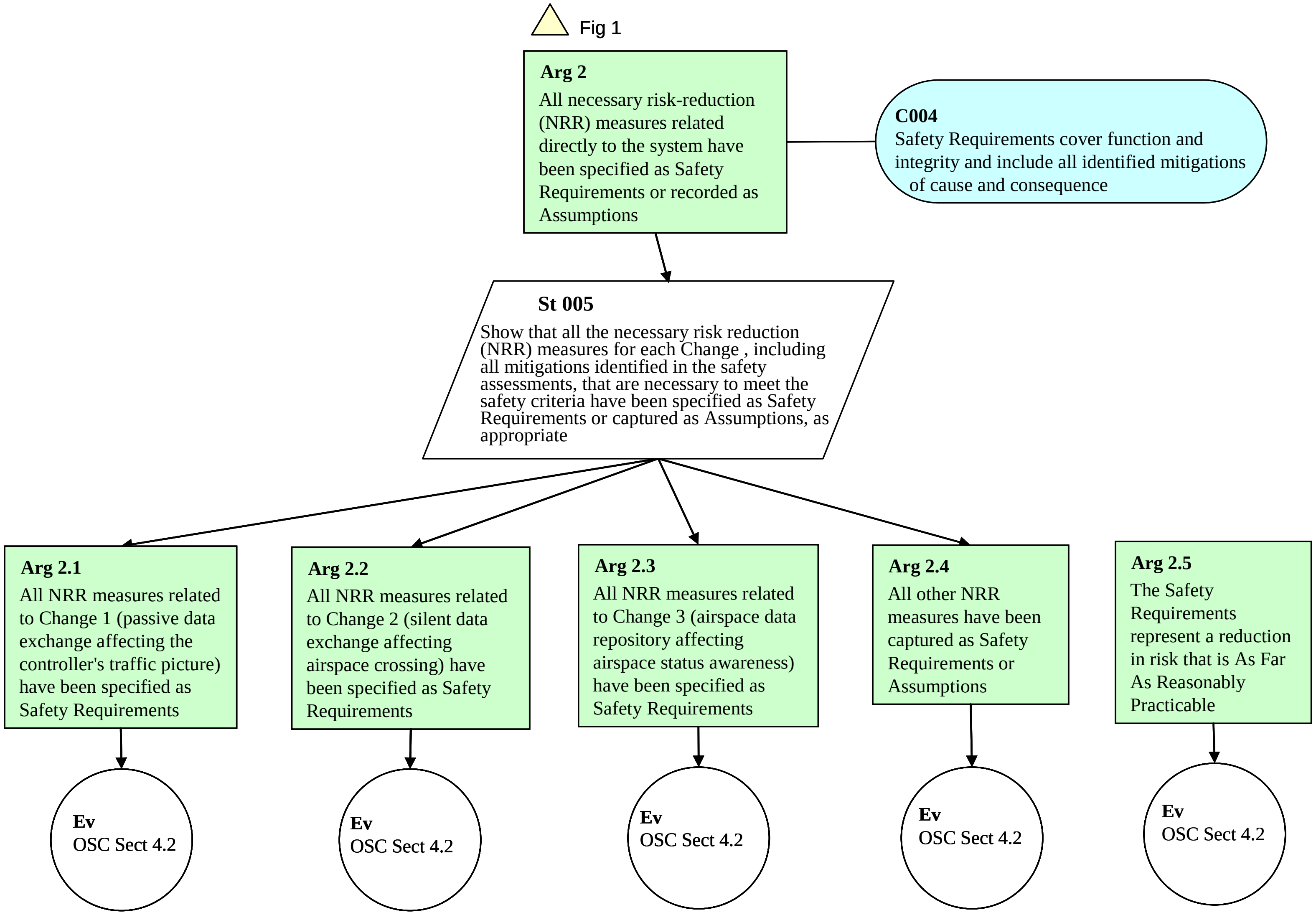


Fig 1
Arg 2
All necessary risk-reduction (NRR) measures related directly to the system have been specified as Safety Requirements or recorded as Assumptions
C004
Safety Requirements cover function and integrity and include all identified mitigations of cause and consequence
St 005
Show that all the necessary risk reduction (NRR) measures for each Change , including all mitigations identified in the safety assessments, that are necessary to meet the safety criteria have been specified as Safety Requirements or captured as Assumptions, as appropriate
Arg 2.1
All NRR measures related to Change 1 (passive data exchange affecting the controller's traffic picture) have been specified as Safety Requirements
Arg 2.2
All NRR measures related to Change 2 (silent data exchange affecting airspace crossing) have been specified as Safety Requirements
Arg 2.3
All NRR measures related to Change 3 (airspace data repository affecting airspace status awareness) have been specified as Safety Requirements
Arg 2.4
All other NRR measures have been captured as Safety Requirements or Assumptions
Arg 2.5
The Safety Requirements represent a reduction in risk that is As Far As Reasonably Practicable
Ev
OSC Sect 4.2
Ev
OSC Sect 4.2
Ev
OSC Sect 4.2
Ev
OSC Sect 4.2
Ev
OSC Sect 4.2

Figure 4 Responsibilities for Safety

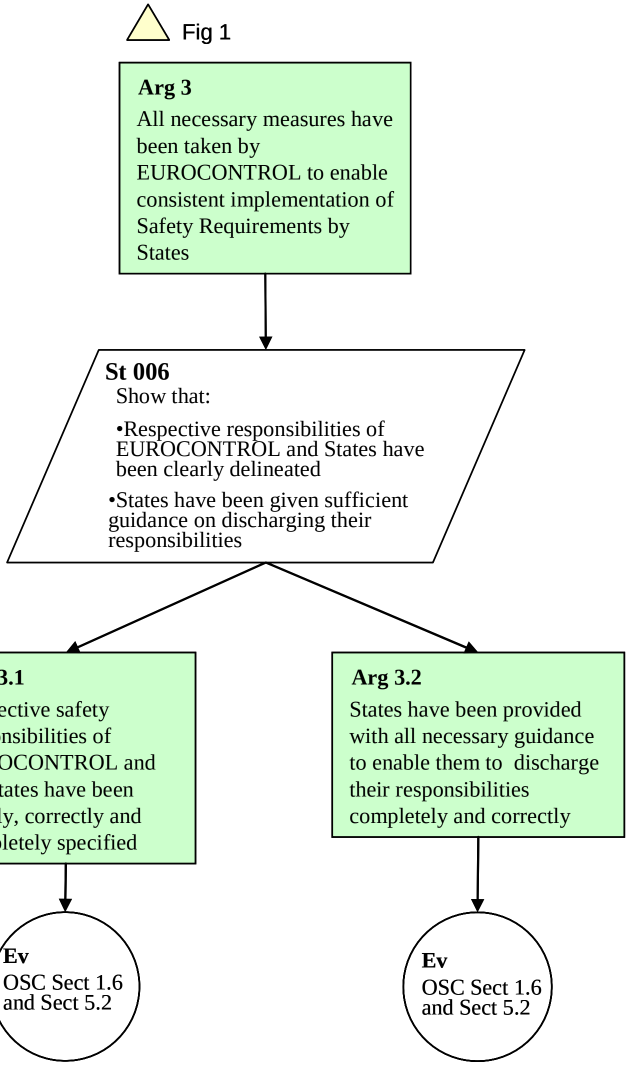


Fig 1
Arg 3
All necessary measures have been taken by EUROCONTROL to enable consistent implementation of Safety Requirements by States
St 006
Show that:
•Respective responsibilities of EUROCONTROL and States have been clearly delineated
•States have been given sufficient guidance on discharging their responsibilities
Arg 3.1
Respective safety responsibilities of EUROCONTROL and the States have been clearly, correctly and completely specified
Arg 3.2
States have been provided with all necessary guidance to enable them to discharge their responsibilities completely and correctly
Ev
OSC Sect 1.6 and Sect 5.2
Ev
OSC Sect 1.6 and Sect 5.2

Figure 5 Backing Evidence

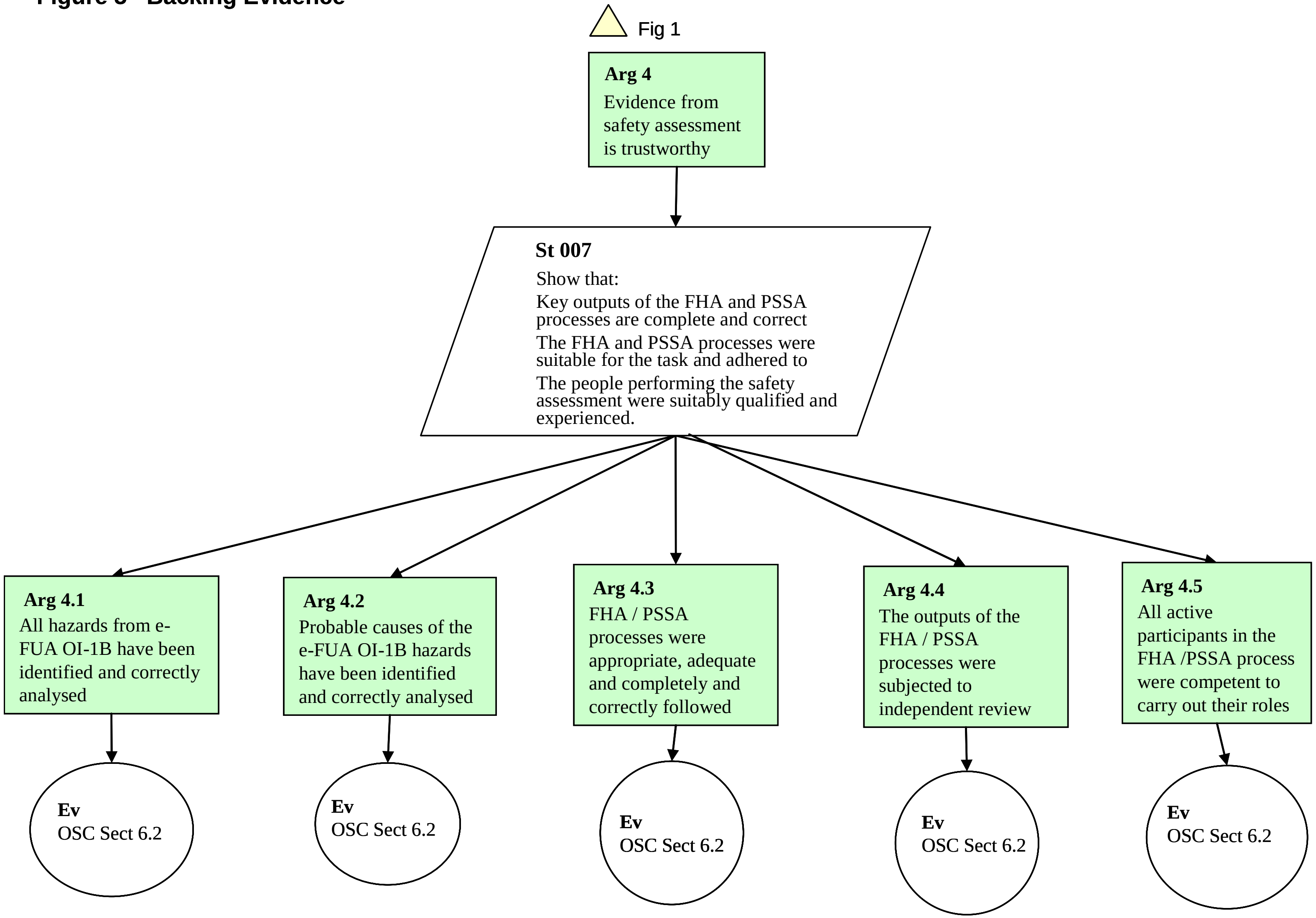


Fig 1
Arg 4
Evidence from safety assessment is trustworthy
St 007
Show that:
Key outputs of the FHA and PSSA processes are complete and correct
The FHA and PSSA processes were suitable for the task and adhered to
The people performing the safety assessment were suitably qualified and experienced.
Arg 4.1
All hazards from e-FUA OI-1B have been identified and correctly analysed
Arg 4.2
Probable causes of the e-FUA OI-1B hazards have been identified and correctly analysed
Arg 4.3
FHA / PSSA processes were appropriate, adequate and completely and correctly followed
Arg 4.4
The outputs of the FHA / PSSA processes were subjected to independent review
Arg 4.5
All active participants in the FHA /PSSA process were competent to carry out their roles
Ev
OSC Sect 6.2
Ev
OSC Sect 6.2
Ev
OSC Sect 6.2
Ev
OSC Sect 6.2
Ev
OSC Sect 6.2

APPENDIX I

FHA/ PSSA Process on Flexible Use of Airspace: Briefing Material

Contents

I. FHA/ PSSA PROCESS ON FUA: BRIEFING MATERIAL

I.1 Introduction

The Functional Hazard Assessment/ Preliminary System Safety Assessment Process on the Enhanced Flexible Use of Airspace Operational Improvement 1B (OI-1B) and OI-2B issued some briefing documents to meeting participants. This appendix provides copies of these documents "as issued" as a record of the process that was performed.

I.2 Briefing Documents Issued to the "Dry Run" Participants

The text below is the briefing material for the FHA/ PSSA "Dry Run" meeting participants.

Enhanced FUA Process Functional Hazard Assessment (FHA)
"Dry Run" Briefing Material

Background to Flexible Use of Airspace

The Flexible Use of Airspace (FUA) Concept is intended to provide the maximum flexibility to all airspace users in a seamless fashion across all ECAC states. Basic FUA was introduced in 1996. By the end of 1998 Basic FUA was implemented in 13 ECAC states and is currently implemented in almost all ECAC states.

The Enhanced FUA Process is a coherent set of actions directed at contributing to a single European Sky sometime after 2015. The actions are grouped into related Directions for Change (DfC). The subject of this project concerns the actions within the DfC "Airspace Management & Civil/Military Co-ordination"; this DfC is designated DfC B in EUROCONTROL's Airspace Strategy document (EUROCONTROL, 2001). Other DfCs, such as "Simplification of Airspace Organisation" are designated as DfCs A to G inclusive.

Within DfC B, the following 6 Operational Improvements (OI-1B to OI-6B) have been identified along with the stated target implementation timeframe:

OI-1B Enhance real-time civil/ military co-ordination, to be complete by 2000.
OI-2B National collaborative/ integrated airspace planning, to be complete by 2003.
OI-3B Extend FUA to lower airspace, to be complete by 2005.
OI-4B Enhance FUA with dynamic airspace allocation and harmonise OAT/ GAT handling throughout Europe, to be complete by 2008.
OI-5B Collaborative European airspace planning, to be complete by 2010.
OI-6B Integrated European airspace, to be complete by 2015.

In the context of the present project, these 6 operational improvements (OI-1B to OI-6B inclusive) are collectively defined as the Enhanced FUA Process. However the FHA will first address OI-1B and will only address OI-2B if time is available.

Within FUA, airspace use is planned with reference to 3 organisational levels:

- Level 1 concerns strategic planning months or years in advance of use;
- Level 2 concerns pre-tactical planning up to 1 day in advance of use; and
- Level 3 concerns tactical planning and co-ordination on the day of operations.

OI-1B only impacts on Level 3, and OI-2B impacts mainly on Level 1.

Introduction to Functional Hazard Assessment

Functional Hazard Assessment (FHA) is the first stage in EUROCONTROL's Safety Assessment Methodology (SAM) (EUROCONTROL, 2000). In essence FHA aims to answer the questions:

- What is the proposed change to the system (system description)?
- What could go wrong as a result of introducing the proposed change (hazard identification)?
- What consequence(s) could arise from the identified hazards (how severe could the effects of the hazard be)?
- How likely are the identified hazards (probability assessment and estimation of the probability that can be tolerated for the estimated severity of the hazard)?
- What can be done to eliminate the hazard, or to reduce its probability and/ or severity (identification of risk reduction measures)?

EUROCONTROL now wish to apply the SAM to the Enhanced FUA Process and, in particular, to OI-1B and possibly OI-2B.

Objectives

The objectives of the Enhanced FUA Process FHA "dry run" are:

- To prepare and finalise the process for the full Enhanced FUA Process FHA. The FHA scope in terms of the system description and key assumptions should be clarified and issues that do not need to be considered should be flagged/ screened out. It is not intended that failure modes/ hazards are assessed in detail during this FHA "dry run"; that will be done in the full FHA.
- To identify key hazards, severities, likelihoods and mitigation measures to form a secure basis of the full FHA.
- To improve and finalise this briefing material.

The overall objective is to maximise the probability of executing a successful full FHA; this is an absolute prerequisite for the production of a timely, robust outline safety case for the Enhanced FUA Process.

Requirements from FHA Participants

The main requirements of the FHA meeting attendees are:

- To familiarise themselves with this briefing material before the meeting;
- To arrive promptly for the meeting start, since the meeting will begin with important information about the meeting process;
- At the meeting, be willing to brainstorm and contribute ideas and experiences.

Proposed Agenda

It is proposed that the main items of the FHA “dry run” will be as follows:

1. Discuss and define the initial system description presented below relevant to OI-1B.

2. Discuss and define any necessary assumptions concerning the safety assessment of OI-1B that may be relevant. An initial assumption set is provided below.

3. Having better defined the relevant system elements and assumptions in 1 and 2 for OI-1B, we propose to conduct a simple brainstorming session where key tasks and functions relevant to the pilot (OAT or GAT), ATC (military or civil), and others are stepped through and example hazards identified and discussed. Such a session should test and clarify the discussions held in items 1 and 2. For example, has the system description been adequately defined, are extra operational or environment assumptions required etc. It is proposed that this brainstorming session would be structured by:

    a. Considering the key FUA airspace structures/ procedures, such as Conditional Routes (CDR 1, CDR 2 and CDR 3), Temporary Reserved Areas (TRA), Temporary Segregated Areas (TSA), Cross Border Areas (CBA), Prior Co-ordination Airspace (PCA), Reduced Co-ordination Airspace (RCA), Restricted areas (R), Danger areas (D) and Prohibited areas (P).
    b. Considering the tasks and roles of military and civil ATCOs, pilots of OAT and GAT, the Air Management Cell (AMC), the Flow Management Position (FMP), the Centralised Airspace Data Function (CADF) and any other relevant actors.
    c. Considering relevant flight phases (pre-departure, departure, climb, en-route, transition from controller to controller, transition from country to country (ECAC to ECAC and ECAC to non-ECAC), descent, transition to final approach, final approach and missed approach) and discussing pilot and ATC tasks from that viewpoint. The current understanding is that only those flight phases in controlled upper airspace are relevant to the Enhanced FUA Process.
    d. Considering the lifecycle of key support equipment (e.g. commissioning, calibration, normal operation, maintenance, decommissioning).
    e. Considering the manning pattern lifecycle (e.g. staff new to role, shift change-over, others?)
    f. Considering any other factors/ roles etc that the meeting participants think are relevant.

Key safeguards and hazard severities (consequences) may also be noted alongside the hazards, but systematic evaluation of the hazards will be performed in the full FHA, not in the “dry run”.

4. Consider improvements to this briefing material.

If time allows, steps 1 to 3 will be repeated for OI-2B.

The above agenda is flexible and can be adapted according to the opinions of the participants at the "dry run". It is proposed that the discussions will be led by a facilitator with on-line notes being projected so that all participants can provide immediate corrections in the event of misunderstanding. A copy of the minutes will be provided post-meeting to allow further comments.

System Description

In order to perform a safety assessment of part of the ATM system (clearly a full assessment of the entire ATM system would be a very large undertaking outside of the scope of the present project) it is necessary to be able to describe the system before making the change, and to be able to describe the changes that will be made (or have been made). It is then possible to consider if old hazards have been reduced or eliminated or new (hopefully lower risk) hazards have been introduced. It is helpful to define a typical system description, even though we recognise that this will differ from country to country or time to time. Important deviations from the typical system description may also need to be identified and considered.

It should be noted that the system change that is under study in this project is the transition from Basic FUA to the Enhanced FUA Process. Implicit in this choice of the safety assessment process is the assumption that Basic FUA, as currently implemented by the majority of ECAC states, is acceptably safe.

System Elements/ Assumptions for Basic FUA

- Current CNS/ ATM capabilities. Primary radar assumed for both OAT and GAT (stealth aircraft assumed not detected by primary radar). Secondary radar surveillance of OAT and GAT by military-ATC and GAT by civil-ATC assumed. VHF voice communication assumed between civil-ATC and GAT and between military-ATC and OAT.
- Civil-Military ATC co-ordination. Voice communication over land telephone line only.
- Aircraft performance. All GAT fitted with collision avoidance equipment such as TCAS. All GAT, OAT and military aircraft assumed to be detected by TCAS.
- Traffic characteristics. Density (lateral, longitudinal and vertical), speed distributions. What should be assumed? Is it critical to the outcome of the FHA?
- The assessment will only consider GAT/ OAT interactions (and GAT/ GAT interactions which arise because of OAT presence) within controlled upper airspace.
- Introduction of OI-1B and OI-2B is assumed to be independent of each other and all other OIs from all the DfCs.

Basic FUA

EUROCONTROL guidance (EUROCONTROL, 2003b) describes criteria for the achievement of Basic FUA as follows:

- Adoption of the FUA concept by the State.
- Information process to communicate FUA nationally.
- Establishment of a National High Level Body at Level 1.
- Assessment of the current airspace and route structures and introduction of flexible airspace structures, such as conditional routes.
- Promulgation of FUA structures, for example in the national AIP.
- Implementation of the AMC or focal point.
- Introduction of the ACA software in the AMC.
- Identification of the Approved Agencies (AAs).
- Education of Flow Management Positions (FMPs)/Area Control Centres (ACCs) on FUA Level 2 functions.
- Establishment of liaison between all parties concerned at Level 2.
- Establishment of ASM Level 2 procedures.
- Implementation of real-time civil/military co-ordination procedures at Level 3. *Implement real-time civil/military controller to controller co-ordination procedures agreed by the civil and military authorities and published in Letters of Agreement (LoAs).*
- Upgrading of ATM system at Level 3. *Upgrade ATM tools and communication facilities between civil and military ATS providers in order to allow :*
    - *direct controller to controller communications with the use of direct telephone line;*
    - *the automated exchange of flight data from the civil to the military controller, including the position and intention of the GAT;*
    - *the provision of national and/or international (CBA) airspace-use data to the control staff concerned with the use of the phone and the fax;*
    - *the use of airspace crossing function based on direct communication facilities (telephone).*

The last 2 main bullet points are particularly relevant to OI-1B.

OI-1B – Enhanced Real Time Civil-Military Co-ordination

EUROCONTROL guidance (EUROCONTROL, 2003b) describes the criteria for the achievement of Enhanced FUA OI-1B as follows:

Enhancement of ATM system at Level 3. (Improvement of the Basic FUA criteria 13)
Enhance ATM tools and communication facilities between civil and military ATS providers in order to allow:

- direct controller to controller communications based on system supported dialogues;
- the automated exchange of flight data from the military to the civil controller, including the position and intention of the OAT;
- the provision of national and/or international (CBA) airspace-use data to the control staff concerned with the use of a harmonised system supported tool;
- the use of airspace crossing function based on system supported dialogues.

Comparison of the Basic FUA and Enhanced FUA criteria indicates the following key changes introduced/ required by OI-1B:

- Direct controller to controller communications based on system supported dialogues (automated exchange of data between civil and military ATCOs using either active silent or passive communication modes), in addition to direct telephone line (Basic FUA).
- The provision of national and/or international (CBA) airspace-use data to the control staff concerned with the use of a harmonised system supported tool (the same tools used by all actors), in addition to the use of phone/fax (Basic FUA);
- The use of airspace crossing function based on system supported dialogues, in addition to the use of direct communication (telephone – Basic FUA).

Furthermore, in Section 5.2 of The ECAC Airspace Management Handbook (EUROCONTROL, 2003a) it highlights a number of modes of civil-military co-ordination (active-verbal, active-silent and passive). The active-silent and passive modes of co-ordination are introduced as OI-1B.

OI-2B - National collaborative/ integrated airspace planning

EUROCONTROL guidance (EUROCONTROL, 2003b) describes the criteria for the achievement of Enhanced FUA OI-2B as follows:

National Collaborative/Integrated Airspace Planning.

- Publish a National Airspace Charter defining the authorities, responsibilities and principles by which the National High-Level Airspace Policy Body conducts the planning of airspace.
- Apply common procedures and guidelines.
- Revise existing Agreements between national civil and military authorities to update accordingly airspace policy and planning rules.

Furthermore, in Section 3.2.1 of The ECAC Airspace Management Handbook it highlights 6 strategic objectives of national collaborative airspace planning.

The participants of the “dry run” meeting may first need to identify the tangible differences in operations that result from implementation of OI-2B in order to be able to conduct an FHA. It is also possible that the skills and experiences required from the meeting participants to consider OI-2B effectively may be different from those sought to consider OI-1B. These issues will be considered during the “dry run” meeting.

FHA Process

The FHA process will be a structured brainstorming of possible hazards associated with the introduction of OI-1B of the Enhanced FUA Process, as described above under “Proposed Agenda”.

Anticipated FHA Outputs

Without pre-judgment, DNV anticipate that the following main hazard will be identified:

- Unplanned loss of separation between GAT and OAT.

However 2 other "second order" high-level hazards may also be feasible:

- Unplanned loss of separation between GAT and GAT that arises from GAT/ OAT interaction;
- Unplanned loss of altitude of GAT leading to possible Controlled Flight Into Terrain (CFIT) that arises because of the presence of OAT.

However the important output from the FHA will be the underlying contributory causes of the above high level hazards. Thus, without prejudgment, the anticipated outputs from the "dry run" FHA might look like Table 1, whereas the full FHA outputs might look like Table 2.

References and Additional Reading

EUROCONTROL, 2000: "Functional Hazard Assessment", SAM SAF.ET1.ST03.1000-MAN-01-00.

EUROCONTROL, 2001: "EUROCONTROL Airspace Strategy for ECAC States", ASM.ET1.ST03.4000-EAS-01-00, Edition 1.0, 18/01/01.

EUROCONTROL, 2003a: "ECAC Airspace Management (ASM) Handbook", ASM.ET1.ST08.5000-HBK-02-00, Edition 2.0, 16 May 03.

EUROCONTROL, 2003b: "Guidance Document for the Implementation of the Concept of the Flexible Use of Airspace", ASM.ET1.ST08.5000-GUI-02-00, Edition 2.0, 18/08/03.

Abbreviations and Acronyms

CBA	Cross Border Area
CDR	Conditional Route
DfC	Direction for Change
ECAC	European Civil Aviation Conference
FHA	Functional Hazard Assessment
FUA	Flexible Use of Airspace
GAT	General Air Traffic
OAT	Operational Air Traffic
OI	Operational Improvement
PCA	Prior Co-ordination Area
RCA	Reduced Co-ordination Area
SAM	Safety Assessment Methodology
TSA	Temporary Segregated Area

Table 1 Anticipated "Dry Run" FHA Outputs (Example)

FUA Structure	Flight Phase	Hazard	Example Comments
CDR 1	En-route	GAT flies CDR 1 when route is withdrawn	

Table 2 Anticipated Full FHA Outputs (Example)

FUA Structure	Flight Phase	Hazard	Consequence	Cause	Current/ planned Safeguards	Severity (absolute scale)	Severity (relative to Basic FUA)	Recommend-ations / Comments
CDR 1	En-route	GAT flies CDR 1 when route is withdrawn	Loss of separation OAT / GAT	Poor communication	Defined procedures for correct communication	?	Similar or lower than Basic FUA due to improved communication channels in enhanced FUA	

I.3 Briefing Documents Issued to the “Full FHA/ PSSA” Participants

The text below is the briefing material for the Full FHA/ PSSA meeting participants.

Enhanced FUA Process Functional Hazard Assessment (FHA) Briefing Material – 25 and 26 November 2003

Background to Flexible Use of Airspace

The Flexible Use of Airspace (FUA) Concept is intended to provide the maximum flexibility to all airspace users in a seamless fashion across all ECAC states. Basic FUA (b-FUA) was introduced in 1996. By the end of 1998 b-FUA was implemented in 13 ECAC states and is currently implemented in almost all ECAC states.

The Enhanced FUA Process (e-FUA) is a coherent set of actions directed at contributing to a single European Sky sometime after 2015. The actions are grouped into related Directions for Change (DfC). The subject of this project concerns the actions within the DfC "Airspace Management & Civil/Military Co-ordination"; this DfC is designated DfC B in EUROCONTROL's Airspace Strategy document (EUROCONTROL, 2001c).

Within DfC B, the following 6 Operational Improvements (OI-1B to OI-6B) have been identified along with the stated target implementation timeframe:

OI-1B	Enhance real-time civil/ military co-ordination, to be complete by 2000.
OI-2B	National collaborative/ integrated airspace planning, to be complete by 2003.
OI-3B	Extend FUA to lower airspace, to be complete by 2005.
OI-4B	Enhance FUA with dynamic airspace allocation and harmonise OAT/ GAT handling throughout Europe, to be complete by 2008.
OI-5B	Collaborative European airspace planning, to be complete by 2010.
OI-6B	Integrated European airspace, to be complete by 2015.

In the context of the present project, these 6 operational improvements (OI-1B to OI-6B inclusive) are collectively defined as the Enhanced FUA Process. However the FHA will first address OI-1B and will only address OI-2B if time is available.

Within FUA, airspace use is planned with reference to 3 organisational levels:

- Level 1 concerns strategic planning months or years in advance of use;
- Level 2 concerns pre-tactical planning up to 1 day in advance of use; and
- Level 3 concerns tactical planning and co-ordination on the day of operations.

OI-1B only impacts on Level 3, and OI-2B impacts mainly on Level 1.

Introduction to Functional Hazard Assessment

Functional Hazard Assessment (FHA) is the first stage in EUROCONTROL's Safety Assessment Methodology (SAM) (EUROCONTROL, 2000a). In essence FHA aims to answer the questions:

- What is the proposed change to the system (system description)?
- What could go wrong as a result of introducing the proposed change (hazard identification)?
- What consequence(s) could arise from the identified hazards (how severe could the effects of the hazard be)?
- How likely are the identified hazards (probability assessment and estimation of the probability that can be tolerated for the estimated severity of the hazard)?
- What can be done to eliminate the hazard, or to reduce its probability and/ or severity (identification of risk reduction measures)?

EUROCONTROL now wish to apply the SAM to the Enhanced FUA Process and, in particular, to OI-1B.

Objectives

The objectives of the Enhanced FUA Process FHA are:

- To agree the final form of the system description and key assumptions on which the FHA and remaining e-FUA safety assessment activities will be based;
- To identify all hazards, or potential hazards, associated with b-FUA and the changes that result from implementing OI-1B (and OI-2B if there is time);
- To assess the effect of the changes introduced by OI-1B on the existing b-FUA hazards and to assess the importance of any new hazards introduced by e-FUA OI-1B;
- To analyse the interrelationship between hazards and their contributory causes; and
- To identify existing and potential risk mitigation measures that could be applied to reduce risks.

The outputs from the FHA will be a crucial component of the Outline Safety Case for OI-1B.

Requirements from FHA Participants

The main requirements of the FHA meeting attendees are:

- To familiarise themselves with this briefing material before the meeting;
- To arrive promptly for the meeting start, since the meeting will begin with important information about the meeting process;
- At the meeting, be willing to brainstorm and contribute ideas and experiences.

Proposed Agenda

An outline agenda is presented below. However, the meeting will be flexible so deviations may arise. OI-2B will be considered if time permits.

Tuesday 25 November

10.00	Meeting start and introductions
10.15	System description and key assumptions
11.00	Coffee
11.15	Hazard brainstorming for b-FUA and changes due to OI-1B
12.30	Lunch
13.30	Analysis of hazards
14.45	Coffee
15.00	Analysis of hazards
16.30	Meeting close

Wednesday 26 November

09.30	Meeting start and recap
09.45	Analysis of hazards
10.45	Coffee
11.00	Analysis of hazards
12.30	Lunch
13.30	Analysis of hazards
14.45	Coffee
15.00	Analysis of hazards
16.00	Meeting close

System Description

In order to perform a safety assessment of part of the ATM system it is necessary to be able to describe the system before making the change, and to be able to describe the system changes that are to be assessed. It is then possible to consider if old hazards have been reduced or eliminated or new (hopefully lower risk) hazards have been introduced. It is helpful to define a typical system description, even though it is recognised that this will differ from country to country or time to time. Important deviations from the typical system description may also need to be identified and considered.

It should be noted that the system change that is under study in this project is the transition from Basic FUA to the Enhanced FUA Process. Implicit in this choice of the safety assessment process is the assumption that Basic FUA, as currently implemented by the majority of ECAC states, is acceptably safe.

The information presented in Table 1 gives the proposed system description and key assumptions for the FHA.

Table 1 Proposed System Description and Key Assumptions

Base Case System Description/ Assumption	Comment/ Variation between States
• Civil and military controllers are separate entities and are not co-located.	Assume this as the base case. Then review for various levels of integration (co-location of military and civil controllers, fully integrated ATC – controllers direct both GAT and OAT).
• Scope of assessment limited to: o Upper airspace (above FL195) o Class C airspace with no GAT flying VFR. o Assessment of hazards that can result in loss of separation between GAT and OAT. o Within state co-ordination issues.	OI-3B will cover lower airspace. OI-5B1 will cover Cross Border Areas.
• CNS/ ATM capabilities. o Primary radar assumed for both OAT and GAT (stealth aircraft assumed not detected by primary radar). o Secondary radar surveillance of OAT by military-controller and GAT by civil-ATC assumed respectively. o GAT detected directly by military secondary radar. o OAT detected directly by civil secondary radar. o VHF voice communication assumed between civil-ATC and GAT and between military-ATC and OAT.	Primary radar might only be in place en-route for military. Extent of coverage and variation between states unknown. Variable between states. Variable between states. Civil secondary radar detects Modes A and C. Rapid maneuvering OAT traffic may not be detected. Primarily UHF for military. Voice communication between controller and pilot (civil-civil and military-military) is assumed (civil-military voice communication may exist in some states).
• Civil-Military ATC co-ordination. Voice communication over land telephone line only.	This should already be in place for b-FUA. If not, then States are non-compliant with b-FUA.
• Aircraft performance. o TCAS cannot be assumed for all GAT flights. o Only OAT formation leader will be detected by TCAS.	
• Traffic characteristics. Density (lateral, longitudinal and vertical), speed distributions. No assumptions made.	
• Ultimate responsibility for separation lies with the pilot, but for purpose of FHA, IFR separation responsibility lies with air traffic control. Responsibility between m-controller and c-ATCO is subject to negotiation (letter of agreement). Responsibility for OAT/GAT separation usually belongs to military controller.	
• Introduction of OI-1B and OI-2B is assumed to be independent of each other and all other OIs from all the DfCs (order of introduction assumed not critical)	Review effect of this assumption later.

Basic FUA

The minimum requirement for b-FUA is that there is direct c-ATCO to military controller telephone and fax communication.

OI-1B – Enhanced Real Time Civil-Military Co-ordination

Comparison of the b-FUA and e-FUA indicates the following key changes introduced/ required by OI-1B:

1. Direct controller to controller communications, using a **silent mode** of co-ordination based on system supported dialogues with the use of **airspace crossing function** (XIN, XRQ, XAP, ACP & REJ messages) **(e-FUA)**, in addition to the use of verbal mode of communication with direct telephone line between the civil and military ATCO (b-FUA).
2. Automated exchange of **flight data,** using a **passive mode** of co-ordination, **from the military to the civil ATCO**, including the **position and intention of the OAT** flight **(e-FUA)**, in addition to the automated exchange of flight data (passive mode of co-ordination) from the civil to the military ATCO, including the position (BFD message) and intention (CFD message) of the GAT flight (b-FUA).
3. The provision of national (TSA/TRA, R/D) and/or international (CBA) airspace-use data to the control staff concerned with the use of a harmonised system supported tool (the same tools used by all actors fed with data from the common Airspace Data Repository) **(e-FUA)**, in addition to the use of phone/fax (b-FUA).

Thus

- **Change 1** entails the provision of **"silent" flight data** exchange protocols (XIN, XRQ, XAP, ACP & REJ messages) in support to the **airspace crossing function between military controller and civil controllers** within their respective areas of responsibility in accordance with LoAs established between the civil and military ATS units concerned
- **Change 2** entails the provision of **"passive" flight data** exchange protocols (BFD, CFD messages) **from military controller to civil controller** within their respective areas of responsibility in accordance with LoAs established between the civil and military ATS units concerned.
- **Change 3** entails the provision of **airspace-use data** exchange protocols, using a harmonised system support tool, between all the actors concerned initially within a country (*airspace status of national CDR*, *TSA/TRA*, *R/D*) [OI-1B] and later on across boundaries (*airspace status of international CDR*, *CBA*) [OI-5B1].

High-Level Hazards of OI-1B and Proposed Functional Model for FUA

Preliminary analysis indicates the following two high-level hazards:

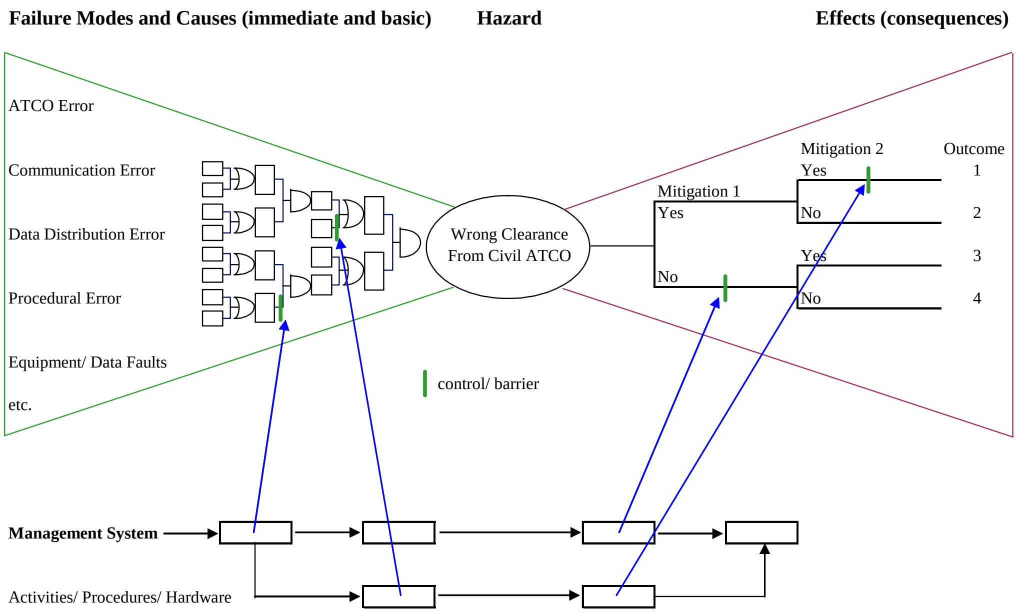
- A civil controller gives an incorrect clearance to GAT;
- A military controller gives an incorrect clearance to OAT.

A functional model for FUA based on these two hazards is presented in Figure 1 (landscape format at the end of this briefing material).

“Bow-Tie” Models

Bow-tie models are so-called because of their shape, see Figure 2. The centre of the bow-tie is the hazard under consideration. To the left of the bow tie are the contributory causes of the hazard structured in a fault tree. To the right of the bow tie are the possible outcomes of the hazard structured in an event tree. One objective of the FHA is to develop this analysis using the expert judgment of the group, and to identify possible risk mitigation measures.

Figure 2 Example Bow-Tie Model for FUA



Risk analysts break-down the risks associated with a hazard in terms of the frequency of occurrence (how often does the hazard arise) and the consequence of the hazard (assuming the hazard has occurred, how bad will is it). Within the bow-tie, hazard frequencies are to the left of the hazard (in the fault tree) and hazard consequences are to the right of the hazard (in the event tree). Risks can be reduced by reducing the hazard frequency, the hazard consequence or both through the application of risk mitigation measures.

The FHA will aim to both identify factors that could affect hazard frequency and consequence and to assess how the frequencies and consequences of existing hazards have changed as a result of implementing e-FUA OIs.

OI-2B - National collaborative/ integrated airspace planning

If time allows, we will attempt to apply the above approach to OI-2B which concerns National collaborative/ integrated airspace planning. Brief introductory notes are provided below.

EUROCONTROL guidance (EUROCONTROL, 2003d) describes the criteria for the achievement of Enhanced FUA OI-2B as follows:

National Collaborative/Integrated Airspace Planning.

- Publish a National Airspace Charter defining the authorities, responsibilities and principles by which the National High-Level Airspace Policy Body conducts the planning of airspace.
- Apply common procedures and guidelines.
- Revise existing Agreements between national civil and military authorities to update accordingly airspace policy and planning rules.

In order to apply the FHA process to OI-2B it will first be necessary to identify the tangible differences in operations that result its implementation perhaps by reference to the functional model shown in Figure 1 below.

References and Additional Reading

EUROCONTROL, 2000a	“Functional Hazard Assessment”, SAM SAF.ET1.ST03.1000-MAN-01-00
EUROCONTROL, 2000b	“Use of Safety Management Systems by ATM Service Providers”, EUROCONTROL Safety Regulatory Requirement (ESARR) 3, Edition 1.0, Released Issue.
EUROCONTROL, 2001a	“EATMP Safety Policy”, Edition 2.0.
EUROCONTROL, 2001b	"Risk Assessment and Mitigation in ATM", EUROCONTROL Safety Regulatory Requirement (ESARR) 4, Edition 1.0.
EUROCONTROL , 2001c	“EUROCONTROL Airspace Strategy for ECAC States”, ASM.ET1.ST03.4000-EAS-01-00, Edition 1.0, 18/01/01.
EUROCONTROL, 2003d	“Guidance Document for the Implementation of the Concept of the Flexible Use of Airspace”, ASM.ET1.ST08.5000-GUI-02-00, Edition 2.0, 18/08/03.

Abbreviations and Acronyms

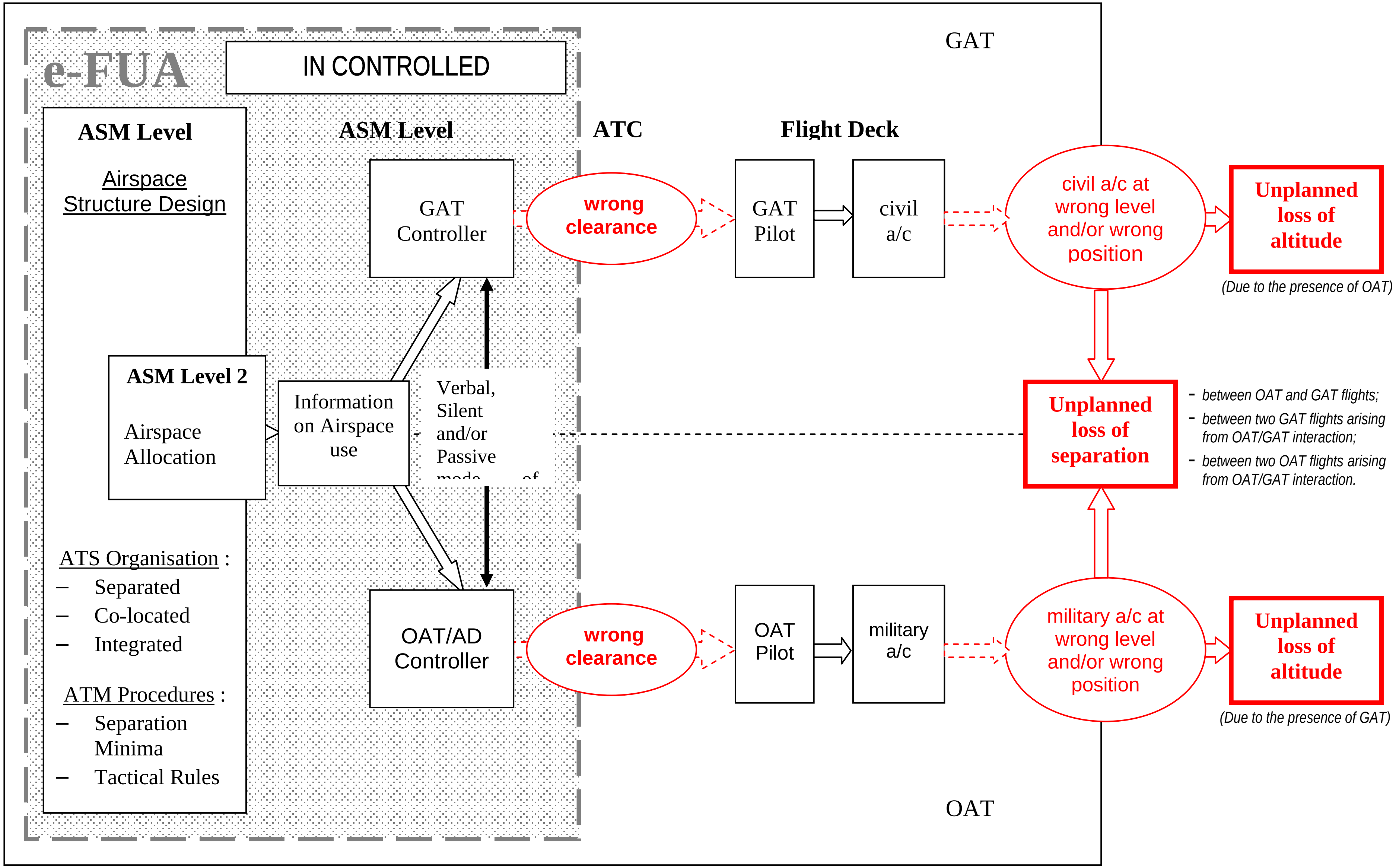
AFN	Airspace/ Flow Management and Navigation Business Division
AMC	Air Management Cell
ANSP	Air Navigation Service Provider
ATCO	Air Traffic Controller
ATM	Air Traffic Management
ATS	Air Traffic Service
ATSP	Air Traffic Service Provider
BFD	Basic Flight plan Data
CBA	Cross Border Area

CDR	Conditional Route, of types: CDR 1, CDR 2 and CDR 3
CFD	Current Flight plan Data
CFIT	Controlled Flight Into Terrain
CRAM	Conditional Route Availability Message
CRM	Collision Risk Modelling
D	Danger area
DAS	EUROCONTROL Directorate of ATM Strategies
DfC	Direction for Change
EATMP	European Air Traffic Management Programme
ECAC	European Civil Aviation Conference
ESARR	EUROCONTROL Safety Regulatory Requirement
FHA	Functional Hazard Assessment
FUA	Flexible Use of Airspace
GAT	General Air Traffic
OAT	Operational Air Traffic
OI	Operational Improvement
P	Prohibited area
PCA	Prior Co-ordination Airspace
PSSA	Preliminary System Safety Assessment
R	Restricted area
RCA	Reduced Co-ordination Airspace
SRC	Safety Regulatory Commission
SRU	Safety Regulatory Unit
SSA	System Safety Assessment
TAA	Temporary Airspace Allocation
TRA	Temporary Reserved Area
TSA	Temporary Segregated Area

Prefixes

b-	basic
c-	civil
e-	enhanced
m-	military

Figure 1 FUA Functional Model


e-FUA
IN CONTROLLED
GAT
ASM Level
Airspace Structure Design
ASM Level
ATC
Flight Deck
GAT Controller
wrong clearance
GAT Pilot
civil a/c
civil a/c at wrong level and/or wrong position
Unplanned loss of altitude
(Due to the presence of OAT)
ASM Level 2
Airspace Allocation
Information on Airspace use
Verbal, Silent and/or Passive mode of
Unplanned loss of separation
- between OAT and GAT flights;
- between two GAT flights arising from OAT/GAT interaction;
- between two OAT flights arising from OAT/GAT interaction.
ATS Organisation :
– Separated
– Co-located
– Integrated
ATM Procedures :
– Separation Minima
– Tactical Rules
OAT/AD Controller
wrong clearance
OAT Pilot
military a/c
military a/c at wrong level and/or wrong position
Unplanned loss of altitude
(Due to the presence of GAT)
OAT

APPENDIX II

FHA/ PSSA Meeting on Flexible Use of Airspace: Meeting Note

Contents

II. FHA/ PSSA MEETING ON FLEXIBLE USE OF AIRSPACE

II.1 Introduction

A Functional Hazard Assessment/ Preliminary System Safety Assessment meeting was held to discuss and agree the hazards that could arise from implementing Operational Improvement 1B (OI-1B) and OI-2B within the Enhanced FUA Process.

This appendix contains the meeting note produced to document the process and outputs from the meeting, including hazard tables developed during the meeting. Comments subsequently received from meeting participants on the meeting note have been removed from version 3 of this appendix as they mainly related to OI-2B.

II.2 Enhanced FUA Process FHA/PSSA Meeting Note

Date: 25-26th November 2003

Location: Conference Room Vega, EUROCONTROL Head Quarters

Attendees: Tom Suffolk, EUROCONTROL AFN
Jean-Paul Lemaire (JPL), EUROCONTROL AFN
Dr. Bernd Tiemeyer, EUROCONTROL – morning 25th only
Per Coulet, EUROCONTROL
Lt. Cl. Eric Chatelus, Dircan – 25th only
Mike Strong, EUROCONTROL MIL BD
Zlatko Meic, EUROCONTROL
Benoit Fonck, CFMU/URB
Mervyn Oliver, EUROCONTROL
Holger Ahrens (HA), DFS
Stu Wain, UK MOD (through HQ NATO) – 25th only
Sqn Ldr Dave Raine, DAP, CAA UK
Mike Steinfurt, EUROCONTROL SD/MIL
Tim Fowler (TF), Det Norske Veritas
Helen Jones, Det Norske Veritas

Introduction

JPL introduced the meeting, then handed over to TF. TF outlined the objectives of the meeting which were:

1. To discuss and agree the base case system description and key assumptions for b-FUA (Basic FUA). These will form the foundation for the Outline Safety Case for Operational Improvement 1B (OI-1B).

2. To agree the operational differences resulting from the implementation of OI-1B and identify the hazards associated with these operations.

3. Assess whether the hazards identified are existing hazards or if they are new to e-FUA (Enhanced FUA). If the hazards are seen to be new or altered by e-FUA, the

consequences and frequency of the hazard will be re-assessed by the group. These hazards can then be mapped onto the functional model to see if it is complete or should be amended.

4. Provide recommendations for the implementation of each of the three changes to ensure that that risks are managed effectively and reduced where possible.

5. Repeat steps 1-4 for OI-2B if time permitted.

System Description and Key Assumptions for FUA

The e-FUA concept was described. Then a PowerPoint presentation was used to describe the risk analysis concepts and the proposed FUA functional model. The three key changes for OI-1B were outlined as below:

Change 1: Communication of Traffic Situation – Passive Mode
The automated exchange of flight data from the military to the civil controller, including position and intention of the OAT (e-FUA, "Passive" mode). This is in addition to the automated exchange of flight data (passive mode co-ordination) from the civil to the military controller including position (BFD message) and intention (CFD message) of the GAT aircraft (b-FUA).

Change 2: Airspace Crossing Dialogue – Silent Mode
Direct controller to controller communications and use of the airspace crossing tool based on system supported dialogues for co-ordination (e-FUA, "Silent" mode). This is in addition to the existing verbal communications via direct telephone line between the civil and military controllers (b-FUA).

Change 3: Communication of Airspace Status – Harmonised Support Tool
The provision of national and/ or international (CBA) airspace use data to the control staff concerned with the use of a harmonised system support tool (the same tool used by all actors fed with data from the common Airspace Data Repository) (e-FUA). This is in intended to replace the use of telephone or fax (b-FUA).

A proposed functional model for FUA was explained to the group to provide a reference point throughout the discussions.

Having described the proposed changes under OI-1B, the proposed assessment assumptions were presented and discussed. Amendments to the proposed assumptions were accepted at this point in the meeting, and also after review (for their relevance to OI-1B) at the end of the meeting. The final system assumptions are shown in Table II.1 (appended).

Hazard Identification and Hazard Assessment for OI-1B (Day 1)

The assessment process was presented and the brainstorming hazard identifications session then began. A list of actors and modes of communication were generated to act as a checklist during the brainstorming session, see Tables II.2 and II.3 appended.

The group first identified the hazards associated with b-FUA (since the risks of such hazards could be affected by e-FUA), see Table II.4 Rows 30-63 inclusive. The group then identified the hazards associated with each of the three OI-1B changes in turn, see Table II.4 Rows 1-29 inclusive.

During the last session of the first day, the group identified a range of consequences that could arise from these hazards, and the possible mitigation measures (or safeguards) that can be used to reduce the severity of these consequences (Table II.4, Row 64).

Hazard Analysis for OI-1B (Day 2)

The hazards identified on Day 1 were prioritised in terms of their direct relation to the three OI-1B changes. The group then analysed each hazard in turn, as recorded in Table II.4.

Day 2 closed with a brainstorm of the key advantages of introducing OI-1B. The results are as follows:

- Increased capacity of airspace / more efficient airspace utilisation.
- Greater commonality between states.
- Improved civil-military coordination.
- Reduced coordination controller workload via silent mode (different participants had different views on this item).
- Improved awareness of traffic situation (civil controllers will know the intentions of OAT controllers under OI-1B of e-FUA, whilst military controllers should know the intentions of civil controllers under b-FUA). (It should be noted that some may argue that civil controllers do not need to know the intentions of OAT, provided that military controllers maintain OAT to GAT separations in excess of the minimum agreed in LoA.)
- Increased accuracy of airspace status information.
- Creates short-term access to large volume training airspace for OAT. Design permitted.
- Increased reliability of maintaining separation (safety).

OI-1B Hazards not Assessed during the Meeting

There was insufficient time to assess all the hazards that were identified on Day 1. However, on review, DNV considered that many of the issues had been addressed already via another hazard and this post-meeting analysis is represented in Table II.4, Rows 30-63 inclusive.

Operational Improvement 2B (OI-2B)

There was also insufficient time to consider OI-2B. OI-2B concerns the promotion of National Collaborative/ Integrated Airspace Planning. EUROCONTROL has described the essential differences between b-FUA and e-FUA for this Operational Improvement in the terms of the following 3 key criteria.

1. Airspace Structure Design : Once the National High-Level Airspace Policy Body has been established within a State (b-FUA), **publish a National Airspace Charter** defining the authorities, responsibilities and principles in terms of Safety, Consultation, Co-operation and Environment **by which the National High-Level Policy Body conducts**

the planning of airspace in a more collaborative working organisation involving all airspace users and ATS providers, civil and military **(e-FUA)**.

2. ATS Organisation : Revise existing Agreements between national civil and military authorities (b-FUA) to **update airspace policy and planning rules** in order to ensure that the Airspace Change processes, procedures and instructions of use are **compatible with appropriate Military and Civil Aviation safety requirements (e-FUA)**.
3. ATM Procedures : **Apply common procedures and guidelines to better accommodate the shared use of airspace between all users groups (e-FUA)**.

Thus

- **Change 1** entails the building of confidence and respect between airspace regulators and all other stakeholders through consultation and co-operation providing fair and effective regulation of the airspace system.
- **Change 2** entails working to maintain and actively seek to improve the safe and effective management of the airspace and its supporting infrastructure while improving standards of service through effective planning and monitoring of the high level body's key processes and activities.
- **Change 3** entails the shared use of national airspace by all user groups and later on the harmonisation of airspace management procedures with neighbouring States [OI-5B1].

With

- **Change 1**, airspace and route structures will be more correctly designed and the safety impact of any proposal for an airspace change considered in order to ensure that national and international plans evolve in an overall risk-reducing manner.
- **Change 2**, adequate civil and military co-ordination facilities and procedures will be provided to enhance safety and flexibility in the use of airspace.
- **Change 3**, application of common procedures will provide unambiguous rules which complement safe flight operations.

In future work EUROCONTROL will develop a description of OI-2B in terms of a functional model which defines which information is used by which actor at which time in the process. Such a model could be used as the basis for an FHA style hazard identification process.

Other Meeting Outputs

There was considerable discussion about the suitability of the names chosen for the 3 Changes introduced under OI-1B (especially passive mode and silent mode) and the exact meaning of each change. If more informative names can be identified it may help more general understanding. However such a change could also introduce confusion if the current names (silent mode etc) are already widely distributed. No suggestions were proposed.

Two final general points that apply to a number of hazards:

- OI-1B is intended to increase controller efficiency which will, in time, result in controllers handling more aircraft. If e-FUA fails (e.g. technical failure) then the consequences of such a failure are likely to be greater than when the ATM system is operating at lower intensity (as it has to under b-FUA).
- Any failures of e-FUA will require controllers to revert to b-FUA style co-ordination. Telephone based co-ordination methods should continue to be learned, and telephone lines retained, at least until such time as e-FUA has been demonstrated to be acceptably reliable.

II.3 Appendix Tables

Table II.1 Proposed b-FUA System Description and Key Assumptions for OI-1B

Base Case System Description/ Assumption	**Comment/ Variation between States**
• Real-time use of airspace allowing a safe OAT-GAT separation either through a joint use of airspace by appropriate civil-military co-ordination or the temporary reservation / segregation of airspace. • Civil and military controllers are separate entities and are not co-located.	Assume this as the base case. Relevant to OI-1B
• Scope of assessment limited to:	
o Controlled airspace above FL195.	OI-3B will cover airspace below FL195. Interaction with terminal airspace to be considered later.
o Class C airspace with no GAT flying VFR.	Relevant to OI-1B
o Assessment of hazards that can result in loss of separation between GAT and OAT / impact on controller workload.	Relevant to OI-1B
o Within state co-ordination issues.	OI-5B1 will cover Cross Border Areas.
o Excludes transfer of control	Relevant to OI-1B
• CNS/ ATM capabilities.	
o Primary radar assumed for both OAT and GAT.	Primary radar might only be in place en-route for military. Extent of coverage and variation between states unknown.
o Secondary radar surveillance of OAT by military-controller and GAT by civil-ATC assumed respectively.	Variable between states.
o GAT detected directly by military secondary radar.	
o OAT detected directly by civil secondary radar.	Variable between states. Civil secondary radar detects Modes A and C. Rapid manoeuvring OAT traffic may not be detected.
o VHF voice communication assumed between civil-ATC and GAT and between military-ATC and OAT.	Primarily UHF for military. Voice communication between controller and pilot (civil-civil and military-military) is assumed (civil-military voice communication may exist in some states). Relevant to OI-1B
• Civil-Military ATC co-ordination. Voice communication over land telephone line only.	This should already be in place for b-FUA. If not, then States are non-compliant with b-

Base Case System Description/ Assumption	**Comment/ Variation between States**
	FUA. Relevant to OI-1B
- Aircraft performance. o ACAS cannot be assumed for all GAT flights. o Only OAT formation leader will be detected by ACAS.	National variation on which aircraft in formation will squawk. Positive / negative impacts of ACAS to be considered later. Irrelevant to OI-1B
- Traffic characteristics. Density (lateral, longitudinal and vertical), speed distributions. No assumptions made.	Irrelevant to OI-1B
- Primary responsibility for separation lies with ATC. Responsibility between m-controller and c-ATCO is subject to co-ordination (according to letter of agreement). Responsibility for OAT/GAT separation usually belongs to military controller. Final responsibility for safety lies with the captain, but for purpose of FHA, IFR separation responsibility lies with air traffic control.	Significant variation between states Relevant to OI-1B
- No UAVs	Irrelevant to OI-1B
- Introduction of OI-1B and OI-2B is assumed to be independent of each other and all other OIs from all the DfCs (order of introduction assumed not critical)	Review effect of this assumption later. Relevant to OI-1B

Table II.2 Actors Relevant to OI-1B

Civil Controller
Military Controller
Air Defence Controller
Area Control Centre - Supervisors
Area Control Centre – Assistants
Air Operators
Airspace Manager
Airspace users (Approved Agencies)
CADF
CFMU
FMP

Table II.3 Communication Modes Relevant to OI-1B

Direct verbal (person-person, speak, listen and show)
Direct written
Indirect verbal (telephone, VHF, UHF)
Fax
Email
SMS
Datalink (by line ground to ground and by transmission air to ground)
Silent co-ordination
System supported communication
Flight data processing system (2ary radar)

Table II.4 Hazard Log – OI-1B

Note text in *italics* is detailed comment received after the FHA/ PSSA meeting from Holger Ahrens.

Row	Hazard	Exists in b-FUA or new	If hazard exists, frequency vs. b-FUA	If hazard exists, Consequence vs. b-FUA	Mitigation measures – existing and proposed	Possible Causes	Consequences	Additional comments
OI-1B Change 1 – Passive Mode								
1	Wrong intention entered	Passive: existing hazard	No change	No change	Training, standardisation, ATCO and system cross-checking, pilot feedback.	Human error	Increase in risk of loss of separation. Inaccurate data, increase in ATCO workload.	Loss of readback with the passive mode - one less mitigation opportunity. However, opportunity to re-check the written word. Automatic syntax checker could help
2	Intention not updated	Passive: existing hazard.	No change	No change	Training, standardisation, ATCO and system cross-checking, pilot feedback.	Human error	Increase in risk of loss of separation. Inaccurate data, increase in ATCO workload.	
3	Unfamiliarity with aircraft / controller's equipment	Passive: new information or systems but not a step change from existing practice	No change	No change	System cross checking, HMI design	Organisational failure – lack of systems, etc	Distraction, increase in ATCO workload.	Additional training required for new systems

Row	Hazard	Exists in b-FUA or new	If hazard exists, frequency vs. b-FUA	If hazard exists, Consequence vs. b-FUA	Mitigation measures – existing and proposed	Possible Causes	Consequences	Additional comments
4	Total loss of function through technical failure – assumed detected	Passive: existing hazard	No change	Consequence of system loss may be greater if passive mode increases numbers of aircraft handled.	Revert to standard co-ordination and separation procedures. Reduced capacity, system redundancy. System failure alerts / confirmation.	Technical failure, power loss, network failure, maintenance / human.	Increase in ATCO workload, reduction in traffic data exchange with other controllers, fewer aircraft handled leading to delays to aircraft.	Technical failure would result in a breakdown in e-FUA.
5	Partial loss of function through technical failure – this is detected data corruption	Passive: existing hazard	No change	Consequence of system loss may be greater if passive mode increases numbers of aircraft handled.	System failure alerts / confirmation. Notification from other controllers / supervisors. Revert to standard co-ordination and separation procedures.	Technical failure, network failure, detected data corruption of the function, partial power loss	Increase in ATCO workload. Greater coordination required.	E-FUA has an increase in passive data transfer compared to b-FUA. It would be possible to route an a/c based solely on passive data in e-FUA where procedures allow this.

Row	**Hazard**	**Exists in b-FUA or new**	**If hazard exists, frequency vs. b-FUA**	**If hazard exists, Consequence vs. b-FUA**	**Mitigation measures – existing and proposed**	**Possible Causes**	**Consequences**	**Additional comments**
6	Partial loss of function through technical failure – this is undetected data corruption	Passive: existing hazard	No change	Possible increase – consequence of system loss will be greater if passive mode increases aircraft numbers handled	System failure alerts / confirmation. Notification from other controllers / supervisors. Revert to basics.	Technical failure, network failure, undetected data corruption of the function, partial power loss?	Possible loss of separation. Increase in ATCO workload. Greater coordination required.	E-FUA has an increase in passive data transfer compared to b-FUA. It would be possible to route an a/c based solely on passive data in e-FUA where procedures allow this.
7	Controller fails to notice / respond to passive data	Passive: existing hazard	Increase – reduced probability of confirmation by telephone	No change	Radar display would show unanticipated activity. Existing rules still apply regarding civil and m-ATC coordination. Controller must be made aware of incoming data - possible colour coding? Telephone from m-ATCO on case by case basis.	Human error	Possible loss of separation. If information not read, impacts on the controller's picture / Situational Awareness. ATCO may base decisions on poor information.	The passive message serves as a written reminder to the receiving controller so may reduce likelihood of memory lapse. However, no response required to confirm that data has been read.

Row	Hazard	Exists in b-FUA or new	If hazard exists, frequency vs. b-FUA	If hazard exists, Consequence vs. b-FUA	Mitigation measures – existing and proposed	Possible Causes	Consequences	Additional comments
8	Data delayed – late input.	Passive: existing hazard	No change – possibly more data input required but less verbal coordination.	No change	Existing rules & SOPs still apply regarding civil and m-ATC coordination. Revert to b-FUA. Telephone from m-ATCO on case by case basis.	Human failure	Full intentions not available to c-ATCO on radar display.	Different displays in different states. Different controllers may have different pictures as a result. In b-FUA the sender will be aware of whether receiver has the data and can confirm with telephone. In e-FUA this is not clear.
9	Data delayed – delay in system delivery (detected)	Passive: as above	No change – possibly more data input required but less verbal coordination.	No change	Existing rules & SOPs still apply regarding civil and m-ATC coordination. Revert to b-FUA. Telephone from m-ATCO on case by case basis.	Technical failure	Full intentions not available to c-ATCO on radar display.	Different displays in different states. Different controllers may have different pictures as a result. In b-FUA the sender will be aware of whether receiver has the data and can confirm with telephone. In e-FUA this is not clear.

Row	Hazard	Exists in b-FUA or new	If hazard exists, frequency vs. b-FUA	If hazard exists, Consequence vs. b-FUA	Mitigation measures – existing and proposed	Possible Causes	Consequences	Additional comments
10	Data delayed – delay in system delivery (undetected)	Passive: existing hazard	No change.	No change	Radar display would show unanticipated activity. Existing rules & SOPs still apply regarding civil and m ATC coordination. Telephone from m-ATCO on case by case basis.	Technical failure	Possible loss of separation. If information not delivered, impacts on the controller's picture / Situational Awareness. ATCO may base decisions on poor information.	
11	Controller responds incorrectly to data	Passive: existing hazard	No change	No change	Training standardisation, c-ATCO.	Human error		
OI-1B Change 2 – Silent Mode								
12	Wrong intention entered	Silent: existing hazard, different mode	No change	No change		Human error – varies between b-FUA (verbal) and e-FUA (data entry).	*Inaccurate data, increase in ATCO workload*	*c-ATCO will be surprised by real intentions, thus his/her workload increases*
13	Intention not updated	Silent: existing hazard	No change	No change	Training, standardisation, ATCO and system cross-checking, pilot feedback.	Human error	Increase in risk of loss of separation. Inaccurate data, increase in ATCO workload.	

Row	Hazard	Exists in b-FUA or new	If hazard exists, frequency vs. b-FUA	If hazard exists, Consequence vs. b-FUA	Mitigation measures – existing and proposed	Possible Causes	Consequences	Additional comments
14	Unfamiliarity with aircraft / controller's equipment	Silent: existing hazard	No change	No change	Training, standardisation. System cross checking, HMI design..	Organisational failure – lack of systems, etc.	Distraction, increase in ATCO workload.	Additional training required for this new system.
15	Total loss of function through technical failure	Silent: existing hazard	No change	Increase	Sender needs reply therefore will seek via telephone. Revert to standard co-ordination and separation procedures. Reduced capacity, system redundancy. System failure alerts / confirmation.	Technical failure	Increase in ATCO workload, reduction in traffic data exchange with other controllers, fewer aircraft handled leading to delays to aircraft.	Technical failure would result in a breakdown in e-FUA. Fall back into b-FUA, therefore telephone still required.
16	Detected corruption through technical failure.	Silent: existing hazard?	Not yet known	No change	Partial data apparent to one or both ATCO's. Confirmation required therefore unlikely to go unnoticed. ATCO's revert back to telephone communication.	Technical failure	*If detected: Increase in ATCO's workload due to necessary co-ordination via telephone*	*Telephone lines still required*

Row	Hazard	Exists in b-FUA or new	If hazard exists, frequency vs. b-FUA	If hazard exists, Consequence vs. b-FUA	Mitigation measures – existing and proposed	Possible Causes	Consequences	Additional comments
17	Undetected corruption through technical failure.	Silent: existing hazard?	Not yet known	No change	Technical design assurance.	Technical failure; sabotage.	If displays nonsense then no problem. If displays viable data then problematic.	
18	Controller fails to notice silent data	Silent: no hazard in e-FUA	No change	No change	Telephone alert from other ATCO.	Human error	No coordination has taken place. Delay – possible increase in ATCO workload.	
19	Controller fails respond (action) to silent data	Silent: no hazard in e-FUA	No change	No change	Telephone alert from other ATCO.	Human error	ATCO gives neither an acceptance nor a rejection. No coordination has taken place. Delay – possible increase in ATCO workload.	
20	Data delayed – late delivery through technical failure or other cause	Silent: existing hazard.	No change	No change	Telephone alert from other ATCO. Technical design. Alternative procedures according to SOP's / contingency procedures.	Technical failure	No coordination takes place. Delay – possible increase in ATCO workload.	

Row	Hazard	Exists in b-FUA or new	If hazard exists, frequency vs. b-FUA	If hazard exists, Consequence vs. b-FUA	Mitigation measures – existing and proposed	Possible Causes	Consequences	Additional comments
21	Controller responds to data with incorrect clearance	Silent: existing hazard	No change	No change	Confirmation / feedback requirement for HMI.	Human error – selects "no" instead of "yes".	Possible loss of separation.	Written data on screen acts as a reminder for ATCO. Allows checking?
22	Loss of both silent and passive communication - undetected	Passive and silent			Telephones act as back-up.	*Technical?*	Increase in workload, *loss of separation*	Highly unlikely that would go undetected.
23	Notification failure / absence	Silent:						Same as failure to respond.
OI-1B Change 3 – Harmonised System Support Tool								
24	Incorrect data conveyed	Harmonised data tool: new system therefore new hazards associated with it. • Existing hazards	Unknown • Unknown – aim to reduce	Unknown • No change	Self-checking within centralised database. Originator will verify if output is correct.	Technical failure	All parties would get same incorrect information – reduced opportunity to cross-check.	Incorrect data can be conveyed at the present time but via a different medium (fax and phone)/ format (displays).
25	Incorrect data entered	Harmonised data tool: new system therefore new hazards associated with it.	No change? Unknown?	Unknown – possible wider implications.	Originator will verify if data inputted is correct.	Human error	All parties would get same incorrect information – reduced opportunity to cross-check.	Level of authorisation required for input needs to be carefully defined.

Row	Hazard	Exists in b-FUA or new	If hazard exists, frequency vs. b-FUA	If hazard exists, Consequence vs. b-FUA	Mitigation measures – existing and proposed	Possible Causes	Consequences	Additional comments
26	Technical failure of harmonised data tool	Harmonised data tool: New hazard	Unknown	No change	Technical design issue. Revert to basics, SOP's, contingency procedures.	Technical failure	*Increases ATCO's workload*	*Telephone required*
27	Unfamiliarity with aircraft / controller's equipment	Harmonised data tool: Not relevant.	N/A					As row 3 and row 14.
28	Data corruption – partial	Harmonised data tool						Similar to incorrect data conveyed (row 24).
29	Data corruption – total	Harmonised data tool						Similar to incorrect data conveyed (row 24).
FUA Hazards (possibly subject to modification by OI-1B) and General ATM Hazards from Brainstorm								
30	Failure of radar data processing system	If revealed failure then existing hazard	No change	No change	Emergency procedure: MIL exercise has to be stopped almost immediately.	*Technical*	*Loss of separation, highly increased workload, back to basics, delay*	This might need to be flagged up to ensure that the current emergency procedures are adequate to cope with this failure under e-FUA.
31	Late communication							See OI-1B Changes 1 and 2 above.

Row	Hazard	Exists in b-FUA or new	If hazard exists, frequency vs. b-FUA	If hazard exists, Consequence vs. b-FUA	Mitigation measures – existing and proposed	Possible Causes	Consequences	Additional comments
32	Radar (display) failure	Existing hazard	No change	No change	Emergency procedure: MIL exercise has to be stopped.	*Technical*	*Loss of separation, highly increased workload, back to basics, delay*	*Not different from everyday business*
33	Facsimile failure	Existing hazard	No change	Possible increase – depending on workload				Need to request a receipt confirmation if sending via electronic media
34	Email failure	Existing hazard	No change	Possible increase – depending on workload				Need to request a receipt confirmation if sending via electronic media
35	Failure of verbal communication (tech. failure), telephone, RT,VHF,UHF	Existing hazard	Un changed	Unchanged		*Technical*	*Increase in workload (ATCO, assistant)*	*Not different from everyday business*
36	Verbal miscommunication (human), e.g. • c-ATCO and m-ATCO • etc	Existing hazard	Reduced frequency of verbal communication – replaced by passive and silent data exchange	Unchanged		*Human Error*	*Loss of separation (not different from everyday business)*	Analysis of verbal communication errors may need detailed consideration of all actors concerned at Level 3 (c-ATCO, m-ATCO, ATCO assistant, ATCO supervisor, etc).

Row	Hazard	Exists in b-FUA or new	If hazard exists, frequency vs. b-FUA	If hazard exists, Consequence vs. b-FUA	Mitigation measures – existing and proposed	Possible Causes	Consequences	Additional comments
37	No verbal communication – no clear understanding of communication requirements • c-ATCO and m-ATCO	• Covered by OI-1B Other pairs similar to b-FUA				*as above*	*as above*	Analysis of communication errors may need detailed consideration of all actors concerned at Level 3 (c-ATCO, m-ATCO, ATCO assistant, ATCO supervisor, etc).
38	Airborne emergencies	Existing hazard						
39	Ground to aircraft (FMS) datalink failure	Existing hazard – unchanged						
40	Flight data processing system failure	Existing hazard – unchanged						
41	Ground to ground datalink failure						For future consideration when datalink implemented fully.	
42	Silent coordination failure - intention not communicated	See Change 2 Existing hazard	No change	No change		Human error		

Row	Hazard	Exists in b-FUA or new	If hazard exists, frequency vs. b-FUA	If hazard exists, Consequence vs. b-FUA	Mitigation measures – existing and proposed	Possible Causes	Consequences	Additional comments
43	Traffic situation information incorrectly displayed between c-ATCO and m-ATCO	See Change 3 and data delayed for Changes 1 and 2.						
44	Correct clearance given but aircraft fails to respond accordingly	Existing hazard.	*No change*	*No change*		*Human error*	*Loss of separation, increase in workload (ATCO/pilot)*	Pilot/ captain error
45	Failure to apply common rules / non standardized procedures – approved agencies (authorities / approved agencies)	Existing hazard	No change, or reduced by improved procedures	No change				Frequency of procedural errors may be reduced by OI-2B
46	Failure to apply common rules / non standardized procedures – AMC	Existing hazard	No change, or reduced by improved procedures	No change				Frequency of procedural errors may be reduced by OI-2B
47	Failure to apply common rules / non standardized procedures - controller level	Existing hazard	No change, or reduced by improved procedures	No change				Frequency of procedural errors may be reduced by OI-2B

Row	Hazard	Exists in b-FUA or new	If hazard exists, frequency vs. b-FUA	If hazard exists, Consequence vs. b-FUA	Mitigation measures – existing and proposed	Possible Causes	Consequences	Additional comments
48	Failure to apply common rules / non standardized procedures – CADF	Existing hazard	No change, or reduced by improved procedures	No change				Frequency of procedural errors may be reduced by OI-2B
49	Ambiguity in common rules / standardized procedures	Existing hazard	No change, or reduced by improved procedures	No change				Frequency of procedural errors may be reduced by OI-2B
50	Incompleteness of common rules / standardized procedures	Existing hazard	No change, or reduced by improved procedures	No change				Frequency of procedural errors may be reduced by OI-2B
51	Absence of common rules / standardized procedures	Existing hazard	No change, or reduced by improved procedures	No change				Frequency of procedural errors may be reduced by OI-2B
52	Disparate displays – absence of information	Existing hazard	No change, or reduced by improved procedures	No change				
53	Disparate displays – different screens • Flight data • Airspace status	Existing hazard	No change, or reduced by improved procedures	No change				

Row	Hazard	Exists in b-FUA or new	If hazard exists, frequency vs. b-FUA	If hazard exists, Consequence vs. b-FUA	Mitigation measures – existing and proposed	Possible Causes	Consequences	Additional comments
54	Incorrect aeronautical information promulgation	Existing hazard	No change, or reduced by improved procedures	No change				
55	Missing / incorrect coordination – • c-ATCO and m-ATCO • Plus other co-ordination groups	Existing hazard	No change, or reduced by improved technology or procedures	No change				Analysis of co-ordination errors may need detailed consideration of all actors concerned at Level 3 (c-ATCO, m-ATCO, ATCO assistant, ATCO supervisor, AMC, CADF etc).
56	System inter-operability problems	New Hazard	Unknown	Unknown	Technical design, certification and testing issue			
57	Complicated /excessive coordination process leading to workload increase	Existing hazard						Risks could be increased if e-FUA (procedures or equipment) badly designed

Row	Hazard	Exists in b-FUA or new	If hazard exists, frequency vs. b-FUA	If hazard exists, Consequence vs. b-FUA	Mitigation measures – existing and proposed	Possible Causes	Consequences	Additional comments
58	Incorrect data entry • c-ATCO and m-ATCO • Other pairs of actors	• Covered under OI-1B • Existing hazard unchanged by e-FUA						
59	Corrupt data -	Covered under Changes 1-3 above						
60	Mis-interpretation of data • c-ATCO • m-ATCO • supervisor • assistant	Covered under Changes 1-3 above						
61	Direct written communication • script	Existing hazard						Covered under communication errors above
62	Systems supported failure							Covered under technical failures above
63	Incomplete / inappropriate distribution of airspace status information • AMC, CADF or CFMU							Covered under communication/ co-ordination errors above

Row	**Hazard**	**Exists in b-FUA or new**	**If hazard exists, frequency vs. b-FUA**	**If hazard exists, Consequence vs. b-FUA**	**Mitigation measures – existing and proposed**	**Possible Causes**	**Consequences**	**Additional comments**
Consequences of an Incorrect Clearance and Mitigation Measures								
64	Incorrect clearance given – e.g. FL, Heading, Timing or Speed.	*Existing hazard*	*No change*	*No change*	• STCA • MTCA • Surveillance and correction • System warning • Second controller / assistant / supervisor • Pilot systems • ACAS • OAT radar • Visual – see and avoid • If no conflicting traffic then no problem!	*Human Error*	• Inadvertent penetration of active TRA. • Loss of separation, airprox, mid air collision.	

Table II.5 Mapping Hazard Log Outputs to Fault Tree Structure

Fault Tree Branch	Rows from Table II.4
Traffic Picture Error:	
Data entry/ read error	1,2,3,7,8,9,10,31,58,60
Passive Mode technical failure	4,5,6,22,43,59,62
Civil/ Military Crossing Error:	
Data entry/ read error	12,13,14,21,31,42,55,58,60
Silent Mode technical failure	15,16,17,22,59,62
Spoken/listening/remembering error	36,37
Telephone technical failure	35
Airspace Status Error:	
Data entry/ read error	25,27,31,60
ADR technical failure	24,26,28,29,59,62
Written status advice error	33,34,61
Spoken/listening/remembering error	36,37
Telephone technical failure	35
Not advised/ not advised to all	63
Modelled in ETA	64
Not modelled in FTA/ ETA because:	
No change from b-FUA to e-FUA	11,30,32,38,39,40,41,44,52,53,54
Not leading to a hazard	18,19,20,23
Related to OI-2B	45-51
Treated outside FTA/ETA	56,57

APPENDIX III

TRACEr Error Recovery Probability Analysis

Contents

III. TRACER ERROR RECOVERY PROBABILITY ANALYSIS

III.1 Introduction

Operational Improvement 1B (OI-1B) of the Enhanced Flexible Use of Airspace (e-FUA) process proposes a number of changes compared to basic FUA (b-FUA) as described in Section 2 of this report.

The safety assessment activities described in this report, and its appendices, have highlighted that a key change of OI-1B is the proposed replacement of verbal communication with electronic communication (defined here to include keyboard entry and menu driven data selection using a selection device such as a mouse or tracker ball) for the majority of civil-military co-ordination requirements. (Note, it is not possible to estimate the proportion of keyed data entry compared to mouse-driven data entry under e-FUA since this will vary according to each controller's personal preference. Both entry modes are likely to be available for inputting the same data. Therefore, it is not possible to make a quantitative comparison of human errors under basic and enhanced FUA at this time.)

A survey of the human error literature and consultation with ATM human factors experts indicated that the rates of human errors for verbal communication and keyed electronic communication are likely to be comparable. Some FUA experts have expressed the opinion that this is inconsistent with their experience and not strongly supported by evidence. At this time, no error rate data is available for selection errors (e.g. using a mouse) using the electronic data strip interface. However, this data could be obtained from either NERC or EUROCONTROL simulations. The ATM human factors experts who have taken part in past simulation trials reported that the error rate for mouse selection depends heavily on the menu/ interface design. Since this is not yet defined, the rates cannot be predicted.

DNV attempted to reconcile these apparently contradictory positions by performing a human error recovery probability analysis using part of the TRACEr[1] technique, see Section III.2 below. (Note that the error recovery probabilities determined by the TRACEr Recovery Success Likelihood assessment are relative qualitative judgements, not numerical values. Some readers may prefer the words "likelihood" or "proportion" rather than "probability" used here.)

This assessment was performed to determine whether there was any difference in the probability of the errors being recovered under e-FUA compared with b-FUA irrespective of which electronic communication mode (keyed or selected) was used. In the majority of cases, human errors are detected and recovered before any harm or inconvenience is caused. Given that the current data indicates that the error rates are similar for electronic and verbal communication, and that with a good interface design selection error should be at least as good as keyed entry (if not better), the human error differences between b-FUA modes and e-FUA modes lie in the detection, diagnosis and recovery stages rather than the frequency of the error itself. Therefore, this assessment aimed to contrast error recovery success probabilities rather than the initial error frequencies.

[1] TRACEr – Technique for Retrospective Analysis of Errors (Shorrock et al., 1998)

The logic of this approach may also be explained as follows:

Verbal error rate under b-FUA	F_B	Electronic communication error rate under e-FUA	F_E
Verbal error recovery probability under b-FUA	P_B	Electronic communication error recovery rate under e-FUA	P_E
Overall communication error rate under b-FUA	F_B x (1-P_B)	Overall electronic communication error rate under e-FUA	F_E x (1-P_E)

Thus if F_B and F_E are comparable, as the literature and the ATM human factors experts suggest, but if P_E is much larger than P_B then the overall communication error rate under e-FUA will be lower as predicted by the FUA experts. The analysis reported in this appendix was designed to assess the qualitative relative magnitude of P_B and P_E.

III.2 Description of TRACEr Error Recovery Success Probability Assessment

A human error recovery assessment was performed on both b-FUA communications and e-FUA communications based on the FHA/ PSSA information (see Sections 4-7 of this report and Appendices I and II) using human error analysis guidewords.

The analysis was performed as follows:

- Communication models (who communicates with who by what means) for b-FUA and e-FUA were defined, see Section III.3.
- Human errors were defined, incorporating the outputs of the FHA (Appendix II) and using human error guidewords, and evaluated with reference to a limited number of representative traffic scenarios, see Section III.5.
- For each human error in turn, an expert judgement assessment of the likelihood of detecting the error, of diagnosing the error and of correcting the error was made using the TRACEr Recovery Success Likelihood matrix (Table III.1) which is based on human factors principles for error recovery. A Recovery Success Likelihood (RSL) of high, moderate-high, moderate, low-moderate or low was assigned to each stage of the error recovery process (detection, diagnosis, correction).
- The overall error RSL for each human error is the lowest assessed RSL.

The overall assessment of the error recovery probabilities (P_B and P_E) was performed by a further stage of expert judgement as described in Section III.6.

Note that the above description is a component part of the total TRACEr technique.

Table III.1 TRACEr Recovery Success Likelihood Scale

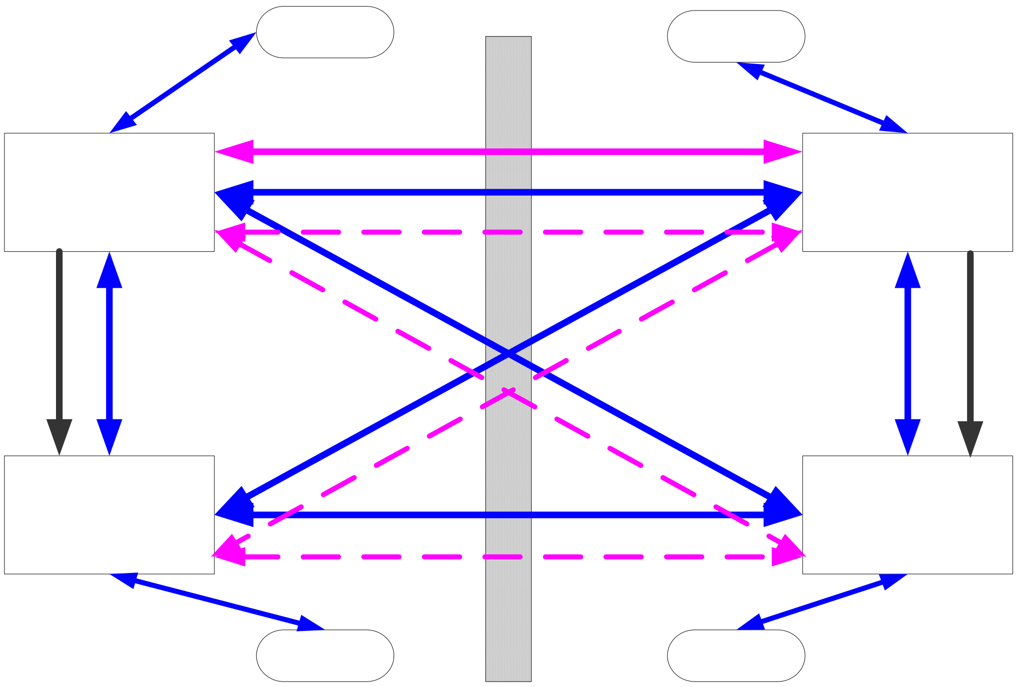
* Please rate the recovery success likelihood. Use the lowest appropriate RSL rating of Detection, Diagnosis, or Correction.

RSL	**Detection**	**Diagnosis/ Interpretation**	**Correction**
High (H)	> Easily detected > Immediate, clear, direct feedback of actions/effects > Active involvement and constant monitoring > Independent/third party checks, automatic checks or cues to check	> No diagnosis required or very reliable diagnosis expected > No ‘expectation bias’/’confirmation bias’	> Easily corrected, requiring no changes to plan, and causing little or no additional workload > Plenty of time available for recovery
Moderate-High (M-H)			
Moderate (M)	> Detectable > Feedback available > Regular but intermittent monitoring > Some cues to check or occasional independent checking by third party or automation	> May require some interpretation or diagnosis > Incorrect diagnosis possible > May be some ‘expectation bias’/’confirmation bias’	> May necessitate changes to plan or corrective action using practised procedure causing some additional workload > Controller prepared and able to intervene > Some time pressure to recover error
Low-Moderate (L-M)			
Low (L)	> Difficult to detect > No feedback, or poor, indirect or delayed feedback > No monitoring or passive monitoring > High reliance on memory to check or suspect error	> Hard to diagnose, diagnosis very likely to be incorrect > Strong ‘expectation bias’/’confirmation bias’	> Plan modification or difficult or complex correction process required, causing considerable workload > Controller unprepared or not familiar with procedures, with limited ability to intervene > Strong time pressure, or insufficient time available for recovery

III.3 Communication Models for FUA Civil-Military Co-ordination

The following functional models of military-civil communications were developed to guide the human error assessment. The models depict the modes of communication between controller both within sectors and across borders (sector or national).

Figure III.1 Communication Pathways Under Basic FUA



Key: ____ = Verbal communication route

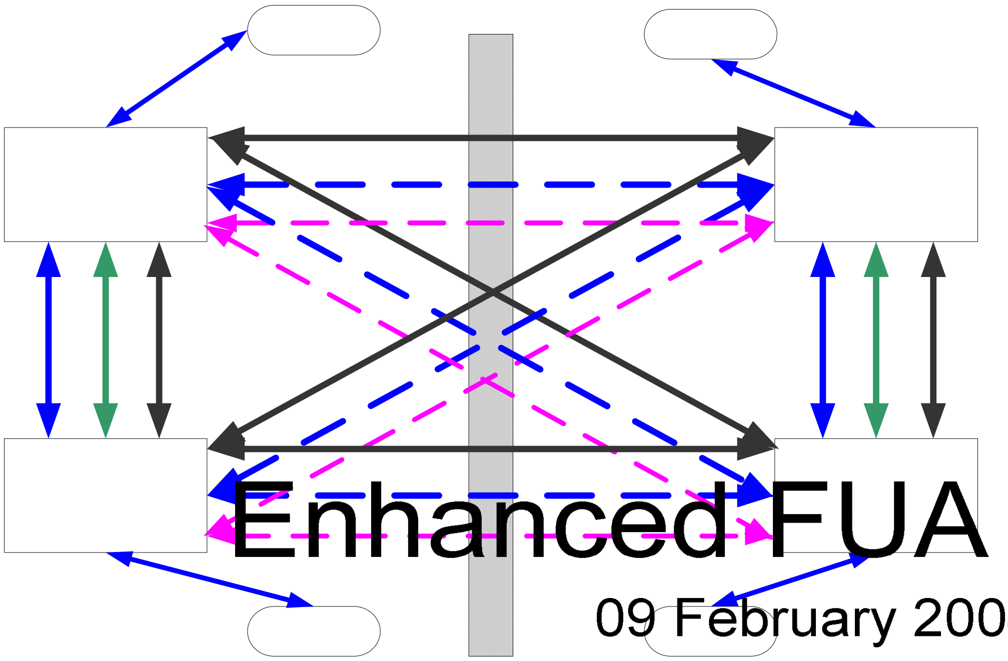
____ = Electronic data entry / written route

Basic FUA Comms

09 February 2004

RT

Figure III.2 Communication Pathways Under Enhanced FUA



Key: ____ = Verbal communication route

____ = Electronic data entry route

____ = Electronic data entry / written route

____ = Electronic data route, no entry required by controller

III.4 Assumptions

The following assumptions have been made regarding the functionality and operation of the systems used in FUA for civil-military co-ordination at Level 3:

- The normal silent mode transaction consists of the m-ATCO requesting a particular clearance from the c-ATCO. The c-ATCO responds to this message by accepting it, rejecting it, or providing a modified clearance. In each case, the system ensures that the message is routed to the correct m-ATCO (similar to “Reply” using email. Thus if the initial request is correctly routed, all subsequent communication is correctly routed.) If the clearance is rejected or accepted, no further communication results until a new clearance request is made. If the response is a modified clearance, the m-ATCO can now either accept, reject or provide a further modified clearance request.
- A visual display of silent mode communication transaction status (i.e. request sent, request rejected, request cleared and clearance executed) will be available as part of the controller interface.
- The silent mode includes contextual and supporting information, such as sector information, to assist the recognition of mis-routed clearance requests.

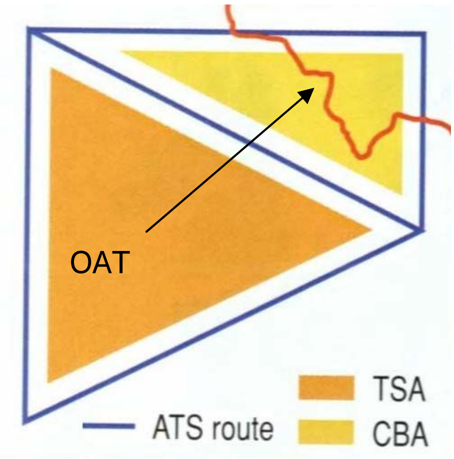
- A syntax check will be incorporated into both the silent and the passive systems to detect data entry errors.
- Silent mode requires data entry from both the military and the civil controllers. Standard phraseology will be used in the silent data exchange. Procedures shall be in place for who should be contacted during co-ordination.
- The new passive exchange of data from the military to the civil controller under e-FUA requires data input by the military controller.
- A telephone system is still in place to communicate between all controllers.
- If e-FUA operations revert to using telephone communication for any reason, this is assumed to be the same as b-FUA and does not influence the results of this analysis performed in this appendix.
- The c-ATCO is responsible for maintaining separation of GAT, whilst the m-ATCO is responsible for maintaining OAT-GAT and OAT-OAT separation.

See also Section 2 for other assumptions.

III.5 Human Error Recovery Probability Analysis

III.5.1 OAT Crossing

The OAT aircraft cross the GAT corridors between military segregated areas as shown below.



Under b-FUA: Civil and military controllers communicate via telephone. m-ATCO will receive additional GAT traffic situation via passive electronic data transfer. c-ATCO will not receive additional OAT traffic situation, though presence of OAT may be indicated on radar screens (perhaps without call sign, height, heading or speed information) through secondary radar depending on local State LoA or technology used. (Note that under b-FUA many aircraft, for example light aircraft flying at low level, may also show as returns on radar screens without additional data. This makes the c-ATCO's interpretation of the traffic situation more difficult under b-FUA.)

Under e-FUA: Civil and military controllers communicate mainly via silent mode but telephones will still be available as a back-up. m-ATCO will receive GAT traffic situation via passive electronic data transfer (similar to b-FUA). c-ATCO will now also receive additional OAT traffic situation via passive data transfer (new under e-FUA).

Scenario 1a: Communication from m-ATCO to c-ATCO within national boundaries relating to co-ordination of OAT aircraft crossing GAT corridors. The main human errors assessed are: mis-communicating the clearance request; mis-directing the clearance request; and not sending the clearance request when required.

Human Errors Under b-FUA for Scenario 1a

Human Error 1a.1: **m-ATCO mis-speaks the clearance request**. This should be detected immediately by the c-ATCO readback. However, there is a certain level of expectation associated with readback and so it is not 100% effective. If the error is not detected immediately, as is most likely, then two possibilities arise:

- If the m-ATCO makes an implausible (incorrect) clearance request it will be either rejected or questioned. This will lead to immediate error recovery. This error recovery success likelihood has not been assessed further since it is assumed to be very high and therefore this would not be considered a critical error.
- If the m-ATCO makes a plausible (incorrect) clearance request it will be accepted. The m-ATCO will then clear the OAT consistent with the m-ATCO's mental picture. The c-ATCO may then detect the error when the OAT aircraft behaves in an unanticipated manner, but under b-FUA the c-ATCO may not have access to sufficient flight information to detect or recover the error. This error could be corrected by issuing a corrective clearance. There may be an increased time pressure associated with this corrective action and it would increase the c-ATCO workload.

b-FUA, human error 1a.1: Detection L-M; Diagnosis M; Correction M; Overall L-M.

Human Error 1a.2: **m-ATCO contacts incorrect c-ATCO.** This error would result either from a misunderstanding about which civilian controller to contact or a simple execution error (e.g. mis-dial). There would be immediate feedback from the c-ATCO who would confirm their identity and also realise that the communicated information does not relate to their operations. The error would result in a short time delay but can be easily recovered by contacting the correct c-ATCO.

b-FUA, human error 1a.2: Detection H; Diagnosis H; Correction H; Overall H.

Human Error 1a.3: **m-ATCO forgets to contact c-ATCO (omission).** In high workload situations, the m-ATCO may intend to contact the c-ATCO but then get distracted by other factors. Therefore the clearance request will not be issued. If this is a fast moving aircraft (probable OAT), this may result in the c-ATCO contacting the m-ATCO to identify the OAT's intention (though under b-FUA the c-ATCO may not have sufficient information to detect or recover the error). A delay may result in an increase in workload for the c-ATCO and a clearance issued based on the current traffic situation. Since the controllers always react to the current traffic picture, this should not cause any changes to existing plans; instead a new plan will be formed based on the new information.

b-FUA, human error 1a.3: Detection L-M; Diagnosis M; Correction L-M; Overall L-M.

Human Errors Under e-FUA for Scenario 1a

***Possible Human Error 1a.4:* m-ATCO mis-enter clearance request data in silent mode.** This could be performed via direct numeric input or via selection from a drop-down menu. The m-ATCO will probably detect their own error immediately and correct it. However, if this is not the case, the next opportunity for detection is when the c-ATCO receives the clearance request via the silent mode. Two possibilities arise:

- If the m-ATCO clearance request is implausible, the c-ATCO will either issue an altered clearance or may telephone the m-ATCO to query the request or may simply reject it. This will lead to immediate error recovery. This error recovery success likelihood has not been assessed further since it is assumed to be very high and therefore this would not be considered a critical error.
- If the m-ATCO clearance request is plausible the c-ATCO is likely to agree it. The m-ATCO will then instruct the OAT consistent with the m-ATCO's mental picture, rather than the actual clearance request. The OAT will then exhibit unanticipated behaviour to the c-ATCO, which will be clear due to passive data exchange. This is likely to result in the c-ATCO telephoning the m-ATCO and the error will be corrected, with a probable increase in c-ATCO's workload. Also the m-ATCO will have a visual display of the actual clearance and may detect his own error.

e-FUA, human error 1a.4: Detection M; Diagnosis M; Correction M; Overall M.

***Human Error 1a.5:* m-ATCO contacts wrong c-ATCO (mis-select).** The m-ATCO might contact the wrong c-ATCO via the silent mode due to e.g. incorrect recipient entry. The c-ATCO would normally realise that this request does not relate to his airspace. If there is no OAT information on screen, this will be immediately obvious as the information would refer to crossing location, speed, heading and direction. This error could be corrected by contacting the correct civil controller although there may be an increase in workload involved.

e-FUA, human error 1a.6: Detection M-H; Diagnosis M-H; Correction M-H; Overall M-H.

***Human Error 1a.6:* m-ATCO forgets to issue clearance request (omission).** The m-ATCO may forget to send the clearance request as intended. This may be detected by the m-ATCO when he receives no reply as expected. Alternatively, the c-ATCO will have OAT information on his screen, via passive data exchange, and could call the m-ATCO to get OAT intention data. The silent mode should provide some visual feedback that a request has been sent so this would support the m-ATCO in detecting such an error. The error could be recovered by sending the clearance request as intended.

e-FUA, human error 1a.7: Detection M-H; Diagnosis M-H; Correction M; Overall M.

Scenario 1b: Communications from c-ATCO to m-ATCO as a response to previous m-ATCO (Scenario 1a) contact by accepting, modifying or rejecting a clearance request. The main human errors assessed are: mis-understanding the clearance request; mis-communicating the clearance response; and not sending the clearance response when required.

<u>Human Errors Under b-FUA for Scenario 1b</u>

Human Error 1b.1: **c-ATCO mis-hears the clearance request**. This should be detected immediately by readback. However, there is a certain level of expectation associated with readback and so it is not 100% effective. If the error is not detected immediately, as is most likely, then two possibilities arise:

- If the c-ATCO hears an implausible (incorrect) clearance request it will be either rejected or questioned. This will lead to immediate error recovery. This error recovery success likelihood has not been assessed further since it is assumed to be very high and therefore this would not be considered a critical error.
- If the c-ATCO hears a plausible (incorrect) clearance request it will be accepted. The m-ATCO will then clear the OAT consistent with the m-ATCO's mental picture. The c-ATCO may then detect the error when the OAT aircraft behaves in an unanticipated manner, but under b-FUA the c-ATCO may not have access to sufficient flight information to detect or recover the error. This error could be corrected by issuing a corrective clearance. There may be an increased time pressure associated with this corrective action and it would increase the c-ATCO workload.

b-FUA, human error 1a.1: Detection L-M; Diagnosis M; Correction M; Overall L-M.

Human Error 1b.2: **c-ATCO mis-speaks or m-ATCO mishears the clearance response**. This should be detected by the m-ATCO readback. However, there is a certain level of expectation associated with readback and so it is not 100% effective. If the error is not detected immediately by readback, then two possibilities arise:

- If the clearance response is implausible, then the m-ATCO will question it. This will lead to immediate error recovery. The error recovery success likelihood has not been assessed further since it is assumed to be very high and therefore this would not be considered a critical error.
- If the clearance response is plausible, the m-ATCO will accept it and clear the OAT accordingly. The c-ATCO may then detect unexpected OAT behaviour, though under b-FUA the c-ATCO may not have sufficient OAT flight data information to provide an effective safety net. This is likely to result in the c-ATCO telephoning the m-ATCO and the error will be corrected, with a probable increase in c-ATCO's workload.

b-FUA, human error 1b.1: Detection L-M; Diagnosis M; Correction M; Overall L-M.

Human Error 1b.3: **c-ATCO does not answer the telephone call from the m-ATCO**. The c-ATCO may be too busy to answer the telephone call from the m-ATCO. The m-ATCO will be aware that co-ordination has not been performed and is responsible for maintaining correct GAT-OAT separation. This error is corrected by making further attempts to contact the c-ATCO or by finding a crossing option that has sufficient separation such that co-ordination is not required.

b-FUA, human error 1b.2: Detection H; Diagnosis H; Correction M; Overall M.

Two additional errors could result under b-FUA if the c-ATCO is too busy to respond immediately to the m-ATCO's clearance request telephone call:

- The c-ATCO could contact the wrong m-ATCO, for example by mis-dialling, when attempting to return the call.
- The c-ATCO may forget to contact the m-ATCO.

In both cases, detection and recovery are high.

In each case the m-ATCO knows that co-ordination has not been performed and is responsible for maintaining GAT-OAT separation. These error modes are not further assessed.

Human Errors Under e-FUA for Scenario 1b

Human Error 1b.4: **c-ATCO mis-reads silent mode request / data.** The m-ATCO could issue a correct request via the silent mode but the c-ATCO may mis-read the request. This is unlikely as the clearance request can be re-read as a reference. How effective this memory-aide will be will depend on the nature of the display. If the c-ATCO does not detect his/ her own error, then two possibilities arise:

- If the mis-read clearance request is implausible the c-ATCO will either re-read the request, reject the request, issue an alternative clearance or telephone the m-ATCO. This will lead to immediate error recovery. The error recovery success likelihood has not been assessed further since it is assumed to be very high and therefore this would not be considered a critical error.
- If the mis-read clearance request is plausible the c-ATCO is likely to accept it. In this case The m-ATCO will then instruct the OAT consistent with the m-ATCO's (correct) initial request and the OAT will then exhibit unanticipated behaviour to the c-ATCO. This is likely to result in the c-ATCO rechecking the clearance request or telephoning the m-ATCO and the error will be corrected, with a probable increase in c-ATCO's workload

e-FUA, human error 1a.5: Detection M-H; Diagnosis M-H; Correction M; Overall M.

Human Error 1b.5 **– c-ATCO mis-enters alternative clearance response information**. If the original clearance is not acceptable, the c-ATCO can issue an alternative clearance response via the electronic data strips or the aircraft's data block on screen; therefore this could be performed via direct numeric input or via selection from a drop-down menu. The c-ATCO may detect their own error immediately and correct it. However, if this is not the case, two possibilities arise:

- If the altered clearance response is implausible, the m-ATCO will probably telephone the c-ATCO to question it. The error recovery success likelihood has not been assessed further since it is assumed to be very high and therefore this would not be considered a critical error.
- If the altered clearance is plausible, the m-ATCO will probably clear the OAT accordingly. The c-ATCO would then be alerted to their error by unanticipated OAT behaviour. This could be recovered by issuing a corrective clearance.

e-FUA, human error 1b.3: Detection M-H; Diagnosis M-H; Correction M; Overall M.

Human Error 1b.6 **– c-ATCO forgets to respond to clearance request (omission).** In high workload situations, the c-ATCO may intend to respond to the m-ATCO but then get distracted by other factors. Therefore the clearance will not be given. This should be prevented by highlighting new requests on the controller's display. Also, the c-ATCO will see the OAT aircraft approaching his airspace and search for a clearance request. If the c-ATCO does not respond, this is likely to result in the m-ATCO contacting the c-ATCO again and repeating his request. A delay may result in an increase in workload for the c-ATCO and a different clearance (than originally intended) may be issued given the current traffic situation. Since the controllers always react to the current traffic picture, this should not cause a problem.

e-FUA, human error 1b.4: Detection M-H; Diagnosis M-H; Correction M; Overall M.

III.5.2 Other Scenarios

It has been assumed that under most circumstances OAT cross GAT corridors and that generally GAT are not cleared to cross OAT airspace (if GAT cross airspace where OAT may be operational, this will often be done on an open conditional GAT route, in which case OAT will need to cross this route using co-ordination as described in Section III.5.1). However if c-ATCO do need to request co-ordination with m-ATCO, the analysis will be broadly similar to that described in Section III.5.1, except that the m-ATCO will now provide the safety net if the GAT behaves in an unexpected way.

A similar error recovery probability assessment could also be presented to support Change 3 of OI-1B. However the replacement of the multiple bilateral communication network by the Airspace Data Repository, as described in Section 2, is a more complex change than the direct replacement of verbal communication with electronic communication. Without even estimated data on the frequency of the initial errors, it is hard to form a judgement of the human error recovery probability results that would result from a TRACEr assessment. Hence such an assessment is not presented here.

III.6 Discussion

Table III.2 summarises the results presented in Section III.5.

Table III.2 Summary of TRACEr Results
Shaded cells indicate the higher error recovery probability (lower risk)

b-FUA Human Error		**e-FUA Human Error**	
1a.1 m-ATCO mis-speak	L-M	1a.4 m-ATCO mis-enters data	M
1a.2 m-ATCO contacts wrong c-ATCO	H	1a.5 m-ATCO contacts wrong c-ATCO	M-H
1a.3 m-ATCO forgets to contact c-ATCO	L-M	1a.6 m-ATCO forgets to contact c-ATCO	M
1b.1 c-ATCO mis-hears clearance request	L-M	1b.4 c-ATCO mis-reads clearance request	M
1b.2 c-ATCO mis-speaks clearance response or m-ATCO mis-hears	L-M	1b.5 c-ATCO mis-enters clearance response or m-ATCO mis-reads response	M
1b.3 c-ATCO does not answer telephone from m-ATCO	M	1b.6 c-ATCO does not respond to m-ATCO silent mode request	M

The evaluation of the relative magnitude of the overall error recovery probabilities (P_B and P_E) discussed in Section III.1 depends in part on the pair wise comparisons in each row of

Table III.2 and in part on an expert judgement of the relative frequency of each type of human error (each row).

Examination of Table III.2 shows that the error recovery probabilities under e-FUA are at least as large as under b-FUA for 5 of the 6 representative human errors evaluated. Thus this analysis shows that e-FUA will be as safe or safer than b-FUA under most probable circumstances. This statement could be false for one of the following reasons:

- If the assumptions stated in Section III.4 are false;
- If one or more major human error mode has been omitted from the analysis and this human error mode is less safe under e-FUA;
- If the frequency of contacting the wrong ATCO is very high in comparison with the other human errors evaluated.

At this stage of the assessment it appears, on balance, that e-FUA should be at least as safe as b-FUA.

III.7 Conclusions

The following conclusions have been drawn from the above analysis:

- Verbal workload should be reduced under e-FUA therefore verbal errors should also reduce.
- Data entry workload will increase under e-FUA and therefore data entry errors are likely to increase.
- There is no human factors evidence identified that shows that data entry errors in ATM have a lower probability than data entry errors elsewhere.
- Specific interface design recommendations could increase the likelihood of error recovery under passive and silent modes, although further research would have to confirm this through user trials.
- Any increase in air traffic density is likely to reduce any benefits gained by these three changes under e-FUA. That is, if controller workload increases then error probabilities will in turn increase once more.

On balance, this analysis indicates that e-FUA is at least as safe as b-FUA. However, as indicated above, this analysis is not exhaustive, it is not a direct analysis of the details of specific system implementation, and it is not based on a persuasive body of research literature. The conclusion of this analysis, therefore, should be considered to be indicative rather than definitive.

FUNCTIONAL HAZARD ASSESSMENT/ PRELIMINARY SYSTEM SAFETY ASSESSMENT REPORT ON ENHANCED REAL TIME CIVIL-MILITARY CO-ORDINATION (OI-1B)

REV 3, 05 OCTOBER 2004

For

EUROCONTROL

DET NORSKE VERITAS

DET NORSKE VERITAS LIMITED
DNV Consulting
Palace House
3 Cathedral Street
London SE1 9DE
United Kingdom

Tel : + 44 (0) 20 7 357 6080
Fax : + 44 (0) 20 7 716 6730
http:\\www.dnv.com

Registered in England
No.: 1503799

Functional Hazard Assessment/ Preliminary System Safety Assessment Report on Enhanced Real Time Civil-Military Co-ordination (OI-1B)

for

EUROCONTROL

Contract No.	20127100
Revision	3
October 2004	

Enhanced FUA Process: Functional Hazard Assessment/ Preliminary System Safety Assessment Report of Enhanced Real Time Civil-Military Co-ordination (OI-1B)

Issue Log

Revision	Issue Date	Prepared by	Reviewed by	Approved by	Comments
0	12 March 2004	Helen Jones Tim Fowler	Edward Smith	Edward Smith	
1	21 May 2004	Tim Fowler	Edward Smith	Edward Smith	
2	27 August 2004	Edward Smith	Tim Fowler	Edward Smith	
3	05 October 2004	Edward Smith	Tim Fowler	Edward Smith	Including final client comments

Contents

APPENDICES

1. INTRODUCTION

1.1 Background

Det Norske Veritas (DNV) has been engaged to assist EUROCONTROL with safety assessment activities associated with the introduction of the Enhanced Flexible Use of Airspace Concept. This report describes part of this work.

The Flexible Use of Airspace (FUA) Concept is intended to provide the maximum flexibility to all airspace users in a seamless fashion across all ECAC states. Basic FUA (b-FUA) was introduced in 1996. By the end of 1998 b-FUA was implemented in 13 ECAC states and is currently implemented in almost all ECAC states.

EUROCONTROL's Airspace Strategy document (EUROCONTROL, 2001c) identifies a coherent set of actions, grouped into 7 Directions for Change (DfC), with the objective of contributing to a single European Sky sometime after 2015. Within the Airspace Strategy DfC B is entitled "Airspace Management & Civil/Military Co-ordination".

Within DfC B, the following 6 Operational Improvements (OI-1B to OI-6B) have been identified along with the stated target implementation timeframe:

OI-1B Enhance real-time civil/ military co-ordination.
OI-2B National collaborative/ integrated airspace planning, to be complete by Q3 2004.
OI-3B Extend FUA to lower airspace, to be complete by Q4 2005.
OI-4B Enhance FUA with dynamic airspace allocation and harmonise OAT/ GAT handling throughout Europe, to be complete by Q4 2006.
OI-5B Collaborative European airspace planning, to be complete by 2008.
OI-6B Integrated European airspace, to be complete by 2012.

These 6 operational improvements (OI-1B to OI-6B inclusive) are collectively called the Enhanced FUA Process (e-FUA).

Within FUA, airspace use is planned with reference to 3 organisational levels:

- Level 1 concerns strategic planning months or years in advance of use;
- Level 2 concerns pre-tactical planning up to 1 day in advance of use; and
- Level 3 concerns tactical planning and co-ordination on the day of operations.

This project report describes the FHA/ PSSA of OI-1B only. This OI impacts only on Level 3. A more detailed description of the changes associated with OI-1B can be found in Section 2 below.

It should be noted that it was originally intended to perform a safety assessment of OI-1B and OI-2B in parallel. However part way through the assessment process it was decided to concentrate on OI-1B and to delay assessment of OI-2B. This explains some references to OI-2B which may be found in this report and its appendices.

1.2 Objectives

The objectives of this report are to:

- Present safety criteria that can be used to assess the safety performance of OI-1B within e-FUA, derived from and consistent with the Safety Policy for e-FUA;
- Document the process and outputs from the FHA/ PSSA meeting for OI-1B within the Enhanced FUA Process;
- Present bow-tie models of the changes that result from implementation of OI-1B to show the probable causal chains that link accidents to basic causes, as relevant to the Enhanced FUA Process;
- To identify potential risk mitigation measures that result from the hazard analysis and from understanding the bow-tie models;
- To present and discuss semi-quantitative arguments that result from the bow-tie models which indicate the relative safety levels of OI-1B compared with basic FUA;
- To derive safety objectives and requirements for OI-1B to meet the overall safety criteria.

1.3 Structure of this Report

This report is structured as follows:

- Section 2 contains a description of OI-1B and in particular, the key changes that arise from OI-1B compared with b-FUA;
- Section 3 presents the safety criteria that have been derived from the Safety Policy for e-FUA that should be applied to OI-1B;
- Section 4 summarises the FHA/ PSSA process that has been performed to assess OI-1B;
- Section 5 presents the e-FUA OI-1B functional model;
- Section 6 describes the event tree analysis conducted for the FHA;
- Section 7 contains the fault tree analysis carried out for the PSSA;
- Section 8 presents the assessment against the safety criteria and derives necessary safety requirements for OI-1B;
- Section 9 contains conclusions and recommendations;
- Section 10 describes how the safety assessment results documented in this report are fed into the Outline Safety Case for e-FUA OI-1B and into the subsequent National Safety Cases to be developed by each ECAC State implementing OI-1B; and
- Section 11 provides the reference list and defines acronyms and abbreviations used.

The briefing material circulated prior to the FHA/ PSSA meeting "dry run" and the full meeting is presented in Appendix I and the meeting note of the FHA/ PSSA experts meeting is contained in Appendix II. Appendix III contains a human factor analysis in support of the PSSA.

2. OPERATIONAL IMPROVEMENT 1B

2.1 Description of Operational Improvement 1B (OI-1B)

Comparison of the b-FUA and e-FUA criteria indicates the following key changes introduced/ required by OI-1B:

1. Automated exchange of **flight data,** using a **passive mode** of co-ordination, **from the military to the civil ATCO** with the **position of the OAT** flight **(e-FUA)**, in addition to the automated exchange of flight data from the civil to the military ATCO, including the position (BFD message[1]) and intention (CFD message[2]) of the GAT flight (b-FUA).
2. Direct controller to controller communications, using a **silent mode** of co-ordination based on system supported dialogues with the use of **airspace crossing function**[3] **(e-FUA)**, in addition to the use of verbal mode of communication with direct telephone line between the civil and military ATCO (b-FUA).
3. The provision of national (TSA/TRA, R/D) and/or international (CBA) airspace-use data to the control staff concerned with the use of a harmonised system supported tool (the same tools used by all parties fed with data from the common Airspace Data Repository) **(e-FUA)**, in addition to the use of phone/fax (b-FUA).

Thus

- **Change 1** entails the provision of **"passive" flight data** exchange protocols (BFD message) **from military controller to civil controller** within their respective areas of responsibility in accordance with LoAs established between the civil and military ATS units concerned.
- **Change 2** entails the provision of **"silent" flight data** exchange protocols (XIN, XRQ, XAP, ACP & REJ messages) in support to the **airspace crossing function between military controller and civil controllers** within their respective areas of responsibility in accordance with LoAs established between the civil and military ATS units concerned.
- **Change 3** entails the provision of **airspace-use data** exchange protocols, using a harmonised system support tool, between all the parties concerned initially within a country (*airspace status of national CDR, TSA/TRA, R/D*) [OI-1B] and later on across boundaries (*airspace status of international CDR, CBA*) [OI-5B1].

[1] The Basic Flight Plan Data (BFD) information concerns the automatic exchange between civil and military control units of all flight plan data that are necessary for the Identification Function.

[2] The Current Flight Plan Data (CFD) information allows the automatic and dynamic update of the flight plan data with executive data, including controller's intentions, that are necessary for the Separation Function.

[3] The Airspace Crossing Function is based on a system-supported dialogue to either only notify the civil controller of the plan of action of a military controller intending to cross an ATS route and vice versa (XIN message) or when a prior OAT/GAT co-ordination is required for airspace or route crossing, to speed-up and facilitate the dialogue between the civil and military controllers (XRQ, XAP, ACP & RJC messages).

2.2 Key Changes Resulting from Implementing OI-1B

The description of the changes that result from implementing OI-1B provided below is based on the detailed discussions of the changes that took place in the FHA/ PSSA experts' meeting on the Flexible Use of Airspace, as described in Section 4.

2.2.1 OI-1B Change 1 (Passive Mode)

Table 2.1 describes the degree of information about a flight that could be available to a controller.

Table 2.1 Levels of Information Availability to Controllers

	None	Surveillance	BFD	CFD
Level of Information	Flight position shown on screen if primary radar available, or no information	Secondary radar data (position, height)	- Aircraft Identification; - SSR Mode and Code; - other flight plan data, if necessary, for correlation with radar data (e.g. type of aircraft, departure/ destination aerodromes, route etc.)	All significant changes to BFD data, including controllers intentions entered by controller entering in data

These levels of information could be provided by one or more of the following communications channels:

- Primary radar;
- Secondary radar;
- Data encoded on secondary radar;
- Direct verbal communication (e.g. by telephone or radio);
- Silent exchange of data;
- Passive exchange of data;
- Data available from own systems without need for data exchange.

Under b-FUA, the information available to controllers is assumed as shown in Table 2.2.

Table 2.2 Source and Level of Information Available to Controllers in b-FUA

	GAT	OAT
c-Controller	BFD + CFD Data via own systems	BFD, or less that BFD Data via primary radar or secondary radar or via direct verbal communication
m-Controller	BFD + CFD Data via passive exchange of data from the civil to the military, including (at least partial) controller intention data (CFD)	BFD + CFD Data via own systems

The civil controller's picture of the traffic situation with respect to OAT may be incomplete. Where further information is required, this is obtained by telephone contact with the military controller, but such extra information would normally only be required to support the OAT/ GAT crossing which is covered under Change 2 below.

The military controller's picture of the traffic situation is more complete (via decoding GAT secondary radar) than the civil controller, but intention data for both controllers can only be obtained from telephone co-ordination, and this would only normally be required to support the OAT/ GAT crossing which is covered under Change 2 below.

Under e-FUA, the information available to controllers is intended to be as shown in Table 2.3.

Table 2.3 Source and Level of Information available to Controllers in e-FUA

	GAT	OAT
c-Controller	BFD + CFD Data via own systems	BFD + CFD Data via passive data exchange (Provision of m-controllers intention only if bilaterally agreed)
m-Controller	BFD + CFD Data via passive data exchange, including full controller intention data	BFD + CFD Data via own systems

Both controllers have full access to BFD + CFD via passive exchange of data (assuming this has been agreed bilaterally through letters of agreement), though the military controller is likely to only enter intention data for OAT when crossing is anticipated.

It should be noted that standard operating procedures may allow clearances to be issued to aircraft only on the basis of radar screen information derived from passive data exchange under e-FUA. For example, if GAT is sufficiently separated to allow OAT to cross without risk of reduced OAT-GAT separation, then co-ordination between civil and military controllers may not be required.

2.2.2 OI-1B Change 2 (Silent Mode)

Change 2 is distinguished from Change 1 in that a notification or a request is sent from one controller to another involving manual action from the controller. In case of a crossing request, an action can only result if that request is positively accepted by the receiving controller. Two examples of such requests are described:

- A military controller can request that the civil controller clears OAT to fly across a GAT airway (e.g. permanent route, conditional route etc).
- A civil controller can request that the military controller clears GAT to fly across an active TSA.

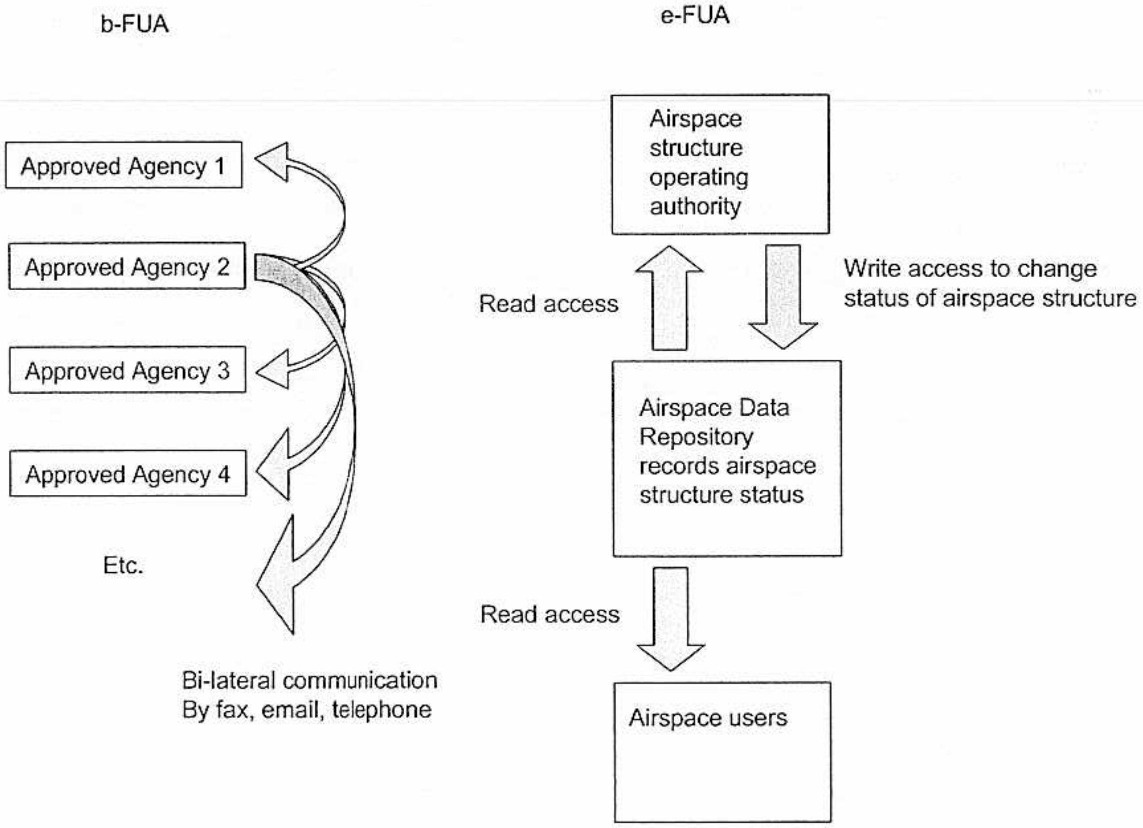
Under b-FUA this co-ordination would be done by verbal telephone conversation. e-FUA allows the request for clearance and its acceptance (as requested, or amended) to be done predominantly by electronic silent exchange.

2.2.3 OI-1B Change 3 (Airspace Data Repository)

Within FUA, approved agencies can apply for airspace allocation. This can result in the opening or shutting of different FUA temporary airspace structures. Military users may also cancel exercises, or finish them early, which can result in the release of temporary allocated airspace for other users.

Under b-FUA airspace status is communicated by fax, email or verbally (telephone) from the originator to all approved agencies. Under e-FUA, the airspace data repository is a central reference of the status of all airspace structures. All approved agencies can read information from this (read only access). Airspace structure "owners" (e.g. military users of a TSA) can also change the status of their airspace structures by updating data in the airspace data repository (write access). The difference is shown graphically in Figure 2.1.

Figure 2.1 Illustration of Effect of Change 3



3. SAFETY CRITERIA APPLIED TO ENHANCED FUA PROCESS (OI-1B)

The Enhanced FUA Process Safety Policy statements and safety objectives are detailed in the Safety Policy (EUROCONTROL, 2003a).

From these statements and objectives two criteria for this safety assessment of OI-1B can be derived:

1. Risks should be no higher than under b-FUA; and
2. Risks should be further reduced as far as reasonably practicable.

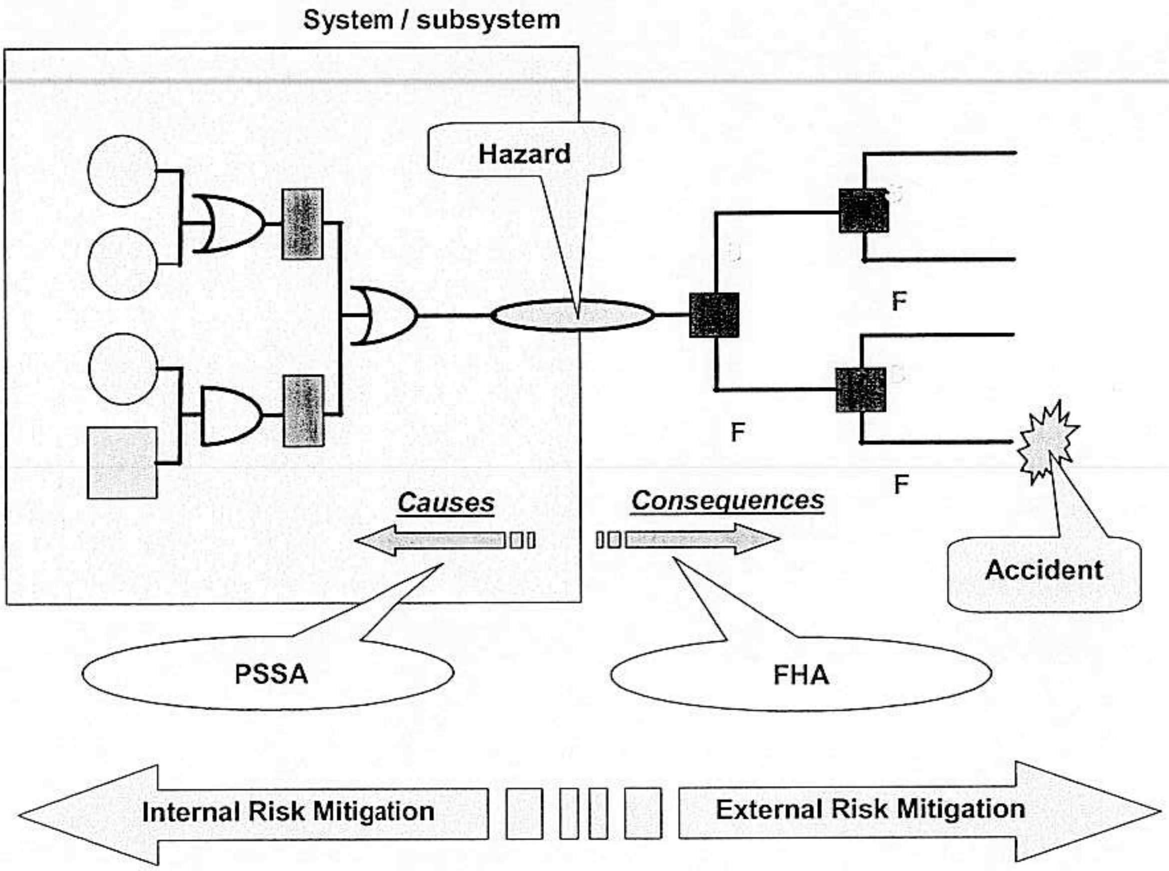
These criteria are consistent with the principles contained in ATM 2000+ and ESARR4 of reducing risk in the face of future increases in traffic and with the EATMP safety policy.

4. SUMMARY OF FHA/ PSSA PROCESS FOR OI-1B

4.1 Introduction to FHA/ PSSA

EUROCONTROL has summarised the inter-relationship between the FHA/ PSSA processes using Figure 4.1.

Figure 4.1 Inter-Relationship between FHA and PSSA



The first stage of the FHA/ PSSA process is to identify the key hazards by examination of a functional model (see Section 5) and through brainstorming. The identification of the key hazards for further analysis requires careful judgement. Many apparent hazards are often actually causes of a relatively small number of main hazards.

Figure 4.1 indicates that each identified main hazard is then analysed in terms of its possible consequences (FHA, for example by using an event tree) and possible causes (PSSA, for example by using a fault tree). One objective of this analysis is to identify the probable causal chains that link basic causes to accidents. In turn, this allows the systematic identification and evaluation of potential risk reduction measures which, if implemented, could further reduce risks.

4.2 FHA/ PSSA Meeting "Dry Run"

A key part of the FHA/ PSSA process is often an experts' meeting. This is used to obtain expert judgement from a group of ATM professionals with experience of different aspects of the process being evaluated (OI-1B of e-FUA in this case). The objectives and processes of the FHA/ PSSA experts' meeting is described more fully in Section 4.3 below.

In many projects it is very important that the experts' meeting is fully successful (it achieves its objectives) for some or all of the following reasons:

- Experts, and their employing organisations, often donate their time to the FHA/ PSSA experts' meeting free-of-charge. It is important to recognise their contribution by not wasting their time in a non-productive meeting.
- It can often be difficult to re-convene experts' meetings within the timescale of a safety assessment project.
- Some external experts may not be fully persuaded of the importance of safety assessment processes. If the FHA/ PSSA meeting fails to meet its objectives, their negative views may be reinforced.

For the above reasons, it is often helpful to plan the FHA/ PSSA meeting in detail so as to maximise the chance of its success. A full "dry run" of the FHA/ PSSA experts' meeting was performed for OI-1B, using EUROCONTROL's internal expertise as meeting attendees. The briefing material for the "dry run" meeting participants is included in Appendix I.

4.3 Main FHA/ PSSA Meeting

The following personnel attended the main FHA/ PSSA session for OI-1B of e-FUA (for both days unless otherwise stated).

Mr Tom Suffolk, EUROCONTROL AFN BD, served for 30 years in the RAF as a pilot, air traffic controller, instructor, supervisor, manager and staff officer. Mr Suffolk retired from the RAF as Wing Commander and joined EUROCONTROL in 1994 as an expert in ASM and civil/military coordination he has been directly involved in the development of the Concept for the Flexible Use of Airspace.

Mr Jean-Paul Lemaire, EUROCONTROL AFN BD, joined the French Air Force Academy as a flying officer in 1966. As navigator he has 3,000 hours flying experience including many as navigator-in-command. In 1977 he graduated as a Civil Aviation Engineer and joined DIRCAM. He has considerable experience in ASM and civil/military coordination. He retired after 27 years service with the FAF in the rank of Colonel and joined EUROCONTROL in 1993 to develop the Concept of Flexible Use of Airspace and, subsequently, the Eurocontrol Airspace Strategy.

Dr. Bernd Tiemeyer, EUROCONTROL – morning Day 1 only.

Major Per Coulet, EUROCONTROL (attended part time) has 28 years experience in the RDAF as an air traffic and air defence controller, fighter allocator and sector controller. He has also served as an instructor and supervisor. He has considerable experience as a staff officer at national and international level and the flight safety inspections of ATC and Air Defence units. He joined EUROCONTROL MIL BD in April 2003.

Lt. Col. Eric Chatelus, Dircam has 24 years service with the FAF as an air traffic control officer chief controller at airports and centres in France. From 1998-2002 he was chief of the ATC section in HQ FAF with responsibility for air traffic controllers. Since 2002 he has been the head of the ASM section at the French military air traffic services directorate responsible for the regulation of military air traffic for French MOD.

Wing Commander Mike Strong, EUROCONTROL MIL BD, has 37 years experience as an air traffic controller, supervisor, instructor, examiner, manager and staff officer. He has served at RAF airfields in the UK and abroad and at joint civil/military ACCs, and has broad experience in a variety of ATM management posts in military and civilian organisations. As a staff officer, he has held responsibility for RAF ATC equipment programmes, UK NATS business planning, safety management, and policy for all airspace activities in the UK outside controlled airspace.

Mr Zlatko Meic, EUROCONTROL, AFN BD is an ASM expert who joined EUROCONTROL from Croatia in 2001. He is a fully qualified ATCO and instructor with experience in the Zagreb ACC, Ljubljana (Slovenia) ACC/APP, Prague ATC Training Centre, as the ATC Operations Manager in Federal ATS Authority of former Yugoslavia and in MOT - CAA of Croatia responsible for international affairs, liaising with ICAO, EUROCONTROL, UN and NATO peace-keeping forces.

Benoit Fonck, CFMU/URB, EUROCONTROL. Served for 15 years in the Belgian Air Force as an air traffic controller, supervisor, manager, staff officer and Head of base ATS. He joined EUROCONTROL in September 2001 as an ASM expert working in the AMN unit on the ASM Handbook and the development of the EUROCONTROL Airspace Strategy Operational Improvements. He joined the CFMU in October 2002 and currently works mainly on the development of the ATFCM Strategy and Evolutions and the improvement of the ASM/ATFCM interface.

Mervyn Oliver, EUROCONTROL. Safety Instructor, has served for over 15 years as an Air Traffic Control Engineer for National Air Traffic Services and spent 2 years in the HQ safety Department. Mr Oliver joined EUROCONTROL in 2000 and is responsible for the System Safety Assessment Courses at the Institute of Air Navigation Services.

Mr Holger Ahrens, DFS is a German civil air traffic controller with considerable experience of flying, ATC and safety matters. He has 1100 hours experience as a German Army helicopter pilot. He was licensed as an ATCO at Bremen ACC from 1989. In 1999 he moved to management duties at Berlin ACC/UAC where he investigated incidents/losses of separation and participated in the safety assessment of the Berlin ACC move to Bremen. He is currently involved on safety assessments for new airspace concepts, new airways and ACC contingency planning.

Wing Commander Stu Wain, RAF has 19 years service with the RAF as a navigator. He has a wide experience of military fast jet flying and has a total of 2000 flying hours on Tornado, Hawk and Jet Provost aircraft in the UK and Germany. He has been a primary and advanced navigation instructor and has experience of staff appointments in the UK. He is currently the UK Delegation to NATO SO ASM.

Squadron Leader David Raine has 29 years experience as an air traffic controller, supervisor, instructor, airport manager and staff officer and has served at RAF airfields in the UK, Germany, Cyprus, the Middle East and the Falkland Islands. He has considerable experience at joint civil/military ACCs, and has broad experience in a variety of ATM staff and management posts in military and civilian organisations including responsibility for airspace changes and airspace policy matters.

Lt Col Mike Steinfurth, EUROCONTROL SD/MIL has 29 years experience as a pilot in the German Air Force flying in Germany and the USA. He has 2800 hours in fighter & reconnaissance aircraft and considerable experience in staff appointments including responsibility for Military Aviation Operations, Aviation Regulation and Operational Requirements and Capabilities. He has considerable experience in the management and command of operations, operational flying and training squadrons.

Dr Tim Fowler (Facilitator), Det Norske Veritas. Tim has worked for DNV for 12 years as a risk management consultant and has nearly 25 years post-graduation experience. He has participated in and managed numerous risk assessment projects and is an experienced hazard identification facilitator.

Ms Helen Jones (Recorder), Det Norske Veritas. Helen is an experienced human factors consultant who has worked for DNV for nearly 3 years. Previously she worked for the Royal Navy and has done project work with NATS on the use of electronic paper strips.

Briefing material was circulated to all the above meeting participants one week before the meeting. This briefing material is included in Appendix I.

The objectives of the FHA/ PSSA meeting were:

- To agree the final form of the system description and key assumptions on which the FHA and remaining e-FUA safety assessment activities will be based;
- To identify all hazards and hazard causes associated with b-FUA and the changes that result from implementing OI-1B;
- To assess the effect of the changes introduced by OI-1B on the existing b-FUA hazards and hazard causes and to assess the importance of any new hazards or causes introduced by e-FUA OI-1B;
- To analyse the interrelationship between hazards and their contributory causes; and
- To identify existing and potential risk mitigation measures that could be applied to reduce risks.

The process used by the meeting was a mixture of brainstorming and discussion to address the objectives above. The outputs from the main FHA/ PSSA meeting, plus subsequent comments received from meeting participants, are documented in Appendix II.

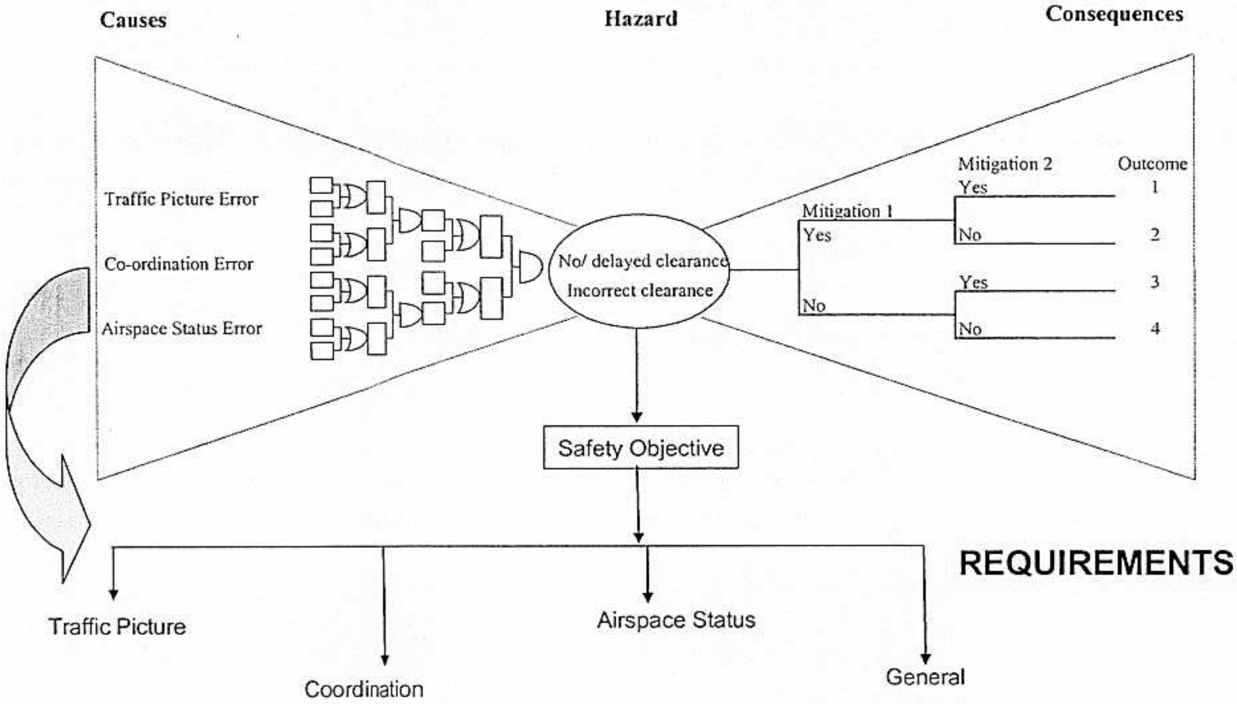
4.4 Post-Meeting Tasks

The FHA/ PSSA session was a highly effective means of gathering expert judgement on a variety of topics including: the operational environment relevant to OI-1B; the functions of OI-1B (what OI-1B entails in detail); the hazards associated with OI-1B; and other similar types of data. However a meeting of experts is less effective at more analytical or quantitative tasks such as refining the structure of functional models, event trees or fault trees. These activities were, therefore conducted after the main experts' meeting as described below.

4.5 Analysis Framework

Figure 4.2 summarises the activities following the brainstorming session. Event tree analysis was conducted and from this a safety objective was derived for the hazard of clearance error, to enable the overall safety criteria to be met. Fault tree analysis (FTA) was then used to determine if this safety objective would be met. The FTA enabled safety requirements to be identified necessary for the objective to be met. These stages are described in Sections 6, 7 and 8.

Figure 4.2 FHA/ PSSA Analysis Framework



5. FUNCTIONAL MODEL OF FUA HAZARDS

The functional model for OI-1B, revised to take account of the FHA/ PSSA meeting outputs and subsequent DAP/ SAF comments, is shown in Figure 5.1. While the changes associated with OI-1B concern ASM Level 3, inputs from ASM Level 1 and 2 have also been shown. These will be relevant for other OIs.

The main output from the model is taken to be timely, correct clearances from civil and military controllers that enable separation between their respective aircraft to be maintained. A brief summary of the functional model's building blocks is given below.

GAT Handling

A large number of tasks are associated with GAT handling. However, in the context of OI-1B the key high level task is providing civil aircraft with timely, correct clearances. To carry out this task requires the following inputs:

- An accurate, up to date picture of the traffic situation.
- Co-ordination with military ATC via airspace crossing dialogue.
- An accurate, up to date picture of airspace status.

OAT Handling

Analogous to GAT handling, the key output from this block is providing military aircraft with timely, correct clearances. To carry out this task requires the same inputs as GAT handling.

Communication of Traffic Situation

This feeds into GAT and OAT handling. The communications channels (how information is communicated) are listed in Section 2.2.1. The actual information communicated and the resulting traffic picture for GAT and OAT Handling functions under b-FUA and e-FUA are shown in Tables 2.2 and 2.3. Under e-FUA the traffic situation should be better understood by the c-ATCO in particular, which will have an impact on GAT handling.

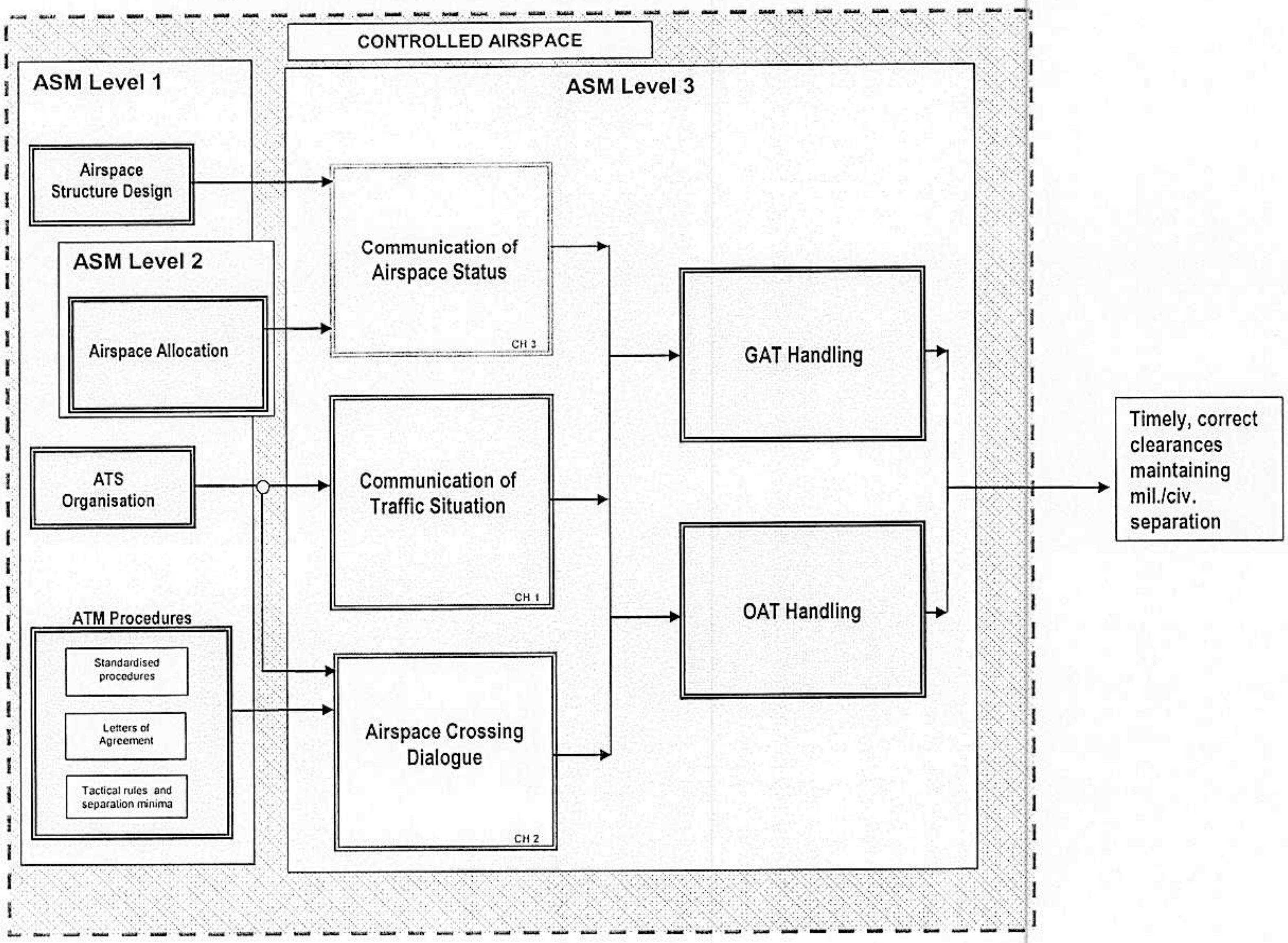
Airspace Crossing Dialogue

This also feeds into GAT and OAT handling. The basic functional description of co-ordination is not affected by OI-1B. However, the mechanisms for conducting the co-ordination process are changed from direct, verbal communication by telephone to silent exchange of electronic data as described in Section 2.2.2.

Communication of Airspace Status

The different mechanisms for feeding airspace status information to GAT and OAT handling under b-FUA and e-FUA are described in Section 2.2.3 and illustrated in Figure 2.1. The actual information content will not change, just the methods of data communication.

Figure 5.1 Functional Model of OI-1B FUA Hazards in Controlled Airspace


CONTROLLED AIRSPACE
ASM Level 1
Airspace Structure Design
ASM Level 2
Airspace Allocation
ATS Organisation
ATM Procedures
Standardised procedures
Letters of Agreement
Tactical rules and separation minima
ASM Level 3
Communication of Airspace Status
CH 3
Communication of Traffic Situation
CH 1
Airspace Crossing Dialogue
CH 2
GAT Handling
OAT Handling
Timely, correct clearances maintaining mil./civ. separation

6. FHA AND EVENT TREE ANALYSIS

6.1 Input Hazards to Event Trees

From the functional model in Figure 5.1 the key hazards relevant to OI-1B were determined to be:

- Failure to provide a timely clearance; and
- Incorrect clearance.

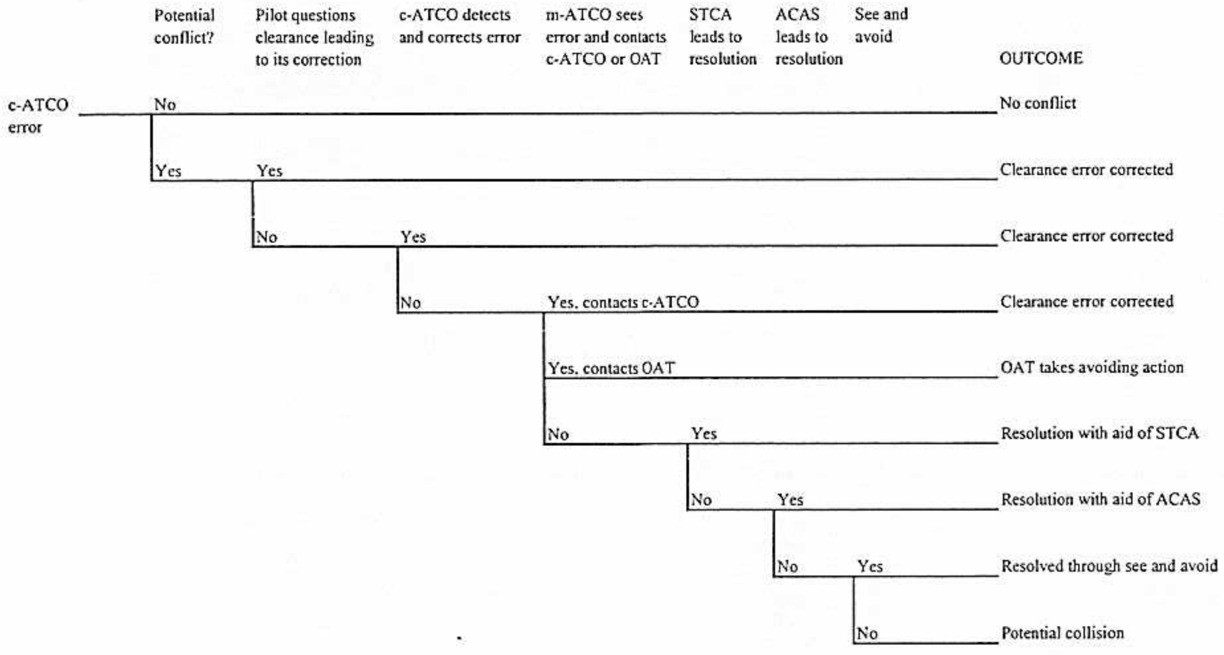
These are referred to in future sections under the umbrella title of "Clearance Error". Event Tree Analysis was used to determine the consequences of clearance error and a review was then conducted of the significance of OI-1B on the probability of these consequences.

6.2 Event Tree Analysis (ETA)

6.2.1 Event Tree Structure

The event tree for the civil controller issuing incorrect clearances is shown in Figures 6.1. This structure is based on row 64 of Table II.4 (Appendix II) and previous ETAs (e.g. Scaife et al, 2001).

Figure 6.1 Event Tree for Civil Air Traffic Controller Clearance Error


Potential conflict?
Pilot questions clearance leading to its correction
c-ATCO detects and corrects error
m-ATCO sees error and contacts c-ATCO or OAT
STCA leads to resolution
ACAS leads to resolution
See and avoid
OUTCOME
c-ATCO error
No
No conflict
Yes
Yes
Clearance error corrected
No
Yes
Clearance error corrected
No
Yes, contacts c-ATCO
Clearance error corrected
Yes, contacts OAT
OAT takes avoiding action
No
Yes
Resolution with aid of STCA
No
Yes
Resolution with aid of ACAS
No
Yes
Resolved through see and avoid
No
Potential collision

Each node of the event tree is described below:

- A clearance error may send an aircraft into empty airspace without a potential collision course.
- The pilot receiving the clearance may consider it to be either inconsistent with his experience or inappropriate considering his own picture of his situation leading to his

questioning the clearance received. On consideration or rechecking the civil controller may issue a corrected clearance.

- The civil controller (or someone else in the ACC) may observe either a developing conflict or the GAT in an unexpected location as a result of the incorrect clearance. This leads to the issue of a corrected clearance.
- The military controller (or a colleague) may observe either a developing conflict or the GAT in an unexpected location as a result of the incorrect clearance. The military controller may either contact the civil controller to prompt the issue of a corrected clearance, or he may contact the OAT to issue an avoidance instruction.
- Short term conflict alert (STCA) could alert the civil controller to a conflict and it may then be resolved.
- ACAS could alert the pilots to a conflict and it may then be resolved.
- Visual acquisition of the other aircraft might allow the pilots to take avoiding action ("see and avoid".

It should be noted that this safety assessment is taking no credit for the STCA and ACAS safety nets. It is including them in the event tree structure to ensure that the proposed system changes (OI-1B) are analysed to ensure that they do not adversely affect the operation of existing "safety nets".

The corresponding event tree for a clearance error by a military controller would be very similar to Figure 6.1, but with the roles of the military and civil controllers and pilots reversed.

The structure of the event tree is designed to illustrate the probable sequence in time for the application of each of these hazard correction measures. However, in practice, the different hazard correction measures may be "triggered" out of the assumed sequence and be just as effective.

6.2.2 Impact of OI-1B on Event Trees

Table 6.1 provides an analysis of the effect of OI-1B within e-FUA compared to b-FUA on each of the hazard mitigation measures identified in the event trees.

Table 6.1 Analysis of Effect of e-FUA on Hazard Mitigation for Civil Controllers

Event Tree Node	Effect of e-FUA OI-1B
Pilot questions clearance leading to its correction.	Implementation of OI-1B will not affect this event tree node as the mode of controller-controller communication has no effect on the pilot's ability to detect an incorrect clearance.
c-ATCO detects and corrects error.	Under e-FUA OI-1B the civil controller has a more complete picture of the traffic situation. Probabilities of successful clearance correction potentially improved.
m-ATCO sees error and contacts c-ATCO.	Military controllers' picture of the traffic situation may be unchanged by e-FUA OI-1B or slightly improved by access to GAT intention data. Probabilities of successful clearance correction either unchanged or potentially improved.
m-ATCO sees error and contacts OAT.	Military controllers' picture of the traffic situation may be unchanged by e-FUA OI-1B or only slightly improved by access to GAT intention data,. Probabilities of successful clearance correction either unchanged or potentially improved.

Event Tree Node	Effect of e-FUA OI-1B
STCA leads to resolution.	Under e-FUA OI-1B the civil controller has a more complete picture of the traffic situation and STCA should have a better picture of civil-military conflicts. Probabilities of successful clearance correction potentially improved.
ACAS leads to resolution.	Implementation of OI-1B will not affect this event tree node.
See and avoid.	Implementation of OI-1B will not affect this event tree node.

Examination of Table 6.1 indicates that the implementation of OI-1B should result in a reduction of risk levels as a result of implementing OI-1B, though the reduction may be small. There is no evidence to suggest that risk levels could increase as a result of changes to the event tree after the implementation of OI-1B compared to b-FUA.

A similar analysis has been applied to event trees where a military controller issues an incorrect clearance.

6.3 Safety Objective for Clearance Error Hazard

Based on the review above, it is concluded that the probability that a potentially dangerous conflict arises following a clearance error is probably reduced with OI-1B compared to b-FUA. However, the reduction is difficult to estimate. Therefore in line with the safety criteria in Section 3 the following safety objective is derived:

The frequency of clearance errors under OI-1B shall be no greater than under b-FUA and it shall be reduced further as far as is reasonably practicable.

In effect this objective takes "no credit" for any potential improvements in risk mitigation within the event trees.

7. PSSA AND FAULT TREE ANALYSIS

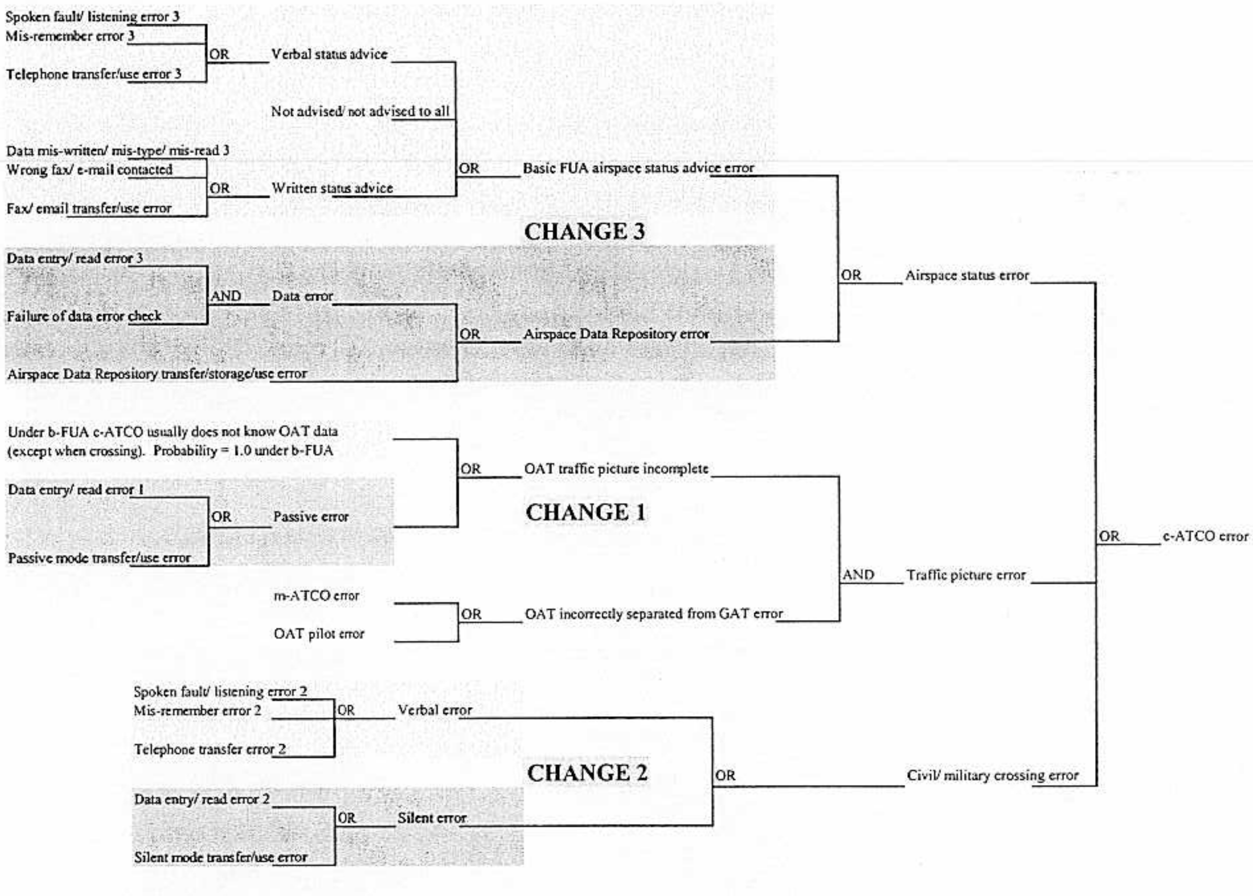
7.1 Introduction

The Preliminary System Safety Assessment analysed the causes of clearance error relevant to OI-1B. A Fault Tree approach was adopted as outlined below based on the Functional Model in Figure 5.1 and the outputs from the brainstorming session. The outputs from the brainstorming session have been mapped onto the fault tree model in Table II.5 of Appendix II.

7.2 Fault Tree Structure

The fault tree for the hazard "Civil controller issues an incorrect clearance to GAT" is shown in Figure 7.1.

Figure 7.1 Fault Tree for Civil Air Traffic Controller Clearance Error


Spoken fault/ listening error 3
Mis-remember error 3
OR
Verbal status advice
Telephone transfer/use error 3
Not advised/ not advised to all
Data mis-written/ mis-type/ mis-read 3
Wrong fax/ e-mail contacted
OR
Written status advice
Fax/ email transfer/use error
OR
Basic FUA airspace status advice error
CHANGE 3
Data entry/ read error 3
AND
Data error
Failure of data error check
OR
Airspace Data Repository error
Airspace Data Repository transfer/storage/use error
OR
Airspace status error
Under b-FUA c-ATCO usually does not know OAT data (except when crossing). Probability = 1.0 under b-FUA
OR
OAT traffic picture incomplete
Data entry/ read error 1
OR
Passive error
Passive mode transfer/use error
CHANGE 1
OR
c-ATCO error
AND
Traffic picture error
m-ATCO error
OAT pilot error
OR
OAT incorrectly separated from GAT error
Spoken fault/ listening error 2
Mis-remember error 2
OR
Verbal error
Telephone transfer error 2
CHANGE 2
OR
Civil/ military crossing error
Data entry/ read error 2
OR
Silent error
Silent mode transfer/use error

The parts of the tree shaded pale yellow relate to b-FUA and the parts shaded blue relate to e-FUA. Unshaded parts are common to basic and enhanced FUA. The yellow and blue shaded parts of the fault tree do not apply simultaneously.

The fault tree reflects the structure of the functional model for OI-1B in that an incorrect clearance can arise from one of 3 main types of error:

- An incorrect understanding of the airspace status;
- An incorrect understanding of the airspace traffic situation in terms of OAT positions relative to GAT;
- An incorrect civil-military co-ordination during OAT crossing of GAT traffic lanes.

(Of course, there are other sources of error which could result in a clearance error by a civil controller, but these are independent of the implementation status of OI-1B and so are not shown.)

In general terms, each of these errors can arise from either a technical fault, a procedural fault (such as it being unclear who should be contacted) or a human error (where the correct information is presented to the controller, but an error is still made). The key changes that arise from implementing Changes 1, 2 and 3 of OI-1B are summarised in Section 7.3 below.

It should be noted that Figure 7.1 does not explicitly include consideration of the controller to pilot communication (verbal or via datalink) because this is not directly affected by OI-1B. However it should be the case that if controller to controller communication is made more efficient, through OI-1B, then there will be more time for controller to pilot communication which may reduce error rates.

The corresponding event tree for a military controller clearance error would be very similar and hence is not repeated. The only difference is under the traffic picture error branch. In some cases there will be no, or few, differences to the military controller's traffic picture. As noted in Tables 2.2 and 2.3 in other cases the military controller may have more intention data from the civil controller. Thus the difference in this scenario is that under b-FUA the military controller lacks intention data whereas under e-FUA the military controller will have all the intention data normally, but there will be a chance of errors with entering extra intention data.

7.3 Analysis and Discussion of Fault Tree Models

7.3.1 Effect of Change 1, Passive Data Exchange, on Traffic Picture Error

The effect of Change 1, Passive Data Exchange, is most pronounced for the civil controller. Under b-FUA the civil controller will not usually be aware of the position or intention of OAT, unless they are involved in a crossing manoeuvre, in which case the data exchange between civil and military controllers is discussed in Section 7.3.2 below. Thus under b-FUA the civil controller is unable to provide a surveillance mitigation if either the OAT pilot or the military controller makes a mistake and OAT to GAT separation is reduced. (Note in some States under b-FUA the civil controller may see positions of OAT via secondary radar, but will not generally have enough information to provide an effective mitigation.)

Under e-FUA, the civil controller will see the position (and the intention, if bilaterally agreed) of OAT within his area. This position data will be correct, provided that passive data exchange is technically operational and the intention data will be correct (if present) if it has, in addition, been correctly entered by the military controller. Thus correct data will normally be presented to the civil controller and hence an additional mitigation (against military controller or OAT pilot error) has been provided. This is a safety benefit provided by e-FUA OI-1B Change 1.

The effect of Change 1 on the military controller is less pronounced. Under b-FUA the military controller sees the positions of GAT in his area via passive data exchange. This information enables him to maintain separation of OAT from GAT. Under e-FUA the military controller may gain additional information on the intention of GAT.

Alongside these safety benefits to controllers' traffic picture, Change 1 introduces alternative potential causes of traffic picture error, specifically:

- Mis-entry errors for intention data are introduced.
- Read errors including where updated information might not be recognised by the controller receiving the data passively. Data exchanged passively can be highlighted to controllers by technology (displayed differently until it is acknowledged). Failure to adopt this could result in different mental pictures for different controllers.
- Data transfer errors caused by technical failures affecting data integrity.

The requirements necessary to ensure that the risk from these new potential causes is reduced as far as reasonably practicable are discussed in Section 8.

7.3.2 Effect of Change 2, Silent Data Exchange, on Airspace Crossing Error

The key differences resulting from Change 2, Silent Data Exchange, is the replacement of verbal communication with electronic communication between civil and military controllers for the majority of situations where co-ordination is required. This means that mis-speak, mis-hear and recall errors are replaced by mis-enter and mis-read errors.

Available human error data suggests that the frequency of mis-speaking/ mis-hearing errors is broadly similar to the frequency of data entry errors, for example:

- For spoken numeric data an error rate of 2 errors per 1000 numbers transmitted (Gibson, 2003);
- For spoken information an error rate of 20 errors per 1000 transactions (Gibson, 2003);
- For mis-typing errors the error rate is similar to spoken information 20 per 1000 transactions (Rabbit, 1978).

This was an initially surprising finding, as some air traffic control professionals consider that electronic exchange of factual information between trained and experienced controllers should be subject to lower error frequencies. Whilst this may be true, the data or referenced work to support the belief has not been identified. Furthermore it should be noted that human factors personnel expected to see broadly similar error frequencies for keyed data entry and verbal communication. Corresponding error data on use of other data entry modes (e.g. mouse selection) would be helpful.

One possibility that could reconcile the available data and the views of the ATC professionals is that initial error frequencies for verbal and electronic communication are comparable, but that error recovery probabilities are higher for electronic communication. In Appendix III there is a qualitative, relative analysis of error recovery probabilities for b-FUA and e-FUA. This analysis shows that the error recovery probabilities for electronic communication (e-FUA) are at least similar to error recovery probabilities under b-FUA and probably better than under b-FUA, provided that the electronic communication procedures are well designed.

The following points should also be noted:

- The main contributor to controller workload is verbal communication since it requires a finite time for information to be exchanged. Under basic FUA, as traffic levels increase workload, and error rates, are likely to increase due to the resulting time pressure on verbal communications. Enhanced FUA would share this increase in workload between the verbal and the visual channels and thus overall workload and error rates should be reduced compared to b-FUA.
- The error rates quoted above may not take explicit account of recall errors, which will be reduced or eliminated under e-FUA. Under basic FUA a verbal communication may be received by telephone, but then forgotten due to distraction or other causes. The electronic visual communication used by e-FUA should serve as a prompt to help a controller remember that an action may be required. The e-FUA electronic message also eliminates the possible need for the controller to write the (verbal telephone) message down, which could reduce transcription errors.
- The electronic communication between controllers used by e-FUA will be quicker. This may provide more time for verbal communication between controllers and pilots which may reduce workload compared to basic FUA.
- There is evidence in the literature from ATM studies to suggest that the combination of verbal and electronic communication channels is more powerful than either in isolation (e.g. Kerns, 1991) since the additional workload is shared between the verbal and non-verbal cognitive processing channels. This reinforces the desirability of continued regular use of the telephone to perform civil military co-ordination because it keeps controllers familiar with the procedures and with communicating with each other as people. This could be important in the case of either an emergency situation, or if e-FUA systems go offline.

It can be concluded therefore that, on the basis of the available information, that implementation of OI-1B Change 2 should be at least as safe as b-FUA and could be safer than b-FUA, provided that suitable safeguards are put in place. Requirements covering data entry, data reading and data transfer are covered in Section 8.

Better data on comparative error frequencies between verbal communication and electronic communication in the ATM context would be helpful. This could be obtained from simulation trials or operational data.

7.3.3 Effect of Change 3, Airspace Data Repository, on Airspace Status Error

The effect of Change 3, the Airspace Data Repository, is the hardest to evaluate because, compared to Changes 1 and 2, the procedural aspects of the use of the Airspace Data Repository are currently less well defined. Nevertheless a qualitative assessment of the proposed changes indicates advantages for e-FUA, i.e.

- Bi-lateral verbal communication is mainly eliminated at Level 3, thus removing mis-spoken, mis-hear and recall errors.
- Under b-FUA there is an increased probability that different parties have different pictures of the airspace status due to not being advised at all.

Set along these advantages, Change 3 introduces alternative causes for data entry and read errors together with data transfer and storage errors. Requirements to safeguard against these causes are addressed in Section 8.

A feature of e-FUA is that any mis-entry errors are communicated to all parties and thus a widespread error is possible. However, this error will be consistent to all parties which generally will be safer than an inconsistent, partially correct airspace status picture.

A potential error mode of the Airspace Data Repository that has been identified is that controllers should not be able to make an airspace structure active and then direct aircraft to use the structure without reference to the airspace structure status in the Airspace Data Repository. Failure to ensure this could allow them to forget to activate the structure (informing others of its use) leading to an inconsistent picture of airspace status between different controllers. Thus the procedures for use of the Airspace Data Repository should force all controllers to check the current status of the airspace structure they use from the Airspace Data Repository, prior to clearing aircraft to use the structure. This is also captured as a requirement in Section 8.

Overall, based on these high level considerations, Change 3 should be at least as safe as b-FUA and could be safer provided that the safety requirements in Section 8 are put in place.

7.4 Other Impacts of the Proposed Changes

In addition to the specific causes of traffic picture error, airspace co-ordination error and airspace status error investigated in the fault trees, the proposed changes 1 to 3 under OI-1B will have other, more general, effects.

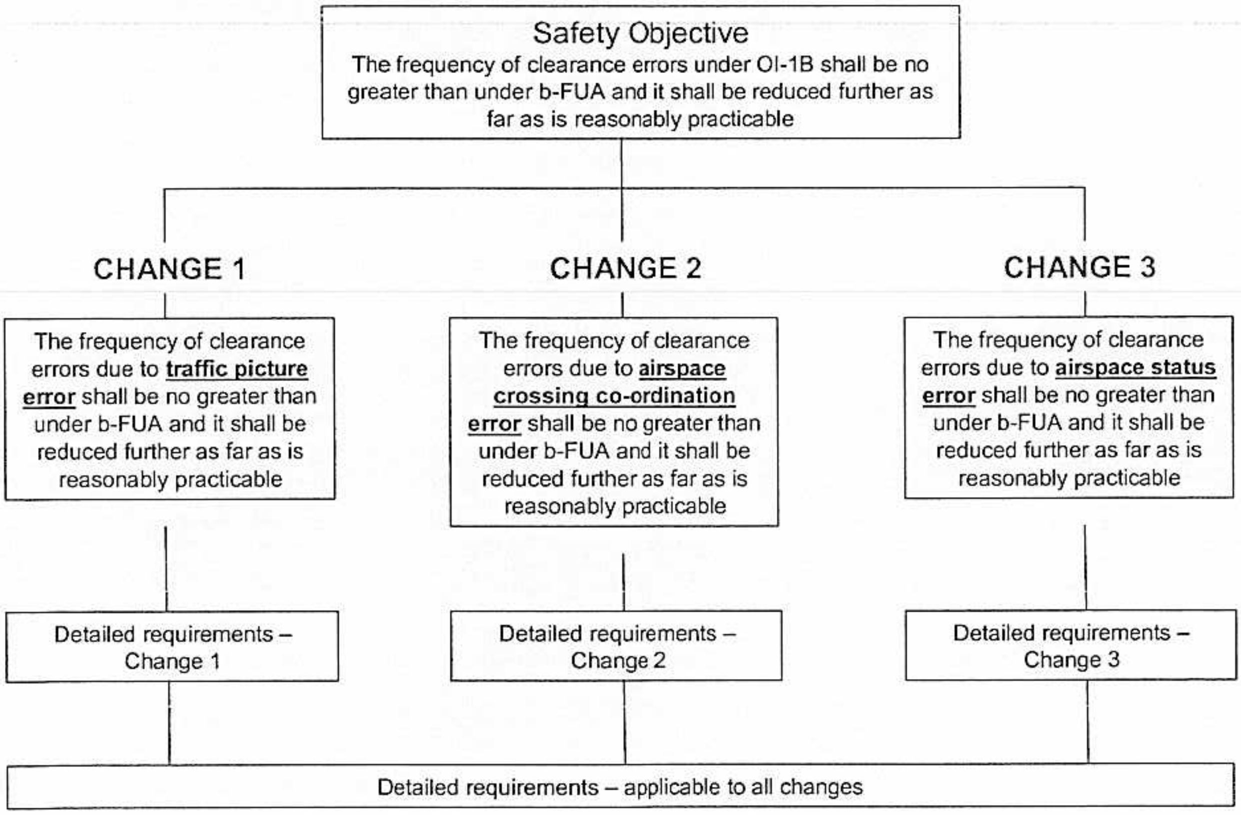
- The main aim of e-FUA is to improve efficiency of airspace utilisation. Hence it is to be expected that OI-1B will lead to higher traffic levels. In the event of a system failure (e.g. surveillance or communications) recovery could be more challenging. Emergency procedures in the event of a system failure need to be addressed and this is covered as a requirement in Section 8.
- More uniform civil-military co-ordination procedures across ECAC States should lead to improved understanding and a safety benefit. However, the possible safety benefit due to this general effect has not been assumed when deriving the safety requirements for OI-1B.

8. SAFETY ASSESSMENT AND SAFETY REQUIREMENTS

8.1 Assessment Against the Safety Criteria and Objective

The Event Tree Analysis in Section 6 enabled the safety criteria in Section 3 to be translated into a safety objective for the hazard of clearance error. This safety objective can be further translated into high-level safety requirements related to the 3 proposed changes as illustrated in Figure 8.1. By cascading the safety criteria down in this way enables a pair-wise comparison of b-FUA v e-FUA for each change. A judgement can be made about the relative risks in the context of each change and more detailed requirements can be identified. These detailed requirements are set out in Section 8.2.

Figure 8.1 Framework for Safety Requirements Development


Safety Objective
The frequency of clearance errors under OI-1B shall be no greater than under b-FUA and it shall be reduced further as far as is reasonably practicable
CHANGE 1
CHANGE 2
CHANGE 3
The frequency of clearance errors due to traffic picture error shall be no greater than under b-FUA and it shall be reduced further as far as is reasonably practicable
The frequency of clearance errors due to airspace crossing co-ordination error shall be no greater than under b-FUA and it shall be reduced further as far as is reasonably practicable
The frequency of clearance errors due to airspace status error shall be no greater than under b-FUA and it shall be reduced further as far as is reasonably practicable
Detailed requirements – Change 1
Detailed requirements – Change 2
Detailed requirements – Change 3
Detailed requirements – applicable to all changes

8.2 Detailed Safety Requirements

8.2.1 Introduction

The detailed safety requirements for Changes 1 to 3 described below relate to the end branches of the fault tree branches representing causes of hazards under e-FUA OI-1B (see Figure 7.1). The sources for the requirements have been:

- The FHA/PSSA structured brainstorming session (see Appendix II); additional mitigation measures comments were proposed (see Hazard Log in Table II.4). These have been considered and where judged effective in reducing risk and practicable they have been included as a requirement.

- The human factors (HF) analysis, TRACEr (see Appendix III); this analysis was based on assumptions of good HF practice and these assumptions have been turned into requirements.
- Consideration of the Event Tree Analysis (ETA) nodes in mitigation of consequences in Section 6.
- Consideration of system integrity using the Fault Tree Analysis (FTA) in Section 7.
- Monitoring requirements from the Safety Plan.

8.2.2 Change 1 – Passive Data Exchange

Requirements	Source of Requirement
Requirements related to Data Entry and Reading (see Figure 7.1, CHANGE 1, "Data entry/ read error 1")	
1.1. Information exchanged by the passive mode shall be labelled as new until accepted by the receiving ATCO.	Hazard Log (row 7)*
1.2. To reduce data entry errors appropriate use shall be made of automatic syntax and spelling checkers for passive data exchange.	Hazard Log (row 1) & TRACEr
Requirements related to Transfer and Use of Data (see Figure 7.1, CHANGE 1, "Passive mode transfer/use error")	
1.3. Passively exchanged data shall be used as a feed into STCA where this provides safety benefits.	ETA
1.4. Before the use of passive data exchange leads to removal of a requirement for co-ordination between civil and military controllers, a site-specific safety assessment shall be carried out to ensure that risk will not increase through this change.	Hazard Log (row 5)
1.5. Systems for passive data exchange shall have integrity levels no lower than those for b-FUA systems (verbal via telephone). This level of integrity shall be achieved irrespective of equipment inter-operability issues.	FTA & Hazard Log (row 56)

* Only first relevant row in Table II.4 referenced

8.2.3 Change 2 – Airspace Crossing Dialogue/ Co-ordination and Silent Data Exchange

Requirements		Source of Requirement
Requirements related to Data Entry and Reading (see Figure 7.1, CHANGE 2, "Data entry/ read error 2")		
2.1.	Each stage of the silent mode co-ordination process shall be coded visually so that the ATCO is immediately aware of the transaction status.	TRACEr
2.2.	Standard phraseology shall be used in the silent data exchange.	TRACEr
2.3.	To reduce data entry errors appropriate use shall be made of automatic syntax and spelling checkers for silent data exchange.	TRACEr
Requirements related to Transfer and Use of Data (see Figure 7.1, CHANGE 2, "Silent mode transfer/use error")		
2.4.	Procedures shall be in place to identify which controller should be contacted during co-ordination. (While these should already be in place under b-FUA, it is especially important under e-FUA as there might not be immediate recognition if data is sent to the wrong person).	TRACEr
2.5.	Silent mode messages after the initial clearance request shall be automatically routed to the correct controller (similar to "Reply" using email).	TRACEr
2.6.	Silent mode communications shall include sufficient contextual and supporting information to enable the identification of mis-addressed messages.	TRACEr
2.7.	The voice communication telephone systems used for co-ordination under b-FUA shall be maintained (both the hardware and through regular ATCO practice).	Hazard Log (row 15)
2.8.	Systems for silent data exchange shall have integrity levels no lower than those for b-FUA systems (verbal telephone). This level of integrity should be achieved irrespective of equipment inter-operability issues.	FTA & Hazard Log (row 56)

8.2.4 Change 3 – Airspace Status and Airspace Data Repository

Requirements		Source of Requirement
Requirements related to Data Entry and Reading (see Figure 7.1, CHANGE 3, "Data entry/ read error 3")		
3.1.	Authorisation levels shall be set for writing to and reading from the ADR.	Hazard Log (row 25)
3.2.	Procedures shall be in place for preparing, entering, checking and retrieving data from the ADR.	Hazard Log (row 25)
3.3.	To reduce data entry errors appropriate use shall be made of automatic syntax and spelling checkers for writing to the ADR.	TRACEr
Requirements related to Storage, Transfer and Use of Data (see Figure 7.1, CHANGE 3, "Airspace Data Repository transfer/storage/use error")		
3.4.	Procedures for use of the Airspace Data Repository shall ensure that all controllers check the current status of the airspace structure they use from the Airspace Data Repository, prior to clearing aircraft to use the structure.	FTA, Section 7.3.3*
3.5.	The Airspace Data Repository systems shall have integrity levels no lower than those for b-FUA (fax or verbal via telephone). This level of integrity shall be achieved irrespective of equipment inter-operability issues.	FTA & Hazard Log (rows 24 and 56)

* Controllers should only see current airspace status; too much information can be distracting

8.2.5 Requirements for OI-1B Applicable to All Changes

Requirements		Source of Requirement
Additional Technical Requirements Related to Data Transfer (see Figure 7.1, CHANGES 1, 2& 3, "transfer errors")		
4.1.	Time delays for exchange of data shall be no greater than those under b-FUA.	Hazard Log (row 30)
4.2.	Data compatibility and system interoperability shall be assured through the design process.	Hazard Log (row 56)
4.3.	The availability of new systems under OI-1B shall be at least as high as equivalent systems under b-FUA, using system redundancy if required.	Hazard Log (row 4)
4.4.	The potential for common cause failure modes and other installation specific issues which could degrade system availability and integrity unacceptably shall be assessed.	Supporting requirements 1.5, 2.8, 3.5 and 4.3
4.5.	All new systems to support OI-1B shall fail safe (that is, shall not appear to be working when they are not, consistent with verbal co-ordination processes performed under b-FUA).	Hazard Log (row 4)
4.6.	Consideration shall be given to whether equipment to support OI-1B should be subject to third party testing and certification. Inter-operability would be a key part of such third party testing.	Hazard Log (row 56)
Additional Human Factors, Procedures and Safety Management Requirements (applicable across all branches of Fault Tree in Figure 7.1)		
4.7.	Consideration shall be given to human factors including human machine interface issues during the design phase of equipment and procedures to support changes required by OI-1B.	Hazard Log (row 3)
4.8.	A system performance and incident evaluation programme shall be implemented during switch-over to OI-1B so that any unexpected operational factors are identified, understood and, if necessary, resolved promptly.	Safety Plan, Section 5.4
4.9.	Controller workload shall be monitored during and following switch-over to OI-1B to determine whether the potential safety benefits discussed in the FHA/PSSA report are being realised.	Safety Plan, Section 5.4 and current report, Section 7.3.2
4.10.	Contingency planning and drills shall include the scenario where passive and silent data exchange systems and/ or the ADR fail.	Hazard Log (rows 4 and 20)
4.11.	As traffic levels increase under e-FUA, it shall be regularly checked that emergency procedures (e.g. in event of surveillance and/ or communications failure) are still adequate.	Hazard Log (row 30)
4.12.	Appropriate training shall be provided for all new systems.	Hazard Log (row 3)

9. CONCLUSIONS AND RECOMMENDATIONS

A generic safety assessment has been conducted to support an Outline Safety Case of OI-1B. Safety requirements have been derived in order that the safety criteria for the proposed operational improvement will be met.

Although the main aim of the operational improvement is to improve efficiency of airspace utilisation, it also has some inherent safety benefits, principally improvement of controllers' traffic picture and providing a more consistent picture of airspace status to all relevant parties. No new hazards have been identified, although replacement causes for existing hazards will result from the changes. The safety requirements identified should ensure that the risk from these replacement causes is no greater than that from existing causes and that it is reduced further as far as reasonably practicable.

It should be noted that currently there is little detail concerning procedures for the Airspace Data Repository, Change 3. It is recommended that when more detail does become available, the safety assessment is revisited to check on its impact.

It is also recommended that further evidence on the error frequencies of verbal and electronic (keyed and menu driven selected data using mouse or tracker ball etc) communication in the ATM sector should be collected and used to validate (or otherwise) the conclusions of this report.

10. RELATIONSHIP OF THIS WORK TO THE OUTLINE SAFETY CASE

This report describes the processes and results of the main safety assessment work performed by DNV and EUROCONTROL in support of the implementation of e-FUA OI-1B. The main outputs from this report will be fed into the Outline Safety Case for e-FUA OI-1B which will describe the full safety argument why OI-1B is acceptably safe in principle for implementation in ECAC States. The safety argument includes reference to operational and management issues that should also be considered in addition to the factors assessed in this report.

The Outline Safety Case also provides ECAC States with a "road-map" to assist them with what they have to do to show that their implementation of OI-1B within their national boundaries is acceptably safe. The work that each State does to demonstrate that OI-1B is acceptably safe should be documented in their own National Safety Cases.

11. REFERENCES, ACRONYMS AND ABBREVIATIONS

11.1 References

EUROCONTROL, 1994a “Report on Organisational Structures and Procedures Required for the Application of the Concept of the Flexible Use of Airspace”, Doc. 94.70.08, March 1994.

EUROCONTROL, 1996a “Functional Specifications for System Support to Airspace Data Distribution and Civil/Military Co-ordination”, DPS.ET1.ST10.2000-FS-01-00, Edition 1.0, 15/05/96.

EUROCONTROL, 2000a “Functional Hazard Assessment”, SAM SAF.ET1.ST03.1000-MAN-01-00

EUROCONTROL, 2000b “Use of Safety Management Systems by ATM Service Providers”, EUROCONTROL Safety Regulatory Requirement (ESARR) 3, Edition 1.0, Released Issue.

EUROCONTROL, 2001a “EATMP Safety Policy”, Edition 2.0.

EUROCONTROL, 2001b "Risk Assessment and Mitigation in ATM", EUROCONTROL Safety Regulatory Requirement (ESARR) 4, Edition 1.0.

EUROCONTROL , 2001c “EUROCONTROL Airspace Strategy for ECAC States”, ASM.ET1.ST03.4000-EAS-01-00, Edition 1.0, 18/01/01.

EUROCONTROL, 2002a “Assessment of EATMP Air Navigation System Safety Assessment Methodology as a Means of Compliance with ESARR4”, SRC DOC 12, Edition 1.0.

EUROCONTROL, 2003a “Enhanced FUA Process Safety Policy, Draft, Edition 0.1, 12/01/04.

EUROCONTROL, 2003b “Enhanced FUA Process Safety Plan”, Draft, Edition 0.1, 12/01/04.

EUROCONTROL, 2003c “Outline Safety Case for Enhanced Real-time Civil/Military Co-ordination (OI-1B)”, Draft, Edition 0.1, 19/03/04.

EUROCONTROL, 2003d “Guidance Document for the Implementation of the Concept of the Flexible Use of Airspace”, ASM.ET1.ST08.5000-GUI-02-00, Edition 2.0, 18/08/03.

EUROCONTROL, 2003e “Safety Assessment Methodology Part II: Preliminary System Safety Assessment”

EUROCONTROL, 2003f “Safety Case Development Manual”, Edition 1.3, 07.07.03

EUROCONTROL, 2003g “EUROCONTROL Handbook for Airspace Management”, ASM.ET1.ST08.5000-HBK-02-00, Edition 2.0, 22/10/03

EUROCONTROL, 2003h “EUROCONTROL Manual for Airspace Planning”, ASM.ET1.ST08.5000-EAPM-02-02, Edition 2.0, 22/10/03

EUROCONTROL, 2003i “Software in ATM Systems”, EUROCONTROL Safety Regulatory Requirement (ESARR) 6, Edition 0.4, Proposed Issue.

Gibson et al, 2003 “First European Conference on Rail Human Factors”, 13-15 October 2003, York, UK.

ICAO, Annex 11 "Amendment 38 to ICAO Annex 11; International Standards and Recommended Practices, Air Traffic Services".

ICAO, 1980 "Manual on the Use of the Collision Risk Model (CRM) for ILS Operations", Doc 9274-AN/904, First Edition 1980.

ICAO, 1998 "Manual on Airspace Planning Methodology

Kerns, 1991 "Data-Link Communications between controllers and pilots: a review and synthesis of the simulation literature", Int. Journal of Aviation Psychology, 1, 181-204, 1991.

Rabbit, 1978 "Detection of errors by skilled typists", *Ergonomics*, **21**, pp. 945-958.

Scaife, R., Shorrock, S. and Smith, E., 2001 "The Practical Application of Error Analysis and Safety Modelling in Air Traffic Management", IBC Human Error Conference, 2001

Shorrock et al, 1998 "The Development of TRACEr: A Technique for the Retrospective Analysis of Cognitive Errors in ATM" Engineering Psychology and Cognitive Ergonomics. Volume Three: Transportation Systems, Medical Ergonomics and Training, Edited by D. Harris. Ashgate Publishing, Aldershot, Hampshire Year: 1999 Pages: 163-171

11.2 Acronyms and Abbreviations

ACAS	Airborne Collision Avoidance System
ACC	–Area Control Centre
ACP	Airspace Crossing Acceptance Message
AFN	Airspace/ Flow Management and Navigation Business Division
AMC	Air Management Cell
ANSP	Air Navigation Service Provider
ATCO	Air Traffic Controller
ATM	Air Traffic Management
ATS	Air Traffic Service
BFD	Basic Flight Plan Data
CBA	Cross Border Area
CDR	Conditional Route, of types: CDR 1, CDR 2 and CDR 3
CFD	Current Flight Plan Data
CFIT	Controlled Flight Into Terrain
CRAM	Conditional Route Availability Message
CRM	Collision Risk Modelling
D	Danger Area
DAS	EUROCONTROL Directorate of ATM Strategies
DfC	Direction for Change
EATMP	European Air Traffic Management Programme
ECAC	European Civil Aviation Conference
ESARR	EUROCONTROL Safety Regulatory Requirement
ETA	Event Tree Analysis
FHA	Functional Hazard Assessment
FTA	Fault Tree Analysis
FUA	Flexible Use of Airspace
GAT	General Air Traffic
GSN	Goal Structured Notation
HMI	Human Machine Interface
ICAO	International Civil Aviation Organisation
JAA	Joint Aviation Authorities

LoA	Letters of Agreement
OAT	Operational Air Traffic
OI	Operational Improvement
P	Prohibited Area
PCA	Prior Co-ordination Airspace
PISC	Pre-Implementation Safety Case
POSC	Post implementation Safety Case
PSSA	Preliminary System Safety Assessment
R	Restricted Area
RCA	Reduced Co-ordination Airspace
RGCSP	Review of the General Concept of Separation Panel (ICAO)
RJC	Airspace Crossing Reject Message
SOP	Standard Operating Procedures
SRC	Safety Regulatory Commission
SRU	Safety Regulatory Unit
SSA	System Safety Assessment
SSR	Secondary Surveillance Radar
TAA	Temporary Airspace Allocation
TLS	Target Level Safety
TRA	Temporary Reserved Area
TRACEr	Technique for the Retrospective and Predictive Analysis of Cognitive Errors
TSA	Temporary Segregated Area
XAP	Airspace Crossing Alternate Proposal Message
XCM	Airspace Crossing Cancellation Message
XIN	Airspace Crossing Intention Notification Message
XRQ	Airspace Crossing Clearance Request Message

Prefixes

b-	basic
c-	civil
e-	enhanced
m-	military
p-	pre