EUROCONTROL

EUROCONTROL Guidance Material for Minimum Safe Altitude Warning
Appendix B-2: Generic Safety Plan for MSAW Implementation

Edition Number	:	1.0
Edition Date	:	19 May 2009
Status	:	Released Issue
Intended for	:	CND Stakeholders

EUROCONTROL

DOCUMENT CHARACTERISTICS

TITLE		
EUROCONTROL Guidance Material for Minimum Safe Altitude Warning **Appendix B-2: Generic Safety Plan for MSAW Implementation**		
Document Identifier	**Edition Number:**	1.0
EUROCONTROL-GUID-127	**Edition Date:**	19 May 2009

Abstract

This document is the first of a set of three documents the purpose of which is to provide guidance material for ANSPs to assure their own implementations of MSAW in accordance with the EUROCONTROL Specification for Minimum Safe Altitude Warning (MSAW) in the ECAC area. This document describes a generic safety plan.

Keywords

Safety
Safety Case
Safety Nets
MSAW
Safety Argument
Safety Plan

Contact Person(s)	Tel	Unit
Hans Wagemans	+32 2 72 93334	CND/COE/AT/AO

STATUS, AUDIENCE AND ACCESSIBILITY					
Status		**Intended for**		**Accessible via**	
Working Draft	☐	General Public	☐	Intranet	☐
Draft	☐	CND Stakeholders	☑	Extranet	☐
Proposed Issue	☐	Restricted Audience	☐	Internet (www.eurocontrol.int)	☑
Released Issue	☑	*Printed & electronic copies of the document can be obtained from ALDA (see page iii)*			

ELECTRONIC SOURCE		
Path:	\\HHBRUNA02\bakkerb$\QC	
Host System	Software	Size
Windows_NT	Microsoft Word 10.0	345 Kb

EUROCONTROL Agency, Library Documentation and Archives (ALDA)
EUROCONTROL Headquarters (50.703)
96 Rue de la Fusée
B-1130 BRUSSELS

Tel: +32 (0)2 729 11 52
E-mail: publications@eurocontrol.int

DOCUMENT APPROVAL

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

AUTHORITY	NAME AND SIGNATURE	DATE
Technical Manager	 Hans Wagemans	19-5-2009
Head of ATC Operations and Systems Unit	 Martin Griffin	19-5-2009
Deputy Director Network Development	 Alex Hendriks	19-5-2009

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
1.0	19-5-2009	First released issue	All

CONTENTS

EXECUTIVE SUMMARY

It is Safety Management best practice and an ESARR 4 requirement to ensure that all new safety related ATM systems or changes to the existing system will meet their safety objectives and safety requirements. ANSPs and National Supervisory Authorities (NSA) will need documented assurance that this is the case before deploying the new or changed system in operation. Typically, the assurance is presented as a safety case.

This document is one of a set of three documents the purpose of which is to provide guidance material for ANSPs to assure their own implementations of MSAW in accordance with the EUROCONTROL Specification. Each document represents a snapshot of the safety assurance work already undertaken at different stages of a project. The document set includes:

1. **Initial Safety Argument for Minimum Safe Altitude Warning: -** Ideally, produced during the definition phase of a project to introduce a change to the ATM system e.g. to introduce MSAW. The process of developing and acquiring the necessary assurance is considerably enhanced if the safety arguments are set out clearly from the outset.

2. **Generic Safety Plan for the implementation of MSAW [This document]: -** Initially produced at the outset of a project as part of the project plan, but focused only on those activities necessary to provide assurance information for inclusion in a safety case. The safety plan will be subject to development and change as the project unfolds and more detail becomes available.

3. **Outline Safety Case for MSAW: -** Commenced at the start of a project, structured in line with the safety argument, and documented as the results of the planned safety assurance activates become available.

The documented assurance should contain the evidence, arguments and assumptions as to why a system is safe to deploy. The process of developing and acquiring the necessary safety assurance is considerably enhanced if the activities to obtain it are planned from the outset, ideally during the system definition phase of a project, and documented in a safety plan.

This document is a generic safety plan for MSAW implementation, covering all the system lifecycle phases. It contains the assurance requirements, assurance objectives and the activities that should be considered at each phase to achieve them. It also indicates who should carry out the activities. The output of the activities in the safety plan should provide the evidence necessary to complete the safety case.

Another advantage of having a safety plan is that it can be offered to the NSA in order to get an early indication of the likelihood that the planned assurance activities will lead to NSA approval of the system.

Although the activities scheduled in a safety plan may be regarded as part of a project plan, it is advantageous for safety management purposes to keep it as separate document. Note that not all the assurance objectives and activities will be known at the outset and the safety plan may need to be updated as system development progresses.

1. INTRODUCTION

Minimum Safe Altitude Warning (MSAW) is a ground-based safety net intended to warn the controller about increased risk of controlled flight into terrain accidents by generating, in a timely manner, an alert of aircraft proximity to terrain or obstacles.

The European Convergence and Implementation Plan (ECIP) contains an objective (ATC02.6) for ECAC-wide standardisation of MSAW in accordance with the EUROCONTROL Specification for Minimum Safe Altitude Warning. The EUROCONTROL Specification for MSAW specifies, in qualitative terms, the common performance characteristics of MSAW as well as the prerequisites for achieving these performance characteristics

The detailed safety work must be undertaken in accordance with European and National regulations and directives, which may refer to the EUROCONTROL recommended methodologies and practices. The current document is part of a set of documents that have been produced under contract by NATS, to serve as guidance material for carrying out the detailed safety work using the EUROCONTROL recommended methodologies and practices.

It is assumed that the safety assurance – i.e. arguments, evidence and assumptions - that MSAW is safe for deployment in operation will be recorded in each ANSPs Safety Case.

In order to facilitate the ANSPs' safety work, this Safety Plan, an accompanying Safety Argument and an Outline Safety Case have been developed by EUROCONTROL to substantiate, as far as possible at this stage, the argument that STCA will be acceptably safe in ATM operations.

2. PURPOSE

The purpose of this Safety Plan is to provide guidance to ANSPs on planning the safety assurance activities, collecting the evidence required to support the safety argument and ensuring that adequate safety assurance documentation will be produced in a timely manner. The Plan should be read with reference to the Safety Argument and the Outline Safety Case and should be adapted / developed by ANSPs to suit their own particular implementation of MSAW.

This Safety Plan contains details of the assurance requirements, assurance objectives and the activities which are necessary to provide evidence that MSAW will be acceptably safe in ATM operations. It identifies who might undertake these activities; the outputs from the activities; and the tools, techniques, methods or standards to be used. The output of the activities in the safety plan should provide the evidence necessary to complete the safety case.

.

3. SCOPE

This Plan identifies the safety activities that should be undertaken in the definition, development and deployment of MSAW. The scope of this document encompasses all phases of a system lifecycle and all system elements (people, procedures and equipment.

4. ROLES AND RESPONSIBILITIES

Four main roles and responsibilities are identified under the acronym **LDCI:**

Role	Responsibility
Lead:	Responsible for ensuring the assurance and evidence is provided
Do:	Responsible for providing assurance and evidence
Consult:	Who should be consulted in the process
Inform:	Who should be informed of the outcome

Table 1: roles and responsibilities

Note: it is accepted that there may not be staff posts with the titles used in the tables presented in section 6 below, but it is assumed that someone will perform the role. ANSPs will need to tailor the roles to their organisation when instantiating this Plan.

5. SYSTEM LIFECYCLE PHASES

5.1 Safety Activities during System Lifecycle

The following Fig 1 is used to illustrate the relationship between the safety assessment and safety assurance activities referred to in this Plan and the system lifecycle:

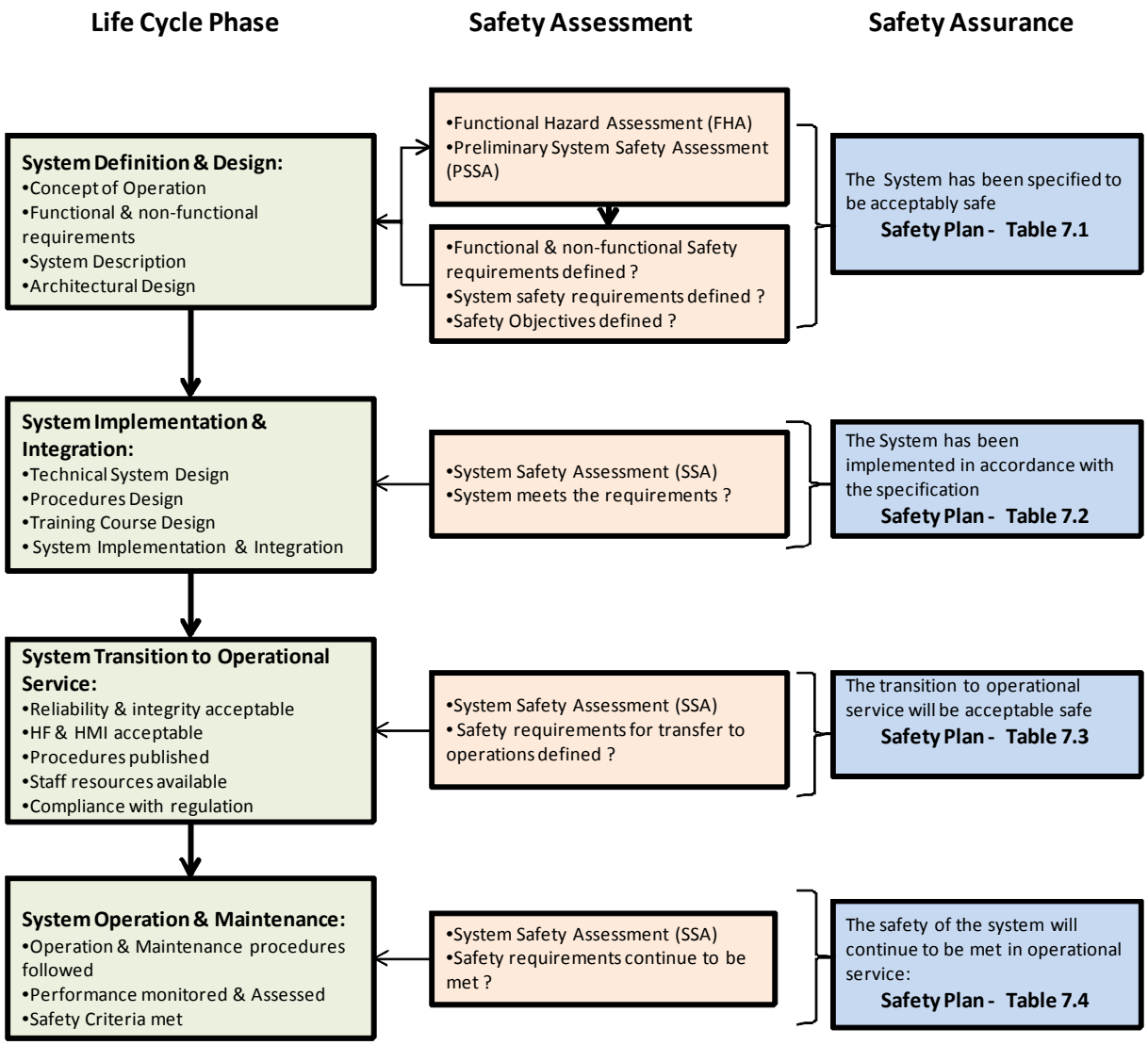

Figure 1: – System lifecycle and safety activities

5.2 System Definition and Design

The basic operational objectives for the system are established during the system definition phase. The concept of operations is developed and the feasibility of implementing it in the existing ATM system is determined.

The policy for MSAW is determined. Assumptions about the system boundaries and its operational environment are recorded.

The functional and non-functional requirements to enable the concept are specified. These are subjected to Functional Hazard Assessment FHA and risk assessment to identify hazards that might impact on the design of the system. Safety objectives and high level safety requirements are derived for the system and mitigation for identified hazards determined.

The system architecture is determined which can reasonably be expected to achieve the functional and non-functional requirements and the safety objectives specified in the FHA.

A preliminary system safety assessment is carried out to determine potential causes of hazards arising from the proposed system design. The resulting safety requirements have to be achieved by the design.

The technical design should comply with the specification, safety requirements and any regulatory requirements.

The assurance objectives and assurance activities are listed in Table 7.1 of the Assurance Strategy

5.3 System Implementation & Integration

The Technical system is developed and implemented in hardware and software. The system elements should meet the safety requirements and be able to meet the safety objectives.

Any hazards to the existing ATM system arising from integration have been identified and addressed.

Training courses are established and running. ATC and Engineering procedures are integrated into ANSP documentation.

The assurance objectives and assurance activities are listed in Table 7.2 of the Assurance Strategy.

5.4 Transfer to Operations

The system (people, procedures and equipment) is assessed as fit for purpose. All limitations and shortcomings are identified and addressed. An approved safety case is completed and is accepted by the ANSP and the regulator where necessary.

The assurance objectives and assurance activities are listed in Table 7.3 of the Assurance Strategy.

5.5 Operation and Maintenance

MSAW status information is continuously monitored and ATC are advised of any changes that might affect the system performance.

MSAW performance is monitored and analysed to ensure that it does not degrade and that it continues to satisfy ANSP safety objectives.

The assurance objectives and assurance activities are listed in Table 7.4 of the Assurance Strategy

6. STRATEGY FOR ASSURANCE

The following Tables contain details of the planned assurance, scheduled according to the system lifecycle phases – a separate table for each.

Each assurance activity is given a unique reference number (column 1) e.g. [Ref 7.1.1]

The assurance requirements (column 2) are derived from the safety argument and referenced accordingly e.g. Arg 1.1.

The assurance objectives (column 3) are based on the objectives proposed in the document Safety Assessment Made Easier [Ref 4] and are considered to be representative of the assurance required in practice. [Note these are provisional assurance objectives, and ANSPs will need to adapt them for their own use]

The safety assurance activities considered necessary to meet the assurance objectives are listed in column 4.

Different people and organisations are likely to be involved in carrying out the assurance activities. It can be valuable to determine what the responsibilities are at the planning stage. An indication of how this might be done is given in column 5. However, this is strictly a matter for the ANSPs and organisations involved, and the resources available.

Satisfactory completion of the planned assurance activities should result in assurance evidence for inclusion or reference in the safety case, as indicated in column 6.

Ref:	Assurance Requirement	Assurance Objectives	Safety Assurance Activity	Responsibility	Documented Evidence
7.1.1 Safety Criteria	Defined safety criteria for use MSAW in ATM operations. [Arg 0].	(1) Show that the criteria by which the safety of MSAW in ATM operations can be checked have been defined.	Confirm by review that acceptable criteria have been defined and are consistent with the assurance objectives.	L: ANSP Management D: ANSP Management C: Incident data base and other ANSPS I: Safety Manager	Criteria defined and documented in safety case
7.1.2 Policy	Defined policy justifying the need for MSAW. [Arg 0]	(1) Show that a clear and unambiguous policy regarding use of MSAW has been produced (2) Show that the policy is consistent with regulatory requirements for safety nets.	Confirm by review that MSAW policy exists and that it is consistent with NSA regulatory requirements and EUROCONTROL specification.	L: ANSP Management D: ANSP Management C: NSA I: Safety Manager	MSAW Policy and results from review documented in safety case
7.1.3 Assumptions	Identified assumptions upon which the safety of MSAW is dependent. [Arg 0]	(1) Show that assumptions have been documented and confirmed by ATC and engineering as appropriate.	Confirm by review that assumptions can be depended on for the planned system.	L: ANSP Management D: ANSP Management C: Operations Managers I: Safety Manager	Assumptions and results from review documented in safety case
7.1.4 Conops	The Concept of Operation (Conops) is safe in itself. [Arg 1.1]	(1) Show that the initial safety issues have been identified and addressed. (2) Show that the minimum functionality has been defined and shown to be compatible with the safety criteria. (3) Show that the differences from existing Conops have been described, in terms of what MSAW will do when introduced into the ATM system. (4) Show that the impact of the Conops on the operational environment (including interfaces with adjacent systems / airspace) has been assessed and shown to be compatible with the safety criteria.	Confirm by review and/or analysis that the Conops exists and that it is consistent with the assurance objectives.	L: ANSP Management D: ANSP Management C: NSA I: Safety Manager	Documented Conops. Results & conclusions from review/analysis summarised in safety case.
7.1.5 Design Completeness	The corresponding MSAW design is complete. [Arg 1.2]	(1) Show that everything necessary to achieve a safe implementation of the Conops – related to human, procedure, equipment and airspace design - has been specified. (2) Show that the all the requirements on, and assumptions about, external elements of MSAW have been captured.	Confirm by review that the specification is complete and correct, and consistent with the assurance objectives.	L: ANSP Management D: ANSP Management C: Operations Managers & HF Expert I: Safety Manager	Written specification & results from review summarised in safety case. Compliance Matrix – traceability to Conops included or referenced in safety case

Table 7.1: System definition and design - safety assurance plan

Ref:	Assurance Requirement	Assurance Objectives	Safety Assurance Activity	Responsibility	Documented Evidence
7.1.6 Functionality	MSAW has been designed to function correctly under all normal conditions. [Arg 1.3]	(1) Show that the MSAW design has been clearly described, and has the potential to show that MSAW functions correctly under all normal environmental conditions (2) Show that the level of detail is sufficient to support the FHA process and the derivation of safety objectives for the overall design.	Confirm by review that the specified MSAW design is consistent with the assurance objectives.	L: ANSP Management D: ANSP Management C: Operations Managers & HF Expert I: Safety Manager	Documented design. Review findings summarised in safety case
7.1.7 Design robustness	The system design is robust against external abnormalities [Arg 1.4]	(1) Show that the MSAW design can react safely to all reasonably foreseeable external failures – i.e. any failures in its environment / adjacent systems that are not covered under Arg1.5. (2) Show that the MSAW design can react safely to all other reasonably foreseeable abnormal conditions in its environment / adjacent systems that are not covered under Arg1.3.	Confirm by design review	L: ANSP Management D: ANSP Management C: Operations Managers & HF Expert I: Safety Manager	Review findings documented and referenced in safety case
7.1.8 Safety Assessment	All risks from internal system failures have been mitigated sufficiently [Arg 1.5] (1) All hazards identified correctly and assessed	(1) Show that the all reasonably foreseeable hazards, at the boundary of the MSAW system, have been identified (2) Show that the severity of the effects from each hazard has been correctly assessed, taking account of any mitigations that may be available / could be provided external to the MSAW. (3) Show that the Safety Objectives have been set for each hazard such that the corresponding aggregate risk is within the specified Safety Criteria (4) Show that the all reasonably foreseeable causes of each hazard have been identified	Application of the FHA process as defined in EUROCONTROL SAM	L: ANSP Management D: FHA Expert C: ATC & Engineering Staff & HF Expert I: Safety Manager	FHA Results summarised in safety case with reference to all relevant documentation. Safety Objectives Tabulated in the safety case
	All risks from internal system failures have been mitigated sufficiently [Arg 1.5] (2) MSAW Safety Requirements Specified	(5) Show that the safety requirements have been specified (or Assumptions stated) for the causes of each hazard, taking account of any mitigations that are / could be available internal to the system, such that the Safety Objectives (and/or Safety Criteria) are satisfied (6) Show that the safety requirements have been verified and validated (7) Show that the all external and internal mitigations have been captured as either safety requirements or assumptions as appropriate (8) Show that the system can actually operate safely under all degraded modes of operation identified under this Argument	Application of the PSSA process as defined in EUROCONTROL SAM	L: ANSP Management D: PSSA Expert C: ATC & Engineering Staff & HF Expert I: Safety Manager	Results from PSSA process summarised in safety case.

Table 7.1 (cont): System definition and design - safety assurance plan

Ref:	Assurance Requirement	Assurance Objectives	Safety Assurance Activity	Responsibility	Documented Evidence
7.1.9 Realistic Specification	That which is specified is realistic. [Arg 1.6]	(1) Confirm that all hazard related aspects of the system design have been captured as Safety Requirements or (where applicable) as Assumptions (2) Confirm that all Safety Requirements are verifiable – i.e. satisfaction can be demonstrated by direct means (e.g. testing) or (where applicable) indirectly through appropriate assurance processes. (3) Confirm that all Safety Requirements are capable of being satisfied in a typical implementation in hardware, software, people and procedures. (4) Confirm that all Assumptions have been shown to be valid.	Review of the design with respect to the safety requirements Verification of testability	L: ANSP Management D: PSSA Expert C: ATC & Engineering Staff & HF Expert I: Safety Manager	Review and verification results summarised in safety case.
7.1.10 Trustworthy Specification	The evidence for safety specification is trustworthy [Arg 1.7]	(1) Confirm that the assurance processes , tools and techniques used were adequate for the task 2) Confirm that the competence of the people using them was adequate for the task	Assessment of the approach and qualifications of people involved followed taking into account the EUROCONTROL Guidance Material for Minimum Safe Altitude Warning Appendix A: Reference MSAW System [Ref 3]	L: ANSP Management D: PSSA Expert C: ATC & Engineering Staff & HF Expert I: Safety Manager	Assessment results summarised in the safety case

Table 7.1(Cont): System definition and design - safety assurance plan

Ref:	Assurance Requirement	Assurance Objectives	Safety Assurance Activity	Responsibility	Documented Evidence
7.2.1 Technical system design	The technical system is designed to meet requirements [Arg 2.1]	(1) Confirm that the design requirements interpret the specification completely and correctly. (2) Confirm that the design is documented and under configuration control. (3) Confirm that the design incorporates all the requirements, completely and correctly.	Review of documented design to confirm completeness and correctness	**L**: ANSP Management D: ATC & Engineering C: Developer I: Safety Manager	Documented design, under configuration control. Results of review and high level description of design in safety case. Design documents referenced in safety case
7.2.2 Technical System Implementation & Integration	The technical system is implemented and integrated as designed [Arg 2.2]	(1) Confirm that the MSAW meets the specified functional and non functional safety requirements (2) Confirm that the MSAW functions correctly and coherently under all normal conditions (3) Confirm that the MSAW is robust against external abnormalities.	HW & SW Reviews Reliability & Integrity Testing Performance analysis Operating Trials Accuracy analysis Task Analysis Simulation Trials	L: ANSP Management D: Developer C: ANSP ATC, Eng, HF experts & regulator I: Safety Manager	Following summarised or referenced in the safety case: • Analysis & test results • Trial results • Simulation results. • Evidence of test coverage Evidence of low probability of residual faults (from analysis of the design process and product)
7.2.3 Procedures	MSAW procedures designed and implemented to meet the requirements [Arg 2.3]	(1) Confirm that the Procedures have been designed to meet the safety requirements (2) Confirm that the procedures have been implemented. (3) Confirm that the Controllers and Engineers are trained and competent to operate MSAW and procedures.	Establish by review that procedures have been included in ANSP ATC procedures, Operating and Maintenance Manuals and/or Documentation	L: ANSP Management D: ANSP Operations Managers C: Document Administration I: Safety Manager	ATC procedures manual, Operating and Maintenance Manuals referenced in safety case Results of review summarised in safety case.
7.2.4 Training	Training courses for Controllers and Engineers designed and implemented to meet the requirements [Arg 2.4]	(1) Confirm that the Training Courses have been designed to meet the safety requirements (2) Confirm that the Training Courses have been implemented	Review of course schedule and feedback reports	L: ANSP Management D: ANSP Training Staff C: ATC & Engineering & HF Expert I: Safety Manager	Course Schedule and list of attendees referenced in safety case Results of review summarised in safety case

Table 7.2: System implementation and integration - safety assurance plan

Ref:	Assurance Requirement	Assurance Objectives	Safety Assurance Activity	Responsibility	Documented Evidence
7.3.1	Transition to Operational Service of the MSAW system will be acceptably Safe [Arg 3]	(1) Confirm that the safety requirements for the transfer to operation have been specified (2) Confirm that the system reliability & integrity accepted as meeting the F&P safety requirements. (3) Confirm that the HF and HMI accepted as satisfactory (4) Confirm that the sufficient trained staff available to operate and maintain the system. (5) Confirm that the procedures are published and promulgated to all relevant staff. (6) Confirm that the operational validation trials satisfactory (7) Confirm that the system shortcomings highlighted and accepted for operation. (8) Confirm that the regulatory approval to operate obtained.	Confirm by review of the results of system acceptance tests and commissioning process, resources, and regulatory approval.	L: ANSP Operations D: ANSP Operations Manager C: Safety Manager I: ANSP Manager	The following should be summarised in the safety case: • Results of review • Results of acceptance tests • Commissioning procedure (reference)

Table 7.3: Transition to operational service - safety assurance plan

Ref:	Assurance Requirement	Assurance Objectives	Safety Assurance Activity	Responsibility	Documented Evidence
7.4.1	The safety of MSAW will continue to be demonstrated in operational service [Arg 4]	(1) Confirm that Staff have been assigned with the responsibility for management of MSAW (to fulfil the above functions) (2) Confirm that a formal process exists for monitoring MSAW Status (3) Confirm that a formal process exists for monitoring MSAW and analysing the results (4) Show that the system remains optimised for its role and keeps pace with changing operational requirements. (5) Show that ATC are advised of any system changes that might affect the safety performance (6) Show that MSAW maintenance procedures are in place and are fit for purpose	Confirm by safety survey	L: ANSP Operations D: ANSP Operations Manager C: Safety Manager I: ANSP Manager	Results of survey summarised in safety case. Update the safety case

Table 7.4: system operation and maintenance - safety assurance plan

7. LIST OF ABBREVIATIONS

ANSP	Air Navigation Service Provider
CFIT	Controlled Flight Into Terrain
Conops	Concept of operation
ECIP	European Convergence and Implementation Plan
FHA	Functional Hazard Assessment
FTA	Fault Tree Analysis
GSN	Goal-Structuring Notation
HF	Human Factors
HMI	Human Machine Interface
MSAW	Minimum Safe Altitude Warning
NSA	National Supervisory Authority
PSSA	Preliminary Safety Assessment Process
SAM	Safety Assessment Methodology
SCDM	Safety Case Development Manual
SPIN	Safety nets Performance Improvement Network (Sub Group)
SRC	Safety Regulation Commission
SSA	System Safety Assessment

8. REFERENCES

1. EUROCONTROL Specification for Minimum Safe Altitude Warning
2. EUROCONTROL Guidance Material for Minimum Safe Altitude Warning
3. EUROCONTROL Guidance Material for Minimum Safe Altitude Warning Appendix A: Reference System
4. Safety Assessment Made Easier version 0.92

END OF DOCUMENT