EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

ASM/ATFCM Procedure 3
Preliminary Safety Case

Edition Number	**:**	**v2.0**
Edition Date	**:**	**July 2010**
Status	**:**	**Proposed Issue**
Intended for	**:**	**Restricted audience**

DOCUMENT CHARACTERISTICS

TITLE		
ASM/ATFCM Procedure 3 Preliminary Safety Case		
	Publications Reference:	
	ISBN Number:	
Document Identifier	**Edition Number:**	v2.0
	Edition Date:	July 2010

Abstract

The European Organisation for the Safety of Air Navigation (EUROCONTROL) ASM Improvement Initiative aims to deliver concrete ASM improvements in 2009 and 2011. One of the objectives is to implement new procedures to support the optimisation of airspace usage for both civil and military airspace users.

This Preliminary Safety Case (PSC) Report provides some of the evidence to support the top-level claim that the activation/deactivation of airspace via application of ASM/ATFCM Procedure 3 contributes to the achievement of an *acceptable level of safety* in the operating environment within which it is implemented.

Keywords

ASM	Airspace activation	PSSA	Civil
ATFCM	FHA	Safety Assessment	Military
Procedure 3	Generic		

Authors

Contact(s) Person	Tel	Unit

STATUS, AUDIENCE AND ACCESSIBILITY					
Status		**Intended for**		**Accessible via**	
Working Draft	☐	General Public	☐	Intranet	☐
Draft	☐	EATM Stakeholders	☐	Extranet	☐
Proposed Issue	☑	Restricted Audience	☑	Internet (www.eurocontrol.int)	☐
Released Issue	☐	*Electronic copies of this document can be downloaded from*			

DOCUMENT APPROVAL

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

AUTHORITY	NAME AND SIGNATURE	DATE

DOCUMENT CHANGE RECORD

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

EDITION NUMBER	EDITION DATE	REASON FOR CHANGE	PAGES AFFECTED
0.1	December 2009	Initial Working Draft	ALL
0.2	April 2010	Updated to include safety assessment results	ALL
1.0	May 2010	Definitive issue	ALL
2.0	July 2010	Final issue following ANT/52 with updated and agreed **HAZ002** title	ALL

Publications

EUROCONTROL Headquarters

96 Rue de la Fusée

B-1130 BRUSSELS

Tel: +32 (0)2 729 4715

Fax: +32 (0)2 729 5149

E-mail: publications@eurocontrol.int

Table of Contents

EXECUTIVE SUMMARY

The European Organisation for the Safety of Air Navigation (EUROCONTROL) ASM Improvement Initiative aims to deliver concrete ASM improvements in 2009 and 2011. One of the objectives of this initiative is to implement new procedures to support the optimisation of airspace usage for both civil and military airspace users.

One of the new procedures ASM/ATFCM Procedure 3 – Unplanned Airspace Activation, provides the facility for military users to book additional airspace that could not have been foreseen in the Airspace Use Pan (AUP). The impact of the unplanned airspace activations will be assessed using the Updated Airspace Use Plan (UUP) process.

Live trials of the new procedures were carried out in November 2008. However, the pre-trial safety analysis identified a number of concerns with ASM/ATFCM Procedure 3 and it became evident that this procedure was more complex than originally envisaged and that further safety analysis was required.

This Preliminary Safety Case provides a sub-set of the evidence to support the top-level claim that the activation/deactivation of airspace via application of ASM/ATFCM Procedure 3 contributes to the achievement of an *acceptable level of safety* in the operating environment within which it is implemented. This claim is broken down into the following five principle safety arguments:

- ASM/ATFCM Procedure 3 has been specified to be acceptably safe (**Arg 1**)
- ASM/ATFCM Procedure 3 has been designed to be acceptably safe (**Arg 2**)
- ASM/ATFCM Procedure 3 will be implemented completely and correctly (**Arg 3**)
- The transition towards full implementation of ASM/ATFCM Procedure 3 will be acceptably safe (**Arg 4**)
- The safety of ASM/ATFCM Procedure 3 in operation will continue to be demonstrated in operational service (**Arg 5**).

In this context, an acceptable level of safety is defined as the 'risks' to other airspace users being:

- no higher than existed prior to the introduction of ASM/ATFCM Procedure 3, and;
- has been reduced As Far As Reasonably Practicable (AFARP).

This Preliminary Safety Case is confined to mainly addressing the first two safety arguments due to the scope of the generic safety assessment undertaken.

It is concluded that, subject to the identified assumptions, resolution of safety issues and recommendations detailed in sections 7 and 8, there is adequate evidence to support **Arg 1** and **Arg 2** i.e. that ASM/ATFCM Procedure 3 has been specified and designed to be acceptably safe.

1 INTRODUCTION

1.1 Background

The Dynamic Management of the European Airspace Network (DMEAN) Concept of Operations calls for a collaborative airspace, flow and capacity management to optimise the use of airspace and the existing en-route and airport capacities through the enhancement of ASM/ATFCM processes. This means the strengthening of the relationship between Airspace Management Cells (AMCs), Flow Management Positions (FMP) and the Central Flow Management Unit (CFMU) through the establishment of more efficient coordination mechanisms. The aim is to minimise the impact of any disruptions (e.g. route closure) and to take advantage of opportunities such as additional route availability in order to enable all airspace users to conduct efficient real-time operations.

Three main weaknesses were identified with today's situation:

- National airspace allocation decisions are not always coordinated with neighbours (they are still not considered from a network perspective).

- There is no possibility for aircraft operators to optimise flight plans on the basis of airspace opportunities (notification of addition route availability is frozen on the day before operations and there is no adequate notification of route updates on the day of operations).

- Possibilities on the day of operations to activate non-planned military areas are limited.

On the basis of these three main weaknesses, three procedures have been developed:

- **ASM/ATFCM Procedure 1**: Optimising capacity usage via an assessment on the impact on the network of expected airspace allocation during activities the day before operation.

- **ASM/ATFCM Procedure 2**: Making better use of airspace opportunities (alteration of airspace restrictions, increase route availability) on the day of operations in order to provide additional route options to aircraft operators.

- **ASM/ATFCM Procedure 3**: Ensuring more flexible use of airspace on the day of operations in order to better respond to ad-hoc military needs while minimising the negative impact on the network.

Live Trials were carried out in November 2008 and confirmed that Procedures 1 and 2 were mature enough to be included in the ASM Handbook. During preparation for the trials it became apparent that safety issues associated with Procedure 3 'Unplanned activation of TSAs/TRAs', were more complex than originally envisaged and as such further work was required to assess the safety hazards and develop a Preliminary Safety Case. These safety issues are documented in the November Live Trial Final Report [1].

1.2 Purpose

This PSC aims to demonstrate that, in principle, the activation/deactivation of airspace via application of ASM/ATFCM Procedure 3 contributes to the achievement of an acceptable

level of safety1 in the operating environment within which it is implemented and that achievable safety requirements have been derived.

1.3 Scope

This PSC report summarises the preliminary safety assurance activities undertaken to derive high level safety requirements for ASM/ATFCM Procedure 3 to ensure that it contributes to the achievement of an *acceptable level of safety* and will continue to do so.

Furthermore, detailed scoping statements related to ASM/ATFCM Procedure 3 are provided in section 4.3.3 of this report.

1.4 Safety Regulatory Context

The following EUROCONTROL Safety Regulatory Requirement (ESARR) is relevant to the generic safety assessment of ASM/ATFCM Procedure 3:

- **ESARR 4**: Risk Assessment and Mitigation in ATM [3] is central to the objectives of the safety assurance in terms of demonstrating that potential risks to safety are identified and appropriately mitigated. The approach taken herein is consistent with the general (qualitative) requirements of ESARR 4, as shown in Appendix A.

1.5 General Safety Case Approach

The approach adopted is based on the Guidelines for the Safety Assessment of ATM Procedures [5] and the Safety Case Development Manual [8] developed by EUROCONTROL and complies with the general (qualitative) requirements of ESARR 4 [3] as presented in Appendix A. Specifically, the approach aims to demonstrate that the risks from hazards associated with ASM/ATFCM Procedure 3 can be controlled so that the procedure will contribute to the achievement of an *acceptable level of safety*. The generic safety assessment has also adopted the guidance provided within the EUROCONTROL Safety Assessment Made Easier (SAME) [11], Part 1 of which was released in January 2010.

1.6 Structure

The ASM/ATFCM Procedure 3 Preliminary Safety Case Report is sub divided into a number of sections as follows:

Section 1 Introduction – presents an overview of the Preliminary Safety Case, its background, purpose and scope.

Section 2 References and Abbreviations – provides a list of the documents referenced and the abbreviations used within this report.

Section 3 Overall Safety Argument – presents the top level argument for ASM/ATFCM Procedure 3.

Section 4 Safety Specification (Arg **1)** – presents the arguments and supporting evidence that substantiate the claim that ASM/ATFCM Procedure 3 has been specified to be acceptably safe.

[1] An *acceptable level of safety* is defined in section 3.2.1.

Section 5 Design Specification (Arg **2)** – presents the arguments and supporting evidence that substantiate the claim that ASM/ATFCM Procedure 3 has been logically designed to be acceptably safe.

Section 6 Implementation, Transition and On-going Operations - presents **Args 3**, **4** and **5** which address the implementation, transition to and operation of ASM/ATFCM Procedure 3.

Section 7 Assumptions, Issues and Limitations– presents the caveats associated with the generic safety assessment on which this report is based.

Section 8 Conclusion and Recommendations – brings together the conclusions and recommendations from the report.

The ASM/ATFCM Procedure 3 Preliminary Safety Case also contains the following Appendices:

Appendix A ESSAR 4 Compliance Statements – shows the degree and extent to which the approach taken is compliant with the analysis process requirements of ESARR 4.

Appendix B ASM/ATFCM Procedure 3 Models – presents the models developed to support the generic safety assessment.

Appendix C ASM/ATFCM Procedure 3 – provides the draft ASM/ATFCM Procedure 3 for ease of reference.

Appendix D ASM/ATFCM Procedure 3 Safety Requirements – presents the complete set of ASM/ATFCM Procedure 3 safety requirements.

Appendix E Goal Structured Notation (GSN) – presents a guide to understanding the ASM/ATFCM Procedure 3 safety argument.

2 REFERENCES AND ABBREVIATIONS

2.1 References

The following references were used to support this Preliminary Safety Case:

[1] November 2008 Live Trial Final Report, No reference, Edition v1.0, 01 March 2009

[2] Safety Assessment Report for ASM/ATFCM Procedure 3, P090015.10.4, Latest edition

[3] EUROCONTROL Handbook for Airspace Management, ASM.ET1.ST08.5000-HBK - 02-00, Edition 2.0, 22 October 2003

[4] ESARR 4, Risk Assessment and Mitigation in ATM, Edition 1.0, 05 April 2001

[5] Guidelines for the Safety Assessment of ATM Procedures (SAAP), SAF.ET1.ST03.1000-SAAP-01-00, Edition 0.10, 25 April 2006

[6] Generic Safety Argument for ATM Safety Assessment, v1.1

[7] Classification of Airborne Equipment Failures, JAA JAR25-1309

[8] DAP/SSH/091, Safety Case Development Manual, Version 2.2, 13 November 2006.

[9] MOM ASM/ATFCM Procedure 3 Safety Assessment Workshop, P09015.10.3, v1.0, 30 November 2009.

[10] Air Navigation System Safety Assessment Methodology, SAF.ET1.ST03.1000-MAN-01, Edition 2.1, 03 October 2006.

[11] Safety Assessment Made Easier, Part 1 – Safety Principles and an Introduction to Safety Assessment, Edition 1.0, 15th January 2010.

[12] Safety Assessment Made Easier, Part 2, Safety Assessment – Theory and Practice, Edition 0.4, 14th November 2009.

[13] Air Traffic Flow and Capacity Management Operations ATFCM Users Manual, Latest Edition

[14] Integrated Initial Flight Plan Processing System IFPS Users Manual, Latest Edition

2.2 Abbreviations

The following abbreviations and acronyms were used within this Preliminary Safety Case:

Abbreviation	Definition
AFARP	As Far As Reasonably Practicable
AFTN	Aeronautical Fixed Telecommunication Network
AIM	ATFM Information Message
ALR	Assurance Level Requirement
AMC	Air Management Cell
AO	Aircraft Operator

Abbreviation	Definition
ATC	Air Traffic Control
ASM	Airspace Management
ATFCM	Air Traffic Flow and Capacity Management
ATFM	Air Traffic Flow Management
AUP	Airspace Use Plan
CADF	Centralised Airspace Data Function
CDR	Conditional Route
CFMU	Central Flow Management Unit
CRAM	Conditional Route Availability Message
eAMI	electronic Airspace Management Information
EFSR	External Functional Safety Requirement
ENV Database	Environment Database
EOBT	Estimated Off Block Time
ESARR	EUROCONTROL Safety Regulatory Requirement
ETA	Event Tree Analysis
FFA	Functional Failure Analysis
FHA	Functional Hazard Assessment
FMP	Flow Management Planning
FPL	Flight Plan
FSR	Functional Safety Requirement
FTP	File Transfer Protocol
FUA	Flexible Use of Airspace
GAT	General Air Traffic
GSN	Goal Structuring Notation
IFPS	Initial Flight Plan Processing System
OAT	Operational Air Traffic
PAL	Procedure Assurance Level
PSC	Preliminary Safety Case
PSSA	Preliminary System Safety Assessment
SAR	Safety Assessment Report
SMR	Safety Monitoring Requirement
TRA	Temporary Restricted Area
TSA	Temporary Segregated Area
UTC	Coordinated Universal Time
UUP	Updated Airspace Use Plan

Table 1: Table of Abbreviations

3 OVERALL SAFETY ARGUMENT

3.1 Objectives

The objectives of this section are to:

- Outline the overall top-level safety argument for ASM/ATFCM Procedure 3
- Present and explain the supporting argument structure and related context and justification
- Explain the decomposition of the safety argument.

The overall safety argument is presented in Figure 1 below using Goal Structuring Notation (GSN). Appendix E presents a guide to GSN.

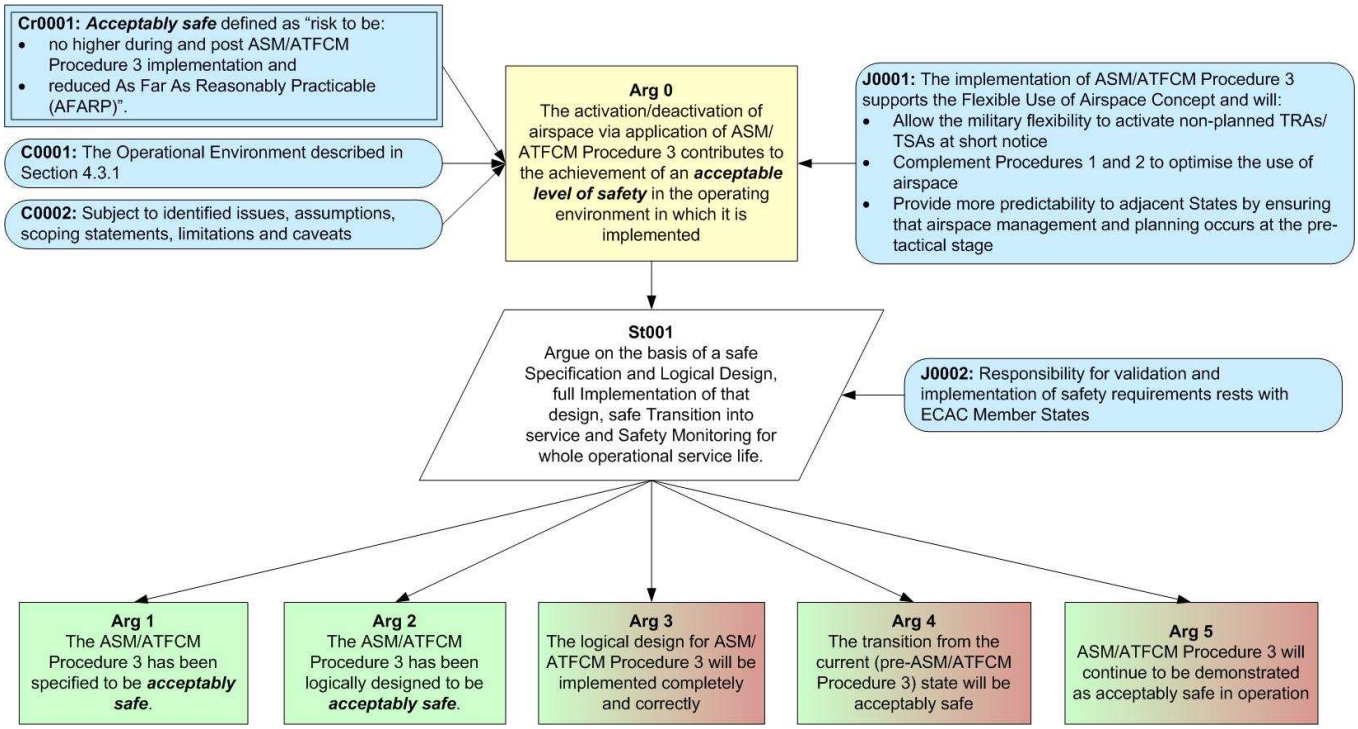


Figure 1: ASM/ATFCM Procedure 3 Overall Safety Argument

3.2 The Safety Claim

The overriding justification for the implementation of the ASM/ATFCM Procedure 3 (**J0001**) is that the ASM/ATFCM Procedure 3 will allow the military flexibility at short notice thus increasing capacity for other traffic and provide more predictability to adjacent States by ensuring that airspace management and planning occurs at the pre-tactical stage.

The primary aim of the generic safety assessment process at this level is to provide assurance to support the Claim (**Arg 0**) that the activation/deactivation of airspace via the applications of ASM/ATFCM Procedure 3 contributes to the achievement of an *acceptable level of safety* in the operating environment within which it is implemented. This claim is made within the context that, the operational environment is defined (**C0001**) and subject to any stated identified issues, assumptions, caveats and limitations (**C0002**).

3.2.1 Safety Criteria

The acceptable level of safety claimed in **Arg 0** is defined by the safety criteria in **Cr0001,** which covers the two criteria as listed below:

- **Relative** – risk to be no higher than existed prior to the introduction of ASM/ATFCM Procedure 3, and;
- **Minimal** – risk to be reduced As Far As Reasonably Practicable (AFARP).

For the above to be valid, it is assumed that current equivalent arrangements for the unplanned activation of airspace are *acceptably safe* (**A0001**). Further assumptions related to the ASM/ATFCM Procedure 3 are defined in section 7.1.

3.3 Strategy for Decomposing the Safety Claim (Arg 0)

The Claim (**Arg 0**) is decomposed into five principle safety arguments as indicated in Figure 1. The decomposition of **Arg 0** is based on the Generic Argument presented in EUROCONTROLs Safety Assessment Made Easier; see [11] and [12].

The strategy for satisfying **Arg 0** is thus to derive a set of ASM/ATFCM Procedure 3 safety requirements to show that ASM/ATFCM Procedure 3 has been correctly specified (**Arg 1**), designed (**Arg 2**), implemented (**Arg 3**), safe transition to operations under the procedure (**Arg 4**) and continued safe operation (**Arg 5**) such that the safety criteria are met.

As illustrated by the shading of the arguments in Figure 1 **Arg 3, Arg 4** and **Arg 5** are outside the scope of this Preliminary Safety Case and will need to be addressed by States implementing ASM/ATFCM Procedure 3.

Arg 1 is addressed in section 4, **Arg 2** is addressed in section 5 and **Args 3**, **4** and **5** are addressed in section 6. Additional guidance material has been included throughout this report to support ANSPs in developing their own safety assessments. Guidance specifically relates to re-use of the generic safety argument, specific issues that need to be addressed in implementation, adaptation of the safety analyses to local circumstances etc.

Guidance material in the remainder of the body of this Preliminary Safety Case is highlighted as appropriate by the use of boxes as below:

> ***Guidance Material - Example***
>
> *Proposed guidance material to support ANSPs in creating their own safety assessments is provided in boxes such as this towards the end of relevant sections.*

4 SAFETY SPECIFICATION (ARG 1)

4.1 Objective

The objective of this section is to show that

- the basic idea behind ASM/ATFCM Procedure 3 is capable of satisfying the safety criteria assuming a suitable procedure design can be produced and implemented; and

- identified safety objectives are derived such that an acceptable level of safety can be achieved.

4.2 Strategy

The overall safety argument for the adequacy of the safety specification for ASM/ATFCM Procedure 3 is presented in Figure 2 below.

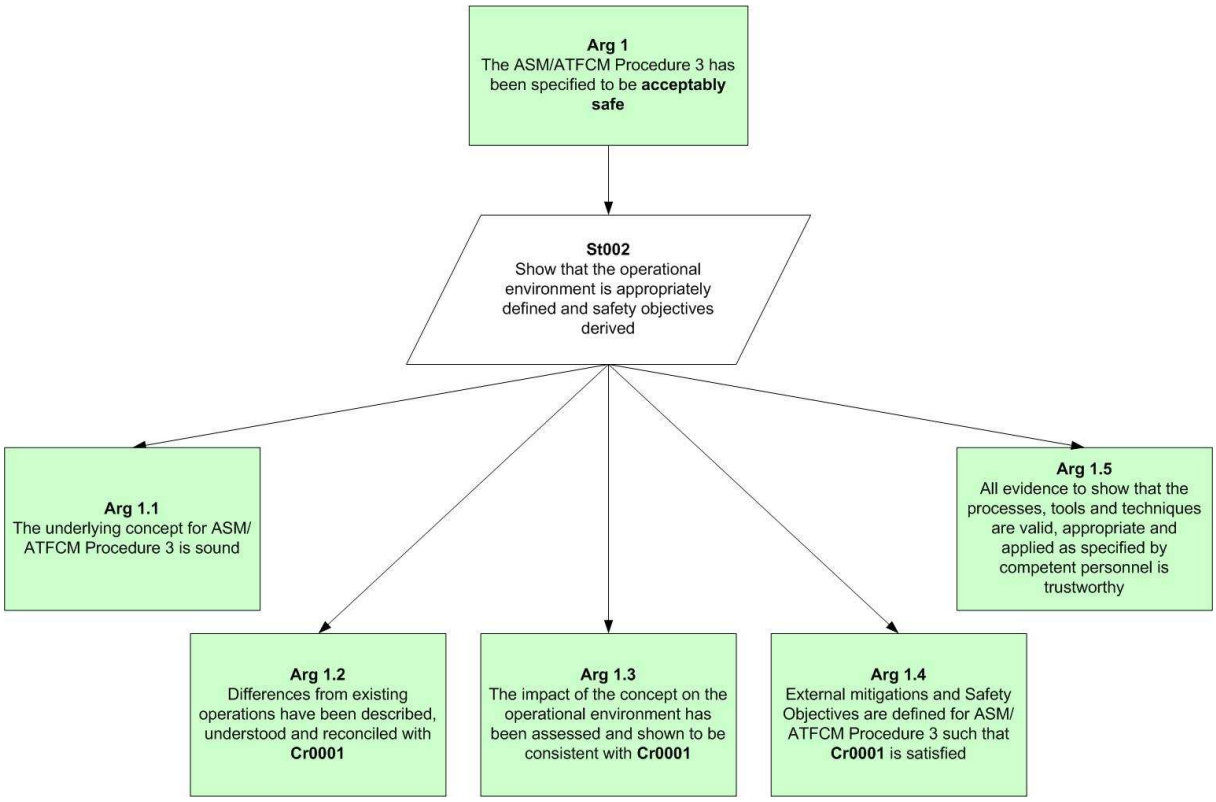


Figure 2: Safety Specification (Arg 1)

Each of the arguments outlined above are addressed in turn in the following sections and any evidence to support them or identification of the outstanding satisfaction issues discussed.

4.3 Definition of Operational Concept and Scope (Arg 1.1)

The aim of this section is to provide an overview of the operational concept and scope of the change proposed by ASM/ATFCM Procedure 3. The change is made within the context of the Flexible Use of Airspace (FUA) concept and will be implemented within the EUROCONTROL Handbook for Airspace Management [3] thus at the concept level the

proposed modification is not fundamentally changing what has previously been agreed for the handbook as a sound concept.

To better bound the context in which the generic safety assessment activity for ASM/ATFCM Procedure has been performed, a series of scoping statements have been formulated; these are presented towards the end of this section and aid in understanding the boundary of the generic safety assessment.

Guidance Material - Demonstration of Sound Concept

For local implementation States will need to demonstrate that the concept of ASM/ATFCM Procedure 3 within their own ATM operations and local arrangements is sound.

4.3.1 Flexible Use of Airspace (FUA) Concept

The basis for the FUA Concept is that airspace should no longer be designated as either military or civil airspace but should be considered as one continuum and used flexibly on a day-to-day basis. Consequently, any necessary airspace segregation should be only of a temporary nature. One of the major objectives of EATM is the more efficient use of airspace by civil and military users through the implementation of the FUA Concept. Airspace Management Cells (AMCs) will ensure that there is a more effective sharing of ECAC airspace through joint civil/military strategic planning and pre-tactical airspace allocation.

The FUA Concept has increased the flexibility of airspace use and has provided ATM with the potential to increase the capacity of the air traffic system. The FUA Concept allows the maximum joint use of airspace by appropriate civil/military co-ordination to achieve the required OAT/GAT separation. The application of the FUA Concept also ensures, through the daily allocation of flexible airspace structures, that any necessary segregation of airspace is based on real usage within a specific time period.

The three Airspace Management (ASM) Levels correspond directly with civil/military ATM co-ordination tasks, each level being related to, and impacting on, the others as outlined in the following section.

4.3.2 EUROCONTROL Handbook for Airspace Management

The EUROCONTROL Handbook for Airspace Management [3] aims to provide, under a single cover, the general ASM functions and Air Traffic Management (ATM) related procedures that are required to apply and fully exploit the Flexible Use of Airspace (FUA) Concept in the European Civil Aviation Conference (ECAC) Member States. The handbook is regarded as a set of actions intended as Recommended Practices to support the harmonisation of flexible ASM throughout the ECAC area. It is not considered a substitute for official national regulations in individual ECAC States nor for the ASM Part of the ICAO European Region Air Navigation Plan.

In 1992 the EATCHIP Task Force on Airspace Structure and Management established a first set of principles for the proper functioning of three ASM Levels; ASM/ATFCM Procedure 3 applies to ASM Level 2 and utilises ASM Level 3 functionality as follows:

- **ASM Level 1 (National and International Airspace Policy) -** Strategic ASM at Level 1 consists of joint civil and military process within a high-level civil/military national body, which formulates the national ASM policy and carries out the necessary strategic planning work, taking into account national and international airspace user requirements. In order to maintain a flexible airspace organisation, States assess and re-assess their national airspace and routes structures to determine working structures for ASM Levels 2 and 3.

- **ASM Level 2 (Day to Day Allocation of Airspace) -** Pre-Tactical ASM at Level 2 consists of the day-to-day management and temporary allocation of airspace through national or sub-regional AMCs. AMCs are joint civil/military ASM focal-points which have the authority to conduct operational ASM within the framework of the States airspace structures, priority rules and negotiation procedures as laid down by the national policy body. AMCs collect and analyse all airspace requests and decide the daily airspace allocation.

  Under ASM/ATFCM Procedure 3, route closure information at much shorter notice than is currently possible is proposed, with the dissemination of changes being promulgated by CFMU via the posting of route availability updates in the same way as is done by CFMU for e-RAD promulgation. The posting of updates will also be synchronised with publication of the relevant Aeronautical Information Message (AIM). ASM/ATFCM Procedure 3 thus provides the ability to manage ad-hoc activations such that a greater proportion of the civil flights affected are notified in advance and are required to change their flight plan prior to departure.

- **ASM Level 3 (Real-Time Use of Airspace) -** Tactical ASM at Level 3 consists of the real-time activation, deactivation or real-time reallocation of the airspace allocated at Level 2 and the resolution of specific airspace problems and/or traffic situations between civil and military ATS units and/or controllers, as appropriate. Flexibility in the use of airspace is enhanced by real-time civil/military co-ordination capability. This flexibility depends on the potential offered by the joint use of airspace by civil and military traffic.

  Under ASM/ATFCM Procedure 3 a reduced number of civil flights will be required to be manually routed around the closed route as the majority will have been notified beforehand.

4.3.3 Scoping Statements

The following scoping statements have been made to further support the generic safety assessment activity.

Reference	Scoping Statement
S0001	The high-level and detailed functional models included in Appendix B identify the 'system boundary' for the purposes of the safety assessment
S0002	The safety of ASM/ATFCM Procedure 3 will be assessed as a generic procedure independent of implementation. Individual States are responsible for assuring an overall acceptable level of safety when implementing the procedure
S0003	Operations in both controlled and uncontrolled ECAC airspace are within scope and include consideration of civil aircraft, military aircraft and military assets
S0004	The safety assessment will consider the ATM perspective i.e. requirements will only be placed at the same level as Procedure 3 e.g. ASM Level 2
S0005	Existing procedures allow two updates will be issued to the AUP i.e. UUP1 and UUP2. It is noted that rolling updates to the AUP will be implemented in the future however; consideration of rolling updates is outside the scope of this safety assessment activity

Table 2: Scoping Statements

Guidance Material - Scoping Statements

For local implementation States will need to determine the applicability of the scoping statements when undertaking local safety assessments in respect of implementation of ASM/ATFCM Procedure 3. If the scoping statements are changed then this may impact

the safety assessments particularly in the allocation of safety requirements and assumptions.

4.4 Differences from Current Operations (Arg 1.2)

Today, the latest the military can plan an airspace activation is prior to 1400 the Day before Operations; the earliest the activation can start is 0600 the following day. Therefore there is 16 hours lead time between notification and start of the activation in which affected flights can be informed of the route closure. Where it is not possible to notify a flight of an activation, such flights are managed tactically by ATC. The number of flights requiring tactical management, is initially low, and will continue to decrease over the time of the activation.

If the military identify a need for airspace activation after the notification period, then that activation is negotiated with ATC and managed tactically by ATC. The activation may be implemented immediately, therefore no flights affected by the route closure are notified and all are managed tactically by the ATC.

Under ASM/ATFCM Procedure 3 the military will have two additional opportunities to plan ad-hoc airspace activations. The first opportunity is prior to 1700 on the Day before Operations; the earliest that the activation can start is 0600 the following day. Therefore there is 13 hours lead time between notification and the start of the activation in which affected flights can be informed of the route closure.

The second opportunity is prior to 0900 on the Day of Operations; the earliest that the activation can start is 1100. Therefore there are 2 hours lead time between notification and the start of the activation in which affected flights can be informed of the route closure.

In principle ASM/ATFCM Procedure 3 is designed to reduce the amount of air traffic requiring tactical management in the execution phase of flight. The impact of each request is assessed at a network level and the final allocation of airspace is decided by the AMC taking into account the impact. In addition time limits in the procedure specify a minimum of lead time of two hours during which airspace users are notified of the route closures. During this time a significant portion of the affected flight plans will be cancelled and re-filed. Therefore the volume of traffic that the ATC is required to tactically manage for the duration of the closure will be significantly reduced potentially reducing the workload on ATC and reducing risk.

Guidance Material - Difference from Current Operations

For local implementation States will need to clearly define how their implementation of ASM/ATFCM Procedure 3 differs from current operations. This may differ from State to State depending on whether ASM/ATFCM Procedure 3 has been modified or tailored from the version developed by EUROCONTROL and documented in the EUROCONTROL ASM Handbook.

4.5 Impact on the Operational Environment (Arg 1.3)

The operational driver behind the development of ASM/ATFCM Procedure 3 is to address the ‘weaknesses in the current system where possibilities for the military to activate non-planned TRAs/TSAs on the day of operations are limited. The operational objective for introducing the procedure is that it will complement already existing procedures to optimise the use of airspace while minimising the impact of any disruptions (i.e. route closures) and therefore enable all airspace users to conduct efficient real-time operations i.e. the primary aim is to increase capacity.

The key properties of the operational environment that may be affected by the implementation of ASM/ATFCM Procedure 3 are described below.

- **Airspace Boundary**: ASM/ATFCM Procedure 3 is available to be implemented by all ECAC States, therefore the boundary of the airspace is the boundary of ECAC States airspace.

- **Types of Airspace**: ASM/ATFCM Procedure 3 concerns temporary airspace activations or restricted areas which can occur in both controlled and uncontrolled airspace.

- **Airspace Structures**: An airspace activation may typically result in the closure of ATS routes and/or CDR1.

- **Types of Airspace Users**: The airspace users affected by ad-hoc activation of TRA/TSA are the military (who request and use the activation area) and civil AO and other civil users (who need to be aware of the activation and re-route any affected flight plan around the area).

- **Types of Traffic**: Within the activation area the military may deploy aircraft or other assets e.g. missiles. The civil aircraft affected are general air traffic (GAT).

- **Phase of Flight**: Ad-hoc activations of TRA/TSA will affect civil flights in both the planning phase and execution the execution phase. Affected flights in the planning phase need to be identified, their flight plan suspended and a new flight plan filed. Flights in the execution phase need to be identified and re-routed tactically.

- **ATM Procedures**: “Ad-hoc” in terms of this procedure means that the need for the activation is identified after the AUP has been published. The procedure will utilise the existing UUP1 and UUP2 process to manage the change.

- **ATM Tools**: The procedure will rely on the ENV database and IFPS to identify and suspend/cancel flight plans affected by the activation.

- **Aeronautical Information**: An additional AIM will be published to provide information on the changes to route availability to airspace users.

- **Legislative Status**: ASM/ATFCM Procedure 3 is planned to be incorporated into the EUROCONTROL Handbook for Airspace Management. The ASM Handbook is a set of recommended practices to support the harmonisation of flexible ASM throughout the ECAC area. It is not a substitute for national regulations in individual ECAC states or for the ASM part of the ICAO European Region Air Navigation Plan.

With respect to risk, there is the potential for ASM/ATFCM Procedure 3 to increase the number of aircraft requiring tactical management in the execution phase, specifically in the case of short notice activations where flight plans of affected flights cannot be changed in time. This potential risk increase is explored further as part of the detailed safety assessment activities.

Guidance Material - Impact on Local Operational Environment

For local implementation States will need to determine the impact on their operating environment based on their tailoring of ASM/ATFCM Procedure 3.

4.6 Satisfying the Safety Criteria (Arg 1.4)

In order to understand the risks associated with implementation of ASM/ATFCM Procedure 3 a Functional Hazard Assessment (FHA) activity has been performed as documented in the Safety Assessment Report for ASM/ATFCM Procedure 3 [2]. This involved the identification of hazards at the boundary of ASM/ATFCM Procedure 3 followed by an analysis of the consequences of those hazards. Based on the results a series of Safety Objectives were then defined for ASM/ATFCM Procedure 3. The following sections summarise these activities.

Guidance Material - Local ASM/ATFCM Procedure 3 Safety Assessment

For local implementation States will need to review the detailed generic safety analyses documented within the Safety Assessment Report for ASM/ATFCM Procedure 3 [2] to tailor the results to local operations and conditions as explained in the Functional Hazard Assessment (FHA) and Preliminary System Safety Assessment (PSSA) guidance material boxes.

4.6.1 Functional Hazard Assessment (FHA)

Ebeni Limited undertook an independent Functional Failure Analysis (FFA) activity, documented in [2], which provided and independent assessment of the hazards and potential consequences of those hazards in relation to ASM/ATFCM Procedure 3. In order to identify hazards each of the primary safety functions related to ATM operations under ASM/ATFCM Procedure 3 was considered based on the model presented in Appendix B.1. The primary safety functions considered were:

- **Safety Function 1**. *Request a change to the airspace structure*.
- **Safety Function 2**. *Reorganise the airspace structures taking into account demand and capacity*.
- **Safety Function 3**. *New structure implemented and disseminated*.
- **Safety Function 4**. *Notification*.
- **Safety Function 5**. *Flight plan checking and re-filing*.
- **Safety Function 6**. *Flights re-routed*[2].

The functional failure guidewords applied to each of the above functions were:

- **Loss** – complete negation of an intention. No part of the intention is achieved and nothing else happens.
- **Error** – any action that is undesirable regardless of cause, e.g. incorrect response to instruction, partial response to instruction or unintentional actions.
- **Intentional Deviation** – a different action than that intended occurs as a result of a deliberate external input.
- **Too early** – an action occurs earlier than expected either relative to Coordinated

[2] Whilst his function is outside ASM/ATFCM Procedure 3, it is included in the model because ASM/ATFCM Procedure 3 impacts the frequency of this function.

Universal Time (UTC) or sequence e.g. military given confirmation of activation before the change is agreed and implemented in the ENV database.

- **Too late** – an action occurs later than expected either relative to UTC or sequence e.g. ENV database is supposed to be updated 2 hours before UUP2 becomes valid, but is updated only 1 hour before UUP2 becomes valid.

- **Too many** – a greater number or value than intended occurs as a result of an action e.g. too many requests for TRA/TSA, too many flights affected by a route closure, too many updates required to be processed in the ENV database.

- **Too few** – a lesser number or value than intended occurs as a result of an action e.g. not all update requests processed in the ENV database.

- **Other** – completeness check, i.e. anything not covered by the guidewords above.

4.6.2 Hazard Identification

The Safety Assessment Report for ASM/ATFCM Procedure 3 [2] documents the detailed approach to the identification of hazards. Two hazards were identified that fall within the defined scope of the generic safety assessments as follows:

- **HAZ001** – Activation request granted which brings one or more aircraft into an active area

- **HAZ002** – Military aircraft/asset operating in an area that Civil ATC are not aware has been activated or operating in an inactive area without Military ATC being aware

The hazards are defined at the boundary of ASM/ATFCM Procedure 3 and reflect the functional failure scenarios that could potentially lead to hazardous situations. Both hazards identified are common to the ***with*** ASM/ATFCM Procedure 3 and ***without*** ASM/ATFCM Procedure 3 situations; however it was identified that the frequency of the hazard occurring would change by the implementation of ASM/ATFCM Procedure 3; more specifically the implementation of ASM/ATFCM Procedure 3 may result in an increase in the tactical management of aircraft.

The potential impact of this may be significant as although the tactical management of aircraft is an activity performed daily by ATC, it has the potential to lead to other safety events including downstream sector overloading, low fuel loads potentially leading to aircraft fuel emergencies, longer flight times or flights being re-directed to different locations. The implementation of ASM/ATFCM Procedure 3 may lead to an increase in occurrence of these safety events. This is assessed further within the Preliminary System Safety Assessment (PSSA) activity outlined in section 5.

Guidance Material - Hazard Identification

For local implementation States may need to revisit the hazard identification documented within the Safety Assessment Report for ASM/ATFCM Procedure 3 [2] if local arrangements, operations and conditions introduce further differences than those described in section 4.4 or additional functionality to the procedure than as specified in the FHA functional model.

4.6.3 Consequence Analysis

A consequence analysis was undertaken as documented in [2] to assess the consequences associated with each hazard for both the ***with*** and ***without*** ASM/ATFCM Procedure 3

situations. The generic safety assessment considered the hazards to the point where there is the potential for an accident. Appendix D of the Safety Assessment Report for ASM/ATFCM Procedure 3 [2] presents the qualitative severity classification scheme used in the generic safety assessment. The consequence analysis conclusions for each of the hazards is summarised as follows:

- **HAZ001** - the worse case consequence is that the civil aircraft continues to fly the flight plan with a total loss of ATC potentially breaching the active area thus resulting in a Severity Classification 2 outcome.

  The consequences of **HAZ001** are considered the same both ***with*** and ***without*** ASM/ATFCM Procedure 3; the mitigations for **HAZ001** are applied in the same way for both the ***with*** and ***without*** ASM/ATFCM Procedure 3 with each mitigation having the same probability of success.

- **HAZ002** - the worse case consequence is that the civil aircraft continues to fly the flight plan with a total loss of ATC which may have the potential to conflict with the flight path of the military aircraft/asset thus resulting in a Severity Classification 2 outcome.

  The consequences of **HAZ002** are the same both ***with*** and ***without*** ASM/ATFCM Procedure 3; the mitigations for **HAZ002** are applied in the same way for both the ***with*** and ***without*** ASM/ATFCM Procedure 3 with each mitigation having the same probability of success.

Guidance Material - Consequence Analysis

For local implementation States will need to revisit the consequence analysis mitigations documented in the Safety Assessment Report for ASM/ATFCM Procedure 3 [2] if additional hazards have been identified. States should verify the conclusion of the consequence analysis that the mitigations are the same ***with*** and ***without*** ASM/ATFCM Procedure 3 when taking into account local arrangements, operations and conditions.

4.6.4 Safety Objectives

Safety objectives have been derived from the safety criteria which in this case are relative, i.e. not based on an absolute Target Level of Safety (TLS). The FHA activities did not identify any unique hazards as a result of the implementation of ASM/ATFCM Procedure 3, therefore the safety objectives are based on ensuring that the safety criteria are achieved, i.e. that the risks to other airspace users is:

- no higher than existed prior to the introduction of ASM/ATFCM Procedure 3, and

- reduced As Far As Reasonably Practicable (AFARP).

Consequently, the safety objective for each hazard must be no greater following implementation of ASM/ATFCM Procedure 3 than currently exists today and where practicable the risks should be further reduced. Therefore two ASM/ATFCM Procedure 3 Safety Objectives have been defined:

Ref.	Safety Objective
SO001	The frequency of granting an activation request which exceeds the forecast ATC capacity shall be no greater than exists in the current situation and where practicable further reduced.

Ref.	Safety Objective
SO002	The frequency of a military aircraft/asset being airborne in an area that Civil or Military ATC is not aware has been activated shall be no greater than exists in the current situation and where practicable further reduced.

Table 3: ASM/ATFCM Procedure 3 Safety Objectives

Guidance Material - Safety Objectives

Once local Functional Hazard Assessment (FHA) activities have been completed, specifically hazard identification and consequence analysis specific to each States implementation of ASM/ATFCM Procedure 3, relevant Safety Objectives should be defined.

4.7 Safety Process Validation and Verification (Arg 1.5)

Fundamental to assuring the safety of ASM/ATFCM Procedure 3 is to demonstrate that a trustworthy process has been followed by competent people and therefore all evidence relating to this PSC is trustworthy.

The safety requirements derived for ASM/ATFCM Procedure 3 documented within this PSC were derived from an ESARR 4 [3] compliant relative safety assessment. The EUROCONTROL Safety Assessment Methodology [10] was used as a guide to compliance with ESARR 4 [3].

The ASM/ATFCM Procedure 3 assessment has been undertaken independently from EUROCONTROL by individuals experienced in the field of safety engineering with extensive knowledge in ATM safety; with reviews from EUROCONTROL as appropriate, to ensure that all evidence relating to processes, tools and techniques within this PSC is trustworthy.

Guidance Material - Safety Process Validation and Verification

For local implementation States will need to document arguments, supported by evidence that local safety assessments have followed a trustworthy process and have been performed by competent personnel.

4.8 Conclusions on Arg 1

This section of the Preliminary Safety Case for ASM/ATFCM Procedure 3 has shown through argument and supporting evidence that, the underlying concept for ASM/ATFCM Procedure 3 is sound (**Arg 1.1**), the differences from existing operations have been described, understood and reconciled with **Cr0001** (**Arg 1.2**), the impact of the concept on the operational environment has been assessed and shown to be consistent with **Cr0001** (**Arg 1.3**), external mitigations and safety objectives are defined for ASM/ATFCM Procedure 3 such that **Cr0001** is satisfied (**Arg 1.4**) and all evidence to show that the processes, tools and techniques are valid, appropriate and applied as specified by competent personnel is trustworthy (**Arg 1.5**); thus **Arg 1** has been satisfied for a generic application of ASM/ATFCM Procedure 3.

5 DESIGN SPECIFICATION (ARG 2)

5.1 Objective

The objective of this section is to show that all elements (e.g. people, procedures, equipment etc.) of the procedure design for ASM/ATFCM Procedure 3:

- have been identified and function completely, correctly and coherently under all normal and abnormal external operational conditions and demands from the ATM environment including failures of external adjacent elements
- all risks from internal procedure failure have been sufficiently mitigated
- all identified external mitigations and safety requirements are implementable
- the process for assuring Arg 2 is trustworthy.

5.2 Strategy

Figure 3 below shows the overall argument structure for **Arg 2**:

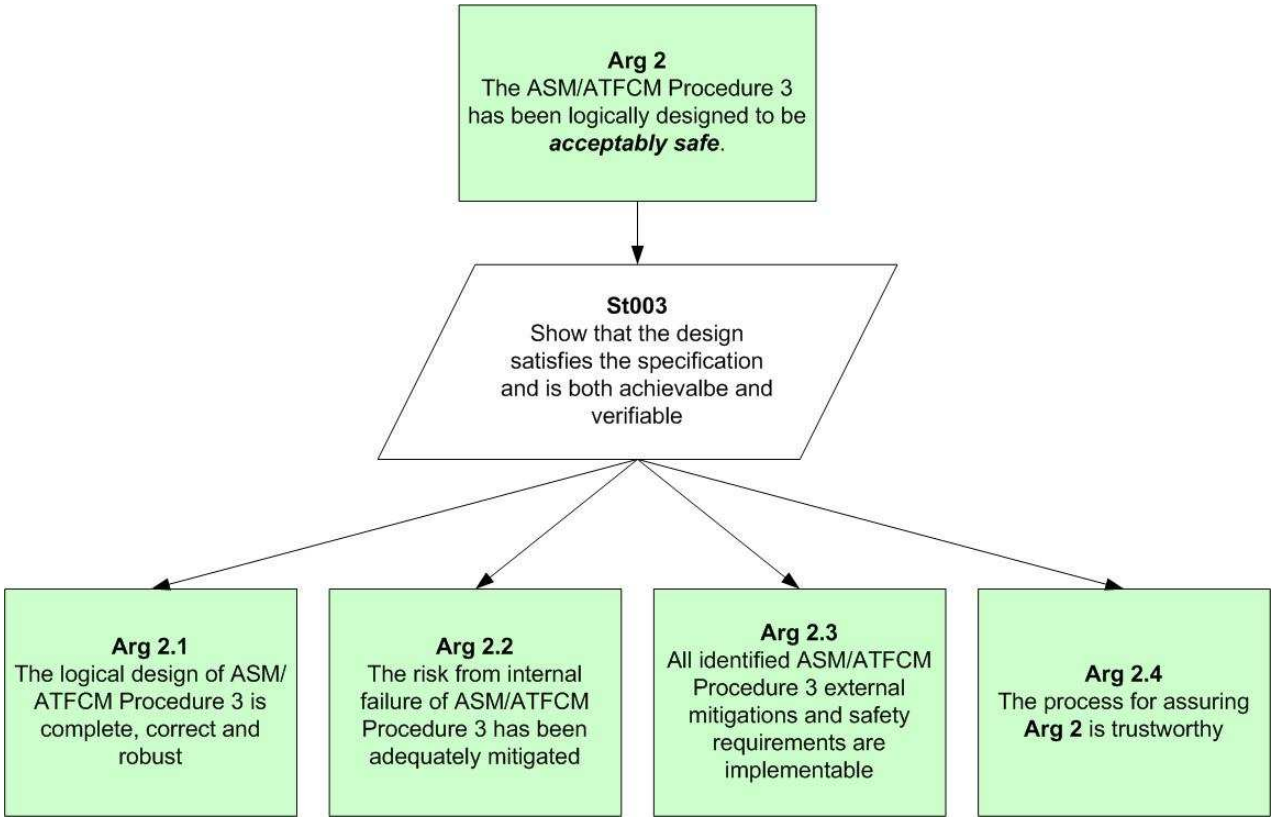


Figure 3: Design Specification (Arg 2)

Each of the arguments outlined above are addressed in turn in the following sections and any evidence to support them or identification of the outstanding satisfaction issues discussed.

5.3 ASM/ATFCM Procedure 3 Logical Design (Arg 2.1)

The aim of this section is to present the arguments and supporting evidence for the completeness, correctness and robustness of the logical design for ASM/ATFCM Procedure 3 via the undertaking of a Preliminary System Safety Assessment (PSSA) activity. The following sections summarise the detailed design analysis activities that have been undertaken in order to satisfy **Arg 2.1**.

5.3.1 Completeness of Logical Design

A logical design represents a high-level, architectural representation of a system or procedure that is entirely independent of the physical implementation of that design. The logical design is depicted within a Logical Model (LM) that describes the main logical elements and the interactions between them including; human tasks, machine-based functions and airspace structures. The model also explains what each of those "actors" provides in terms of functionality and performance.

The ASM/ATFCM Procedure 3 logical identifies all such logical elements for the procedure, associated environment and interactions between logical elements as presented in Appendix B.2

A second Logical Interaction Model for ASM/ATFCM Procedure 3 is presented in Appendix B.3 and identifies in more detail the specific interactions between Stakeholders. More specifically the model demonstrates how the key safety functions are fulfilled i.e.:

- using the UUP1 and UUP2 process to provide two additional opportunities for the military to request airspace activations on the day before (for UUP1) or the day of (for UUP2) operations

- providing a timeline and framework for AMCs, FMPs and CFMU to assess the impact of the request

- using the existing tools of the ENV database and IFPS to suspend / cancel the flight plans for affected flights where possible.

Both the models were developed based on information provided within the EUROCNTROL Handbook for Airspace Management and the Draft ASM/ATFCM Procedure 3 itself. The models were presented and validated by a team of experts at the ASM/ATFCM Procedure 3 Safety Assessment Workshop [9].

Guidance Material - Logical Design Representation & Analysis

For local implementation States should verify the logical design representations of their ASM/ATFCM Procedure 3 implementation. If different then States will need to perform the relevant Preliminary System Safety Assessment (PSSA) activities. The detailed design analysis (performed by States) may or may not include the safety analysis activities outlined within this section of the Preliminary Safety Case e.g. logical interaction analysis, task analysis, causal analysis etc. however evidence of having followed a robust safety process resulting in a thorough assessment is required.

5.3.2 Logical Design Analysis

In order to demonstrate design correctness and robustness the actions of and interactions between each logical element within the logical models were analysed to identify the necessary logical system behaviour required to ensure the safety of the system under

consideration i.e. ASM/ATFCM Procedure 3, and thus derive safety requirements or assumptions as appropriate.

The logical design analysis documented within the Safety Assessment Report for ASM/ATFCM Procedure 3 [2] identified 21 Functional Safety Requirements (FSR) (**FSR001** - **FSR005**, **FSR012** - **FSR018**, **FSR022** - **FSR026** and **FSR034** - **FSR037**) which are presented in Appendix D.1 along with 3 External Functional Safety Requirements (EFSRs) (**EFSR001** - **EFSR003**) which are presented in Appendix D.3 .

5.3.3 Task Analysis

Based on the guidance provided within the EUROCONTROL Safety Assessment of ATM Procedures (SAAP) [5], a task analysis was performed to identify potential deviations from successful completion of ASM/ATFCM Procedure 3.

Each task e.g. step within the Draft ASM/ATFCM Procedure 3, is reviewed against 'normal' operating scenarios 'abnormal' conditions with the aim to find and correct all the deficiencies in the design. Operational scenarios were defined that demonstrate 'normal' and 'abnormal' conditions as outlined in Appendix H of [2].

The task analysis identified an additional 13 Functional Safety Requirements (**FSR006** – **FSR011**, **FSR019** – **FSR021** and **FSR027** – **FSR030**).

5.4 Mitigation from Internal Failure (Arg 2.2)

In order to model the internal failures of ASM/ATFCM Procedure 3, fault trees have been constructed using Fault Tree Analysis (FTA) based on the results of the Safety Assessment Workshop as detailed in [9]. The completed causal analysis results are presented in Appendix H of the Safety Assessment Report for ASM/ATFCM Procedure 3 [2] a summary of which is provided in the following section.

5.4.1 Causal Analysis

The focus of the causal analysis is to determine how failure of the procedure could lead to one of the identified hazards. The causes of the hazards occurring in the without ASM/ATFCM were not analysed as they are independent from ASM/ATFCM Procedure 3.

The Fault Tree Analysis focuses on the primary contributors to the failure sequences based on the results of the Safety Assessment Workshop [9]. Although more obscure scenarios could be developed, the complexity of the failure mode(s) would be such that the likelihood of occurrence would be insignificant when compared to the primary causes. Based on the results of the causal analysis the following conclusions have been drawn with regards primary mitigation for the causes of each hazard:

- **HAZ001** - The successful Network Impact Assessment is the key mitigation to preventing the number of flights requiring tactical management exceeding the ATC capacity.

- **HAZ002** - Clear communication and the provision of consistent information is the key mitigation to prevent military assets being airborne without Civil ATC being aware of the airspace activation.

The completed causal analysis results are shown in Appendix I of the ASM/ATFCM Procedure 3 Safety Assessment Report [2]. This analysis identified one additional External Functional Safety Requirement (**EFSR004**) and two Safety Monitoring Requirements (**SRM001** and **SMR002**). A complete list of ASM/ATFCM Procedure 3 safety requirements are presented in Appendix D.

5.5 Safety Requirements Specification and Achievability (Arg 2.3)

This sub-argument refers to the safety requirements defined for ASM/ATFCM Procedure 3 and the need to ensure that the safety requirements and mitigations are capable of being satisfied in a typical implementation in hardware, software, people and procedures as appropriate for ATM operations under ASM/ATFCM Procedure 3.

The purpose of the generic safety assessment was to derive a set of safety requirements such that, if satisfied, an acceptable level of safety can be demonstrated. The safety requirements documented in this Preliminary Safety Case consider all the tasks and logical element relationships that relate to ASM/ATFCM Procedure 3. Evidence for satisfaction of the requirements and validation of assumptions should be provided as part of the ASM/ATFCM Procedure 3 Preliminary Safety Case and subsequent implementation.

5.5.1 Safety Requirements Summary

Safety requirements have been derived from the detailed design analysis documented in the Safety Assessment Report for ASM/ATFCM Procedure 3 [2] and categorised as appropriate.

Guidance Material - Safety Requirements

Based on the results of local detailed design analysis activities of ASM/ATFCM Procedure 3, appropriate safety requirements should be derived. The safety requirements documented in Appendix D are generic and can be used as a starting point, however, should be assessed in light of States local implementation of ASM/ATFCM Procedure 3.

The safety requirements presented in Appendix D are derived from the following sources and are subject to the resolution of any outstanding safety issues:

- **Functional Safety Requirements (FSR)** - derived from the logical design analysis and task analysis as described in section 5.3.2; see Appendix D.1

- **External Functional Safety Requirements (EFSR)** - derived from the logical design analysis and the causal analysis described in sections 5.3.2 and 5.4.1; see Appendix D.3 EFSRs have been placed on Stakeholders external to ASM/ATFCM Procedure 3 and are thus outside the scope of the generic safety assessment.

- **Safety Monitoring Requirements (SMR)** - derived from the causal analysis as described in section 5.4.1; see Appendix D.4

- **Safety Integrity Requirements (SIR)** - a Procedure Assurance Level (PAL) has been derived from the cause/consequence analyses and guidance provided in the EUROCONTROL Safety Assessment Methodology [10].

  The safety integrity requirements were determined by examining the base events of the Fault Tree that fall within the boundary of the analysis (shown in Appendix I of [2]). Since the design is implemented entirely within a procedure then the only SIR required is a Procedure Assurance Level; see Appendix D.5 .

Guidance Material - Safety Integrity Requirements Satisfaction

For local implementation States will need to ensure satisfaction of the Procedural Assurance Level Requirement documented in Appendix D.5 . The EUROCONTROL Safety Assessment of ATM Procedures (SAAP) [5] document provides guidance on how to satisfy such a requirement.

5.5.2 Safety Requirements Achievability

A summary of all safety requirements is presented Appendix D along with traceability to the required step in ASM/ATFCM Procedure 3 where relevant. Tracing of the safety requirements into ASM/ATFCM Procedure 3 provides adequate evidence of achievability. Where ASM/ATFCM Procedure 3 does not fully address the FSR the procedure must be updated accordingly, see **Safety Issue SI001.**

A structured workshop was undertaken as part of the ASM/ATFCM Procedure 3 generic safety assessment facilitated by experienced safety engineers. The workshop included attendees from a number of ECAC States from within the AMC, Military and ATC domains; attendees from EUROCONTROL included ASM, CFMU and AIS/AIM, all of whom have reviewed and agreed the Draft ASM/ATFCM Procedure 3 presented in Appendix C. During the workshop, the minutes of which are documented in [9], when specifically questioned, no concerns with regards achievability of the safety requirements were highlighted.

Guidance Material - Safety Requirements Achievability Traceability

For local implementation States will need to ensure that any local instantiation of ASM/ATFCM Procedure 3 adequately reflects the safety requirements derived from the detailed design analysis activities.

5.6 Safety Assessment Process (Arg 2.4)

Fundamental to assuring the safety of ASM/ATFCM Procedure 3 is to demonstrate that a trustworthy process has been followed by competent people.

The generic safety assessment in support of ASM/ATFCM Procedure 3 is based on the Safety Assessment Methodology and the Safety Assessment Made Easier approaches documented in [11] and [12] respectively. The generic safety assessment has also adopted the guidance provided within the EUROCONTROL Safety Assessment of ATM Procedures (SAAP) [5].

The safety requirements derived for ASM/ATFCM Procedure 3 documented within this Preliminary Safety Case were derived from an ESARR 4 [3] compliant relative safety assessment i.e. using a qualitative comparison of the risk ***with*** and ***without*** ASM/ATFCM Procedure 3. The EUROCONTROL Safety Assessment Methodology [10] was adopted as a guide to compliance with ESARR 4 [3], see Appendix A for further details.

The generic safety assessment for ASM/ATFCM Procedure 3 has been undertaken independently from EUROCONTROL by individuals experienced in the field of safety engineering with extensive knowledge in ATM safety.

Guidance Material - Safety Process Validation and Verification

For local implementation States will need to document arguments, supported by evidence that local safety assessments have followed a trustworthy process and have been performed by competent personnel.

5.7 Conclusions for Arg 2

This section of the Preliminary Safety Case for ASM/ATFCM Procedure 3 has shown though argument and support evidence that, the logical design of ASM/ATFCM Procedure 3 is complete, correct and robust (**Arg 2.1**), the risk from internal failure of ASM/ATFCM Procedure 3 has been adequately mitigated (**Arg 2.2**), all identified ASM/ATFCM Procedure

3 external mitigations and safety requirements are implementable (**Arg 2.3**) and that the process for assuring **Arg 2** is trustworthy (**Arg 2.4**); thus **Arg 2** is satisfied for a generic application of ASM/ATFCM Procedure 3 subject to the resolution of **Safety Issue SI001**.

6 IMPLEMENTATION, TRANSITION AND ON-GOING OPERATIONS

6.1 State Implementation (Arg 3)

The implementation of ASM/ATFCM Procedure 3 will be the responsibility of individual ECAC States. However, whilst performing the generic safety assessment as documented in the Safety Assessment Report for ASM/ATFCM Procedure 3 [2] a series of External Functional Safety Requirements (EFSR) have been derived. These safety requirements should be demonstrated as being satisfied by States implementing/incorporating ASM/ATFCM Procedure 3 into their daily operations, see **Recommendation R001**. Each of the EFSRs are presented in Appendix D.3

Guidance Material - External Functional Safety Requirements

The tactical re-routing of flights for which the appropriate flight plans could not be changed in time was highlighted as a concern within the November Live Trail Report [1], during the Safety Assessment Workshop [9] and within the analysis documented in [2]. Consequences of this can include downstream sector overloading, low fuel loads potentially leading to aircraft fuel emergencies, longer flight times or flights being re-directed to different locations.

EFSR004 requires that: *States shall consider the impact of an increased frequency of TRA/TSA requests and the associated time needed to process such requests given local traffic densities in the implementation/tailoring of ASM/ATFCM Procedure 3*

EFSR004 has been identified as requiring satisfaction by States to ensure that the minimum time frame for activation of airspace based on local conditions and also the specification of the maximum tolerable frequency of activation requests is determined. This will reduce the likelihood that the number of aircraft requiring tactical re-routing exceeds the capacity of the ATC and is essential to assuring the safety objectives are satisfied.

6.2 Transition to ATM Operations (Arg 4)

In addition to States needing to demonstrate safe implementation of ASM/ATFCM Procedure 3, **Arg 4** requires evidence that all preparations for the transition to operational service have been completed by individual States who intend to implement ASM/ATFCM Procedure 3. “Transition” must be interpreted as including the safety of each stage of a phased implementation of changes specifically in relation to ensuring the continued satisfaction of the safety criteria. As with the implementation of ASM/ATFCM Procedure 3, the responsibility for this argument lies with the individual States who intend to implement Procedure 3.

6.3 Continued Safety of ATM Operations (Arg 5)

The argument for continued safe operation is the responsibility of implementing States. A programme of safety monitoring and improvement ensuring that all appropriate safety measures are in place will be fundamental to demonstrating the continued safe operation of ASM/ATFCM Procedure 3 and its continued satisfaction of the safety criteria.

However, the following Safety Monitoring Requirements (SMR) have been identified during the generic safety assessment as documented in [2] and are the responsibility of EUROCONTROL, see **Recommendation R002**.

Ref.	Safety Monitoring Requirement
SMR001	EUROCONTROL shall monitor the frequency of inconsistencies between AIM messages and associated UUPs
SMR002	EUROCONTROL shall ensure that the increased number of TRA/TRA requests as a result of ASM/ATFCM Procedure 3 does not increase the frequency of which CFMU fail to update the ENV database in time

Table 4: ASM/ATFCM Procedure 3 Safety Monitoring Requirements

7 ASSUMPTIONS, ISSUES AND LIMITATIONS

The following caveats apply to the analysis summarised within this Preliminary Safety Case and need to be considered in the context of this overall conclusions presented in section 8.

7.1 Assumptions

The following assumptions have been made during the generic safety assessment activity.

Ref.	Assumption	Validation
A0001	Current operations without the implementation of ASM/ATFCM Procedure 3 are considered tolerably safe.	This assumption was validated as reasonable at the Safety Assessment Workshop, see [9]
A0002	CFMU will update the ENV database on receipt of the UUP in a timely manner.	In accordance with the ATFCM Users Manual [13]
A0003	Civil Airspace Users are informed of CDR closures via the Conditional Route Availability Message (CRAM) and are also available via the NOP Portal.	In accordance with the ATFCM Users Manual [13]
A0004	The Conditional Route Availability Message (CRAM) is available on the CFMU NOP Portal in HTML format and a hardcopy is also sent to all registered addresses in ADEXP format via the AFTN Network.	In accordance with the ATFCM Users Manual [13]
A0005	CFMU process all Flight Plans submitted to the Initial Flight Plan Processing System (IFPS).	In accordance with the IFPS Users Manual [14]
A0006	CDR Closure and Route Availability information is promulgated by CFMU via the Conditional Route Availability Message (CRAM) once a day. Further changes will be disseminated via AIM. It is noted that an additional method of information dissemination, an eAMI, is planned to be implemented in the future however; consideration of eAMI messages are outside the scope of this safety assessment activity	In accordance with the ATFCM Users Manual [13]
A0007	The IFPS checks and cancels or suspends affected flight plans (as specified in Commission Regulation (EC) No 1033/2006 or in Integrated Initial Flight Plan Processing System.	In accordance with the IFPS Users Manual [14]
A0008	CFMU take appropriate measures to ensure that the AIM correctly represents information in the UUP prior to promulgation.	In accordance with the ATFCM Users Manual [13]

Table 5: ASM/ATFCM Procedure 3 Assumptions

Guidance Material - Assumptions

For local implementation States will need to document all assumptions made whilst performing local safety assessments including documenting the support evidence for their validation.

7.2 Safety Issues

The following safety issues were identified during the generic safety assessment activities. All of the safety issues below require further discussion and resolution.

Ref	Issue	Resolution	Status
SI001	Safety requirements traceability has identified 12 Functional safety Requirements that do not currently trace to ASM/ATFCM Procedure 3	The 11 Functional Safety Requirements listed in Appendix D for which there is no traceability should be included within ASM/ATFCM Procedure 3	**CLOSED**

Table 6: ASM/ATFCM Procedure 3 Safety Issue

Guidance Material - Safety Issues

For local implementation States will need to document and close any safety issues identified whilst performing any safety assessment activities.

7.3 Limitations

No specific limitations have been identified as part of the generic safety assessment activity for ASM/ATFCM Procedure 3.

Guidance Material - Limitations

For local implementation States will need to document any limitations on the application of ASM/ATFCM Procedure 3 that have been identified whilst performing any safety assessment activities.

8 CONCLUSION AND RECOMMENDATIONS

8.1 Summary

The aim of this Preliminary Safety Case has been to present and summarise the evidence to support the top level claim that the activation/deactivation of airspace via application of ASM/ATFCM Procedure 3 contributes to the achievement of an acceptable level of safety in the operating environment within which it is implemented. This claim is broken down into the following five principle safety arguments, the first two of which are addressed by this report:

- ASM/ATFCM Procedure 3 has been specified to be acceptably safe (**Arg 1**)
- ASM/ATFCM Procedure 3 has been designed to be acceptably safe (**Arg 2**)
- ASM/ATFCM Procedure 3 will be implemented completely and correctly (**Arg 3**)
- The transition towards full implementation of ASM/ATFCM Procedure 3 will be acceptably safe (**Arg 4**)
- The safety of ASM/ATFCM Procedure 3 in operation will continue to be demonstrated in operation service (**Arg 5**).

In this context, the safety criteria define what is meant by an acceptable level of safety, where risk is:

- no higher than existed previously, AND;
- reduced As Far As Reasonably Practicable (AFARP).

This Preliminary Safety Case addresses the first two safety arguments only, due to the scope of the generic safety assessment undertaken.

The consequence analysis undertaken has shown that the identified mitigations for the with and without ASM/ATFCM Procedure 3 situation are logically the same whilst the detailed design analysis has identified 34 Functional Safety Requirements (FSR), 4 External Functional Safety Requirements (EFSR), 2 Safety Monitoring Requirements (SMR) and 1 Assurance Level Requirement (ALR).

It is concluded that, subject to the identified assumptions and resolution of safety issues detailed in section 7, in light of the recommendations made in section 8.2, there is adequate evidence to support **Arg 1** and **Arg 2** i.e. that ASM/ATFCM Procedure 3 has been specified and designed to be acceptably safe.

8.2 Live Trails - November 2008

A live trial of ASM/ATFCM Procedure 3 was attempted in November 2008 during the preparation of which it became apparent that there were a number of safety concerns associated with ASM/ATFCM Procedure 3 which needed to be addressed. The key identified concerns were:

- TRA intrusions caused by application of ASM/ATFCM Procedure 3 with GAT flights about to take off or already airborne (i.e. the flight plan cannot be re-filed)

This first concern has been confirmed by the hazard analysis documented in section 4.6, which defines the how the TRA intrusions may occur and identifies appropriate mitigations to prevent them from occurring.

- Re-routing of flights for which the flight plan could not be changed in time may result in unexpected sector overloads.

  This second issue is addressed via Functional Safety Requirements (FSR) **FSR013**, to **FSR016** and External Functional Safety Requirement (EFSR) **EFSR004** (see section 6.1). Satisfaction of this requirement by both CFMU and States should reduce the likelihood that the number of aircraft requiring tactical re-routing exceeds the capacity of the ATC and is essential to assuring that the safety objectives are satisfied

8.3 Recommendations

The following recommendations have been identified during the ASM/ATFCM Procedure 3 generic safety assessment activities.

Recommendation R001 During State implementation of ASM/ATFCM Procedure 3, evidence in support of satisfaction of the External Functional Safety Requirements (EFSR) presented in section 6.1 should be documented.

Recommendation R002 EUROCONTROL should put into place the relevant safety monitoring and improvement measures in order to satisfy with the Safety Monitoring Requirements (SMR) presented in section 6.3.

Appendix A ESSAR 4 Compliance Statements

ESARR 4		Compliance Statement
Ref	**Requirement**	
4	Within the overall objective of ensuring safety, the objective of this requirement is to ensure that the risks associated with hazards in the ATM System are systematically and formally identified, assessed, and managed within safety levels, which as a minimum, meet those approved by the designated authority.	The approach satisfies the objective of ESARR4, section 4, by following a rigorous and systematic safety process. All risks associated with ASM/ATFCM Procedure 3 hazards have been identified and managed within the safety levels defined and safety requirements generated as appropriate.
5	An ATM service provider shall ensure that hazard identification as well as risk assessment and mitigation are systematically conducted for any changes to those parts of the ATM System and supporting services within his managerial control, in a manner which:	
5.1a	addresses the complete life-cycle of the constituent part of the ATM System under consideration, from initial planning and definition to post-implementation operations, maintenance and de- commissioning;	Compliant with lifecycle requirements in scope associated with safety requirement specification: other Arguments will address the other aspects
5.1b	addresses the airborne and ground components of the ATM System, through cooperation with responsible parties;	Compliant; all relevant components addressed. Cooperation with responsible parties addressed through workshops undertaken as part of FHA and PSSA activities [2]
5.1c	addresses the three different types of ATM elements (human, procedures and equipment), the interactions between these elements and the interactions between the constituent part under consideration and the remainder of the ATM System.	Compliant; human, procedures and equipment elements addressed as well as all associated interactions
5.2	The hazard identification, risk assessment and mitigation processes shall include:-	
5.2a	a determination of the scope, boundaries and interfaces of the constituent part being considered, as well as the identification of the functions that the constituent part is to perform and the environment of operations in which it is intended to operate;	Compliant; a rigorous approach has been taken to define the scope, boundaries, interfaces, functions and operational environment)
5.2b	a determination of the safety objectives to be placed on the constituent part, incorporating :- (i) an identification of ATM-related credible hazards and failure conditions, together with their combined effects, (ii) an assessment of the effects they may have on the safety of aircraft, as well as an assessment of the severity of those effects, using the severity classification scheme provided in Appendix A, and a determination of their tolerability, in terms of the hazard's maximum probability of occurrence, derived from the severity and the maximum probability of the hazard's effects, in a manner consistent with Appendix A;	Compliant with safety objectives process. Identification of all associated failure conditions and full cause/ consequence analysis using Event Tree Analysis, Fault Tree Analysis.

ESARR 4		Compliance Statement
Ref	**Requirement**	
5.2c	the derivation, as appropriate, of a risk mitigation strategy which :- (i) specifies the defences to be implemented to protect against the risk bearing hazards, (ii) includes, as necessary, the development of safety requirements potentially bearing on the constituent part under consideration, or other parts of the ATM System, or environment of operations, and (iii) presents an assurance of its feasibility and effectiveness;	Compliant; all mitigations and/or safety requirements / assumptions have been derived for the concept specification. Further work will be required to further refine analysis for implementation and further lifecycle stages.
5.2d	verification that all identified safety objectives and safety requirements have been met (i) prior to its implementation of the change, (ii) during any transition phase into operational service, (iii) during its operational life, and (iv) during any transition phase till decommissioning.	Compliant in part through identification of set of safety requirements / assumptions for the procedure.
5.3	The results, associated rationales and evidence of the risk assessment and mitigation processes, including hazard identification, shall be collated and documented in a manner which ensures:-	
5.3a	that correct and complete arguments are established to demonstrate that the constituent part under consideration, as well as the overall ATM System are, and will remain, tolerably safe including, as appropriate, specifications of any predictive, monitoring or survey techniques being used;	Compliant with argument requirements. The approach uses Goal-Structuring Notation (GSN) to help frame a logically consistent and complete argument.
5.3b	that all safety requirements related to the implementation of a change are traceable to the intended operations/functions.	Compliant; full details are provided within the ASM/ATFCM Procedure 3 document set indicating traceability.
A-1	Before the risks associated with introduction of a change to the ATM System in a given environment of operations can be assessed, a systematic identification of the hazards shall be conducted. The severity of the effects of hazards in that environment of operations shall be determined using the classification scheme shown in Figure A-1.	Compliant; full hazard identification process followed and severity classified as appropriate.
A-2	Safety objectives based on risk shall be established in terms of the hazards maximum probability of occurrence, derived both from the severity of its effect, according to Figure A-1 and from the maximum probability of the hazard's effect, according to Figure A-2.	Compliant; safety objectives established in terms of hazards maximum probability of occurrence.

Table 7: ESARR 4 Compliance Statements

Appendix B ASM/ATFCM Procedure 3 Models

B.1 ASM/ATFCM Procedure 3 High Level Functional Model

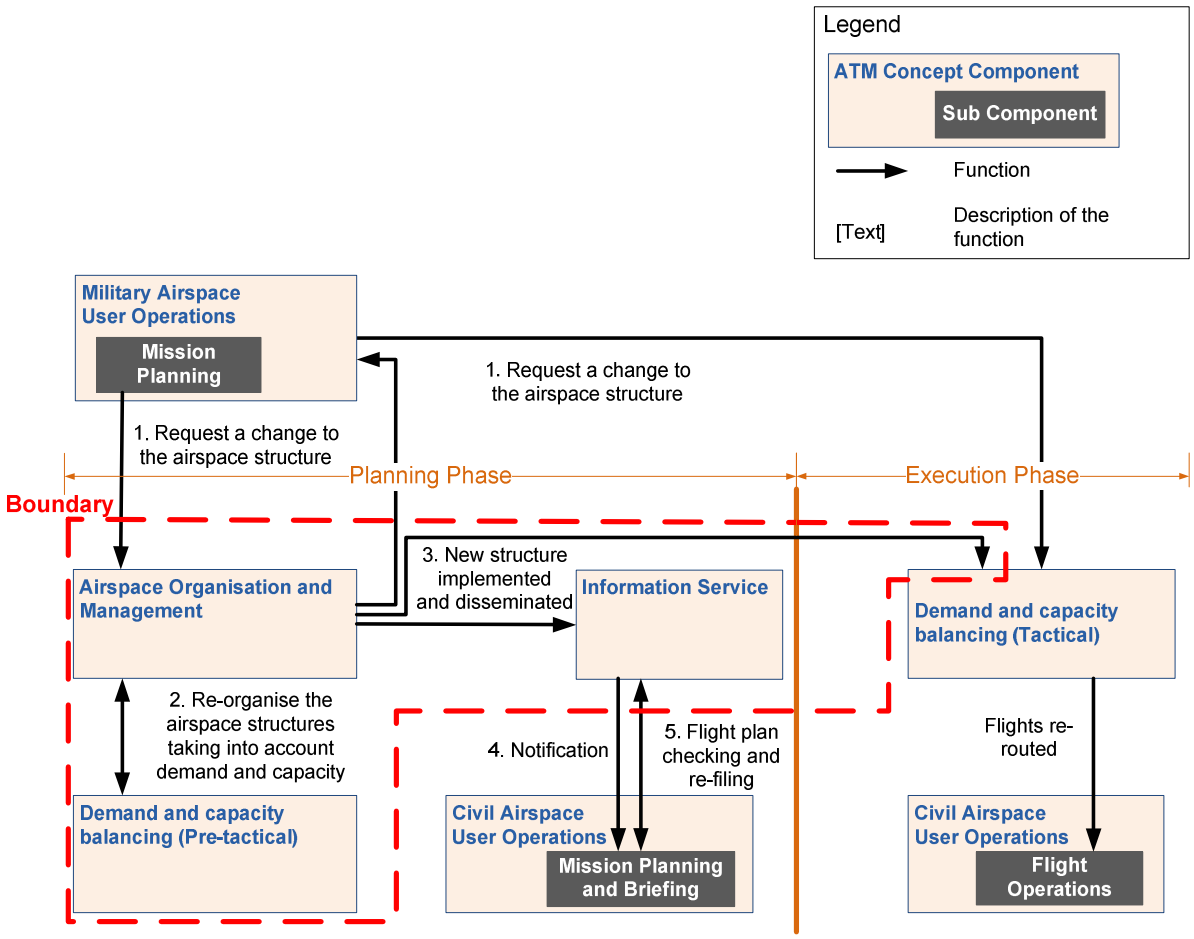


Figure 4: ASM/ATFCM Procedure 3 High Level Functional Model

The ATM Concept Components and sub-components in the model are based on the ATM Operational Concept Document [10] which is intended as a guide to the implementation of CNS/ATM technology by providing a description of how the emerging and future ATM system should operate. The functions are illustrated by the arrows between the Concept Components.

'Planning phase' refers to flights which are more than two hours EOBT and ASM level 2 functions. 'Execution phase' refers to flights which are less than two hours EOBT and ASM level 3 functions. The ASM/ATFCM Procedure 3 boundary is shown in red. Functions within the boundary are tasks/objectives within ASM/ATFCM Procedure 3. Functions which cross the boundary are inputs to or outputs from ASM/ATFCM Procedure 3. Functions outside the boundary are tasks/objectives which are independent of ASM/ATFCM Procedure 3 but may be affected by ASM/ATFCM Procedure 3 implementation (or failure to implement).

B.2 ASM/ATFCM Procedure 3 Logical Model

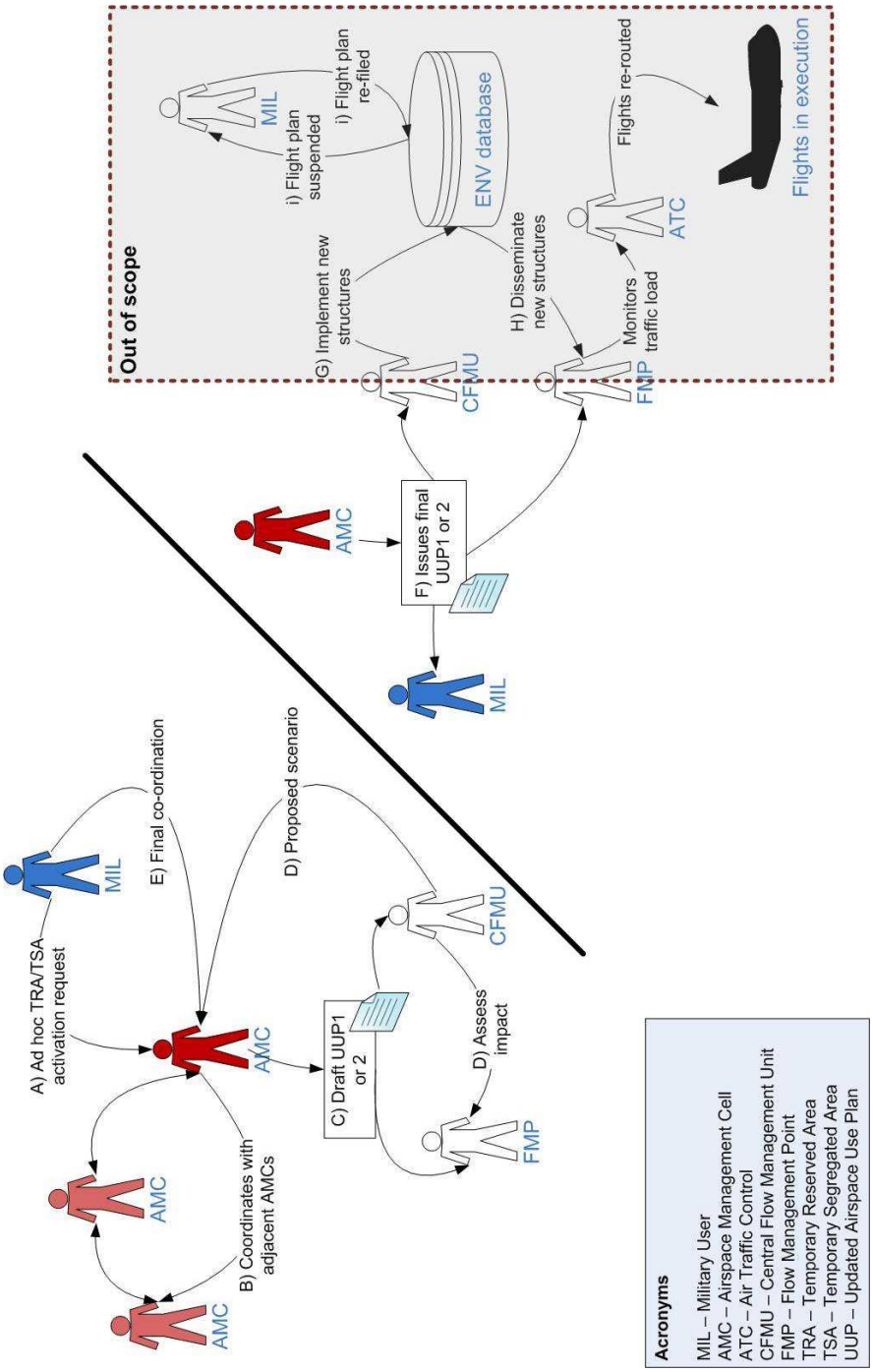


Figure 5: ASM/ATFCM Procedure 3 Logical Model

B.3 ASM/ATFCM Procedure 3 Logical Interaction Model

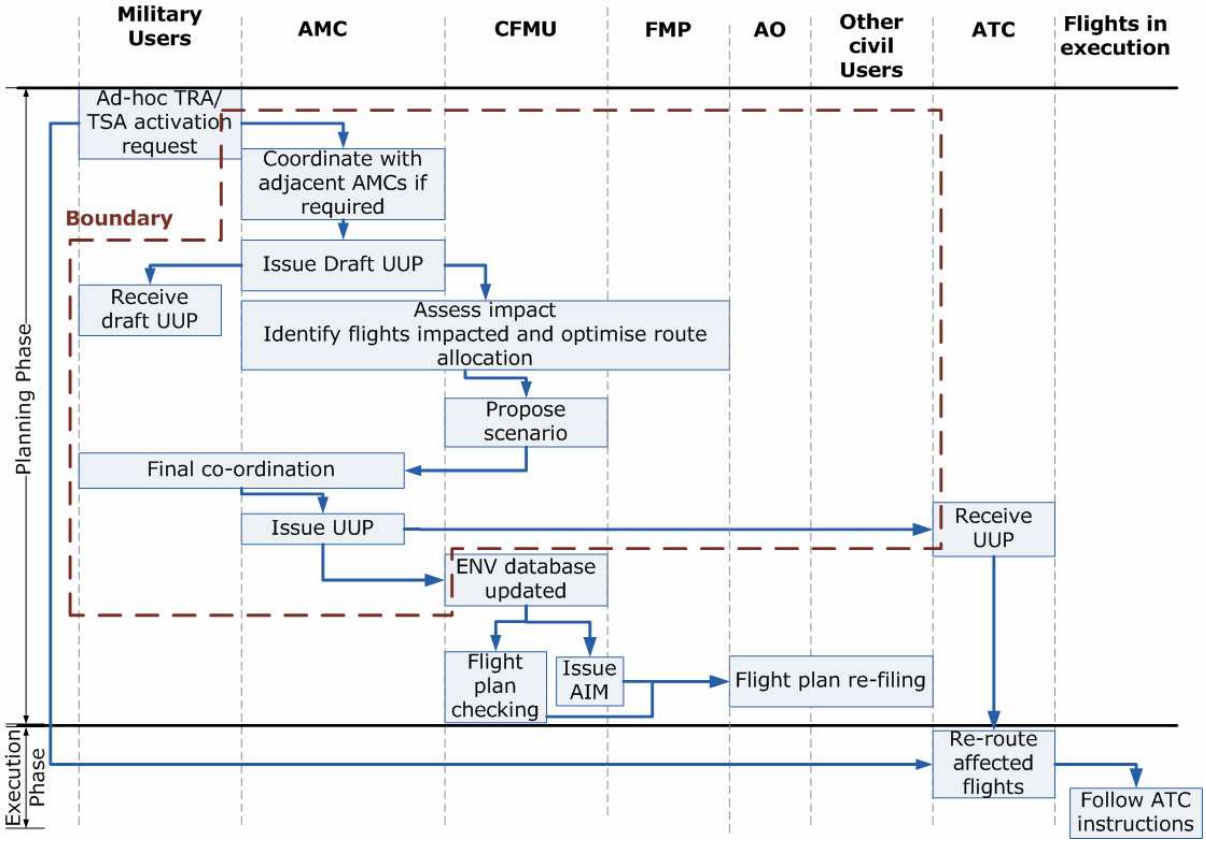


Figure 6: ASM/ATFCM Logical Interaction Model

Appendix C ASM/ATFCM Procedure 3

C.1 ASM/ATFCM Procedure 3 Ad-hoc activation of TSAs/TRAs

C.1.1 As Required the Day Before Operations

a) The Airspace Users that need additional airspace reservations should advise the AMC on the unplanned activation of airspace required (in addition to those published by AUP earlier). For this purpose, as from CRAM publication up to 1600 UTC Summer/1700 UTC Winter time, Airspace Users should send to the AMC their request on additional airspace activation needs which were not envisaged by and published in the relevant AUP.

b) If required, the AMC may carry out coordination with neighbouring AMCs and identify potential available areas.

c) AMC should inform national FMPs and CFMU regarding intentions to implement new or increase already published airspace segregations (in time and/or space) via promulgation of Draft UUP1 at 1600 UTC.

d) CFMU and the AMC should assess the impact of the request at local and network level (e.g. on-loading sector, sector re-configuration, etc). During this step, CFMU should identify the flights that would be impacted by the route closure and consider this element in the assessment, and look for opportunities (reducing the network impact) and coordinate with the AMC for optimisation of airspace allocation (e.g. changing the activation time, flight level band, CDRs closure details). The result of this analysis and potential alternative scenarios (if any) should be sent by CFMU to the AMCs and to the FMP(s) concerned for their consideration.

e) AMCs should receive the Scenario proposed by CFMU and conduct final coordination with Airspace Users, if required.

f) AMCs should take the final airspace allocation decision, and, if required, compose and release the resulting UUP1 information by 1700 UTC Summer/1800 UTC Winter at the latest.

g) The new airspace structure (activated ad hoc area and closed CDR) should be implemented in the CFMU ENV database (only valid as from 0600 UTC Summer/0700 UTC Winter on the Day of operations) to ensure FPL consistency.

h) The new CDR closure information should be disseminated by CFMU through:

- AIMs, which also are available on the NOP portal
- eAMI

Dissemination of information via eAMI is being done through the posting of CDR availability updates onto FTP server in the same way as is being done by CFMU for e-RAD promulgation. Such a process will allow AOs to upload the updates. The posting of updates onto the FTP server is synchronized with publication of relevant AIM.

i) If FPLs are available, FLS messages should be sent by CFMU to flights concerned. AOs concerned should re-file FPLs accordingly.

C.1.2 As Required on the Day of Operations

a) As from UUP1 publication and up to 0800 UTC Summer/0900 UTC Winter time, the Airspace Users that need additional airspace reservations should advise the AMC on the unplanned activation of airspace required (in addition to those published by AUP earlier) for the day of operation (D).

b) AMC should inform national FMPs and CFMU regarding the intention to implement new or increase already published airspace segregations (in time and/or space) via promulgation of Draft UUP2 at 0800 UTC Summer/0900 UTC Winter.

c) Between 0800 - 0900 Summer (0900 - 1000 Winter) CFMU and the AMC should assess the impact of the request at local and network level (e.g. on-loading sector, sector reconfiguration, etc). During this step, CFMU should identify the flights that would be impacted by the route closure, consider this element in the assessment and look for opportunities (reducing the network impact), and coordinate with the AMC for optimisation of airspace allocation (e.g. changing the activation time, flight level band, CDR closure details). The result of this analysis and potential alternative scenarios (if any) should be sent by CFMU to the AMCs and to the FMP(s) concerned for their consideration.

d) AMCs should receive the Scenario proposed by CFMU and FMPs and conduct final coordination with Airspace Users, if required.

e) AMCs should take its final airspace allocation decision, and, if required, compose and release the resulting UUP2 information by 0900 UTC Summer /1000 UTC Winter at the latest.

f) The new airspace structure (activated ad hoc area and closed CDR) should be implemented in the CFMU ENV database (only valid as from 1100 UTC of the day of operations) for ensuring FPL consistency

g) The CDRs ad hoc closures caused by new unexpected airspace area activations should be disseminated by CFMU through:

- AIMs, which also are available on the NOP portal; and
- eAMI

Dissemination of information via eAMI should be done through the posting of CDR availability updates onto FTP server in the same way as is being done by CFMU for e-RAD promulgation. Such a process would allow AOs to upload the updates. The posting of update information onto FTP servers should be synchronized with the publication of relevant AIM.

h) If FPLs are available, FLS messages should be sent by CFMU to flights concerned

- Should the flight be in the Planning Phase, interested AOs should re-file FPLs accordingly.
- Should the flight be in the Execution Phase, it may continue as planned. The rerouting will be provided by the ATC controller to the pilot

Note 1: Flight in the planning phase means a flight in any stage of preparation 2 hours and more before EOBT.

Note 2: Flight in execution phase means a flight as from 2 hours before EOBT onwards (including the airborne stage).

Appendix D ASM/ATFCM Procedure 3 Safety Requirements

D.1 Logical Design Analysis Functional Safety Requirements

Ref.	Safety Requirement	Traceability to ASM/ATFCM Procedure 3
FSR001	ASM/ATFCM Procedure 3 shall require the Military user to issue an ad-hoc request for TRA/TSA activation to the AMC on D-1 after publication of the CRAM but before 16:00 UTC Summer time	A1.1 para a)
FSR002	ASM/ATFCM Procedure 3 shall require the Military user to issue an ad-hoc request for TRA/TSA activation to the AMC on D after publication of the UUP1 but before 08:00 UTC Summer time on the day of operations	A.1.2 para a)
FSR003	ASM/ATFCM Procedure 3 shall require AMCs to coordinate requests for TRA/TSA activation with adjacent AMCs if required	A1.1 para b) ***NOTE***: draft procedure only addressed requests received on the day before operations
FSR004	ASM/ATFCM Procedure 3 shall require AMC to issue a draft UUP1 to CFMU, FMP and the Military user on D-1 at 16:00 UTC Summer time	A1.1 para c)
FSR005	ASM/ATFCM Procedure 3 shall require AMC to issue a draft UUP2 to CFMU, FMP and the Military user on D at 08:00 UTC Summer time	A1.2 para b)
FSR012	ASM/ATFCM Procedure 3 shall require CFMU, AMC, and FMP to use the draft UUP1 or draft UUP2 to assess the impact of the activation on the network	A1.1 para d) A1.2 para c)
FSR013	ASM/ATFCM Procedure 3 shall ensure the network impact assessment undertaken by CFMU and AMC achieves a realistic understanding of the amount of traffic that will need to be managed tactically	A1.1 para d) A1.2 para c)
FSR014	ASM/ATFCM Procedure 3 shall require CFMU and AMCs to ensure that the amount of traffic managed tactically is within the expected capacity of ATC	A1.1 para d) A1.2 para c)
FSR015	ASM/ATFCM Procedure 3 shall ensure that the CFMU and AMC network impact assessment identifies solutions to optimise route allocations	A1.1 para d) A1.2 para c)
FSR016	ASM/ATFCM Procedure 3 shall ensure that when CFMU and AMCs are assessing the capacity of ATC, allowance is made for ATC to deal with an additional event in parallel with the route closure	A1.2 para c)
FSR017	ASM/ATFCM Procedure 3 shall require CFMU to ensure that if the ENV database is known to have failed at the time of the capacity assessment, the expected increase in the number of flights requiring tactical management shall be included in the assessment	A1.1 para d) A1.2 para c)
FSR018	ASM/ATFCM Procedure 3 shall require CFMU to ensure that if the IFPS is known to have failed at the time of the capacity assessment, the expected increase in the number of flights requiring tactical management shall be included in the assessment	A1.1 para d) A1.2 para c)
FSR022	ASM/ATFCM Procedure 3 shall require AMC to liaise with the Military to co-ordinate the details of the activation	A1.1 para e) A1.2 para e)

Ref.	Safety Requirement	Traceability to ASM/ATFCM Procedure 3
FSR023	ASM/ATFCM Procedure 3 shall ensure that the AMC and FMP makes a final decision on the allocation of airspace	A1.1 para f) A1.2 para e)
FSR024	ASM/ATFCM Procedure 3 shall require the AMC to ensure that the time limits of any activation are within the time limits of the scenario proposed by CFMU	A1.1 para f) A1.2 para e)
FSR025	ASM/ATFCM Procedure 3 shall require the AMC to promulgate the final decision on airspace allocation via a UUP1 to CFMU, Military and ATC on D-1 at 17:00 UTC Summer time	A1.1 para e)
FSR026	ASM/ATFCM Procedure 3 shall require the AMC to promulgate the final decision on airspace allocation via a UUP2 to CFMU, Military and ATC on D at 09:00 UTC Summer time	A1.2 para e)
FSR034	ASM/ATFCM Procedure 3 shall require each State to agree the mechanism by which AMC negotiates alternative scenarios to an initial activation request	A1.1. para d) A1.2 para c)
FSR035	ASM/ATFCM Procedure 3 shall require CFMU to make available updated information on CDR availability to all Stakeholders	A1.1 para h) A1.2 para g)
FSR036	ASM/ATFCM Procedure 3 shall define the mechanism, content and format by which CDR availability is promulgated	A1.1 para h) A1.2 para g)
FSR037	ASM/ATFCM Procedure 3 shall require CFMU to update the ENV database with changes from the final airspace allocation decision in a timely manner	No traceability

Table 8: Logical Design Analysis Functional Safety Requirements

D.2 Task Analysis Functional Safety Requirements

Ref.	Safety Requirement	Traceability to ASM/ATFCM Procedure 3
FSR006	ASM/ATFCM Procedure 3 shall require States to ensure that adjacent AMCs, CFMU and FMP shall acknowledge receipt of draft UUP1	No traceability
FSR007	ASM/ATFCM Procedure 3 shall require States to ensure that adjacent AMCs, CFMU and FMP shall acknowledge receipt of draft UUP2	No traceability
FSR008	ASM/ATFCM Procedure 3 shall require the Military user to acknowledge receipt of the draft UUP1	No traceability
FSR009	ASM/ATFCM Procedure 3 shall ensure that the Military confirm that the draft UUP1 information is acceptable	No traceability
FSR010	ASM/ATFCM Procedure 3 shall require the Military user to acknowledge receipt of the draft UUP2	No traceability
FSR011	ASM/ATFCM Procedure 3 shall ensure that the Military confirm that the draft UUP2 information is the same as the initial request made	No traceability
FSR019	ASM/AFTCM Procedure 3 shall require CFMU to propose a scenario to the AMC on D-1 before 17:00 UTC Summer time	A1.1 para d)
FSR020	ASM/ATFCM Procedure 3 shall require CFMU to propose a scenario to the AMC on D before 09:00 UTC Summer time.	A1.1 para d)

Ref.	Safety Requirement	Traceability to ASM/ATFCM Procedure 3
FSR021	ASM/ATFCM Procedure 3 shall require all proposed scenarios from CFMU to be provided in a consistent written format	A1.2 para c)
FSR027	ASM/ATFCM procedure 3 shall require the Military to acknowledge receipt of the UUP1 as soon as possible once received from the AMC	No traceability
FSR028	ASM/ATFCM procedure 3 shall require the Military to acknowledge receipt of the UUP2 as soon as possible once received from the AMC	No traceability
FSR029	ASM/ATFCM Procedure 3 shall ensure that AMC upload the UUP1 to the ENV database using the CIAM interface	No traceability
FSR030	ASM/ATFCM Procedure 3 shall ensure that AMC upload the UUP2 into the ENV database using the CIAM interface	No traceability

Table 9: Task Analysis Functional Safety Requirements

D.3 External Functional Safety Requirements

Ref.	Safety Requirement
EFSR001	States implementing ASM/ATFCM Procedure 3 shall agree dedicated roles and responsibilities for initiating requests for TRA/TSA activation
EFSR002	States implementing ASM/ATFCM Procedure 3 shall agree dedicated roles and responsibilities for receiving requests for TRA/TSA activation
EFSR003	States implementing ASM/ATFCM Procedure 3 shall define the mechanism, content and format of requests for TRA/TSA activation
EFSR004	States shall consider the impact of an increased frequency of TRA/TSA requests and the associated time needed to process such requests given local traffic densities in the implementation/tailoring of ASM/ATFCM Procedure 3

Table 10: External Functional Safety Requirements

D.4 Safety Monitoring Requirements

Ref.	Safety Requirement
SMR001	EUROCONTROL shall monitor the frequency of inconsistencies between AIM messages and associated UUPs
SMR002	EUROCONTROL shall ensure that the increased number of TRA/TRA requests as a result of ASM/ATFCM Procedure 3 does not increase the frequency of which CFMU fail to update the ENV database in time

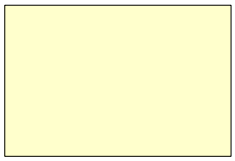
Table 11: Safety Monitoring Requirements

D.5 Assurance Level Requirement

Ref.	Safety Requirement
PAL001	The demonstrable level of confidence that ASM/ATFCM Procedure 3 must satisfy in order to manage risks due to procedural implementation shall be Procedure Assurance Level 3

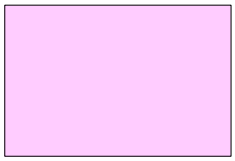
Table 12: Assurance Level Requirement

Appendix E Goal Structured Notation (GSN)

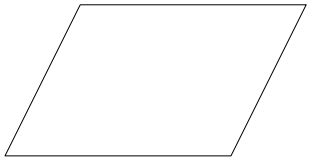


Safety Argument Goal (Top level argument)

Safety Argument Goal (sub-argument)



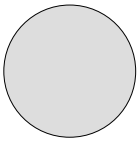
Safety Argument Goal (sub-argument – outside scope)



Safety Argument strategy for achieving the Goal

Criteria to support goal

Assumption/Context/Justification to support goal or strategy



Reference to supporting evidence

Figure 7: Guide to Goal Structured Notation