

EUROCONTROL



**EUROCONTROL Guidance
Material for Minimum Safe Altitude
Warning
Appendix B-1: Initial Safety
Argument for MSAW System**

Edition Number	:	1.0
Edition Date	:	19 May 2008
Status	:	Released Issue
Intended for	:	CND Stakeholders



DOCUMENT CHARACTERISTICS

TITLE		
EUROCONTROL Guidance Material for Minimum Safe Altitude Warning		
Appendix B-1: Initial Safety Argument for MSAW System		
Document Identifier	Edition Number:	1.0
EUROCONTROL-GUID-127	Edition Date:	19 May 2008
Abstract		
<p>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 possible Safety Argument.</p>		
Keywords		
Safety Nets MSAW Safety Argument Safety Plan	Safety Case	
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	<input type="checkbox"/>	General Public	<input type="checkbox"/>	Intranet	<input type="checkbox"/>
Draft	<input type="checkbox"/>	CND Stakeholders	<input checked="" type="checkbox"/>	Extranet	<input type="checkbox"/>
Proposed Issue	<input type="checkbox"/>	Restricted Audience	<input type="checkbox"/>	Internet (www.eurocontrol.int)	<input checked="" type="checkbox"/>
Released Issue	<input checked="" type="checkbox"/>	<i>Printed & electronic copies of the document can be obtained from ALDA (see page iii)</i>			

ELECTRONIC SOURCE		
Path:	\\HHBRUNA02\bakkerb\$\QC	
Host System	Software	Size
Windows_NT	Microsoft Word 10.0	443 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

1. INTRODUCTION	3
2. PURPOSE OF THIS DOCUMENT	3
3. SCOPE	4
4. SAFETY ARGUMENT.....	4
4.1 Introduction	4
4.2 GSN Symbols Used	4
4.3 Overall Argument structure	5
4.4 Top Level Argument [Arg 0]	6
4.5 Safety Criteria	6
4.6 Context.....	7
4.7 Assumptions.....	7
4.8 Justification 01	7
4.9 Strategy.....	8
4.10 Assurance Objectives	8
5. MSAW SPECIFICATION AND SAFETY REQUIREMENTS	8
5.1 Introduction	8
5.2 MSAW has been specified to be acceptably safe [Arg 1]	9
5.3 The Conops is safe in itself [Arg 1.1]	10
5.4 The corresponding MSAW design is complete [Arg 1.2]	11
5.5 MSAW has been designed to function correctly under all normal conditions [Arg 1.3]	11
5.6 The MSAW design is robust against external abnormalities [Arg 1.4].....	12
5.7 All risks from internal MSAW failures have been mitigated sufficiently [Arg 1.5].....	12
5.8 The specified MSAW is realistic [Arg 1.6].....	14
5.9 The evidence for the safety specification is trustworthy [Arg 1.7].....	15
6. MSAW COMPLIANCE WITH THE SAFETY REQUIREMENTS.....	16
6.1 Introduction	16
6.2 MSAW has been implemented in accordance with the specification [Arg 2].....	16

6.3	The MSAW technical design meets the safety requirements [Arg 2.1]	17
6.4	The MSAW technical elements are implemented and integrated as designed [Arg 2.2]	17
6.5	MSAW procedures are designed and implemented to meet the safety requirements [Arg 2.3].....	18
6.6	Training Courses for Controllers and Engineers designed and implemented to meet the safety requirements [Arg 2.4].....	18
6.7	Transition to operational service of MSAW will be acceptably safe [Arg 3].....	19
7.	SYSTEM OPERATION AND MAINTENANCE.....	20
7.1	The safety of MSAW will continue to be demonstrated in operational service (Arg 4).....	20
8.	LIST OF ABBREVIATIONS.....	22
9.	REFERENCES	23

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 be acceptably safe in ATM operations. 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** [This document]:- 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**: - 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 activities become available.

An initial safety argument for MSAW is set out in this document and it is intended for use by ANSPs in developing assurance for MSAW applications. The argument should follow a logical structure, and be complete regarding the scope of the system, its environment, and any assumptions that have to be taken into account regarding these.

Development and review of the safety argument is aided by the use of a graphical presentation rather than just text alone. It is easier to follow the logic of the argument in graphical form and to check it for completeness and correctness. Such an approach is employed in this document, based on a EUROCONTROL adaptation of Goal-Structuring Notation [GSN].

ANSPs may find it convenient to present their argument as a stand-alone document initially, as is the case with this document. However, the argument will ultimately form part of the safety case document and the stand-alone version will then become defunct.

The evidence required to support the argument is identified in this document. The activities necessary to obtain this evidence should be scheduled in a safety plan. The combination of the safety argument and the output from the safety plan should provide all that is necessary to make a safety case.

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.

The overall purpose of the safety work is to provide assurance to, firstly the ANSP, and secondly the National Supervisory Authority (NSA), that the use of MSAW will be acceptably safe in ATM operations. The assurance is documented and presented in the form of a Safety Case. The documented assurance should include an adequate and credible argument regarding the safety of MSAW, and the evidence to support it.

It is good practice to develop the safety argument at the start of the MSAW project. Doing so will help to ensure that any constraints affecting the safety aspects of the project are understood, that the criteria for success are defined, any assumptions are identified and the nature and scope of the necessary safety assurance evidence is highlighted. The safety argument can be then be used to structure the safety case.

This document:

- Explains how to construct a safety argument for MSAW
- Explains how to provide evidence in support of the safety arguments
- Provides example of arguments to be modified, adapted or expanded to fit with own MSAW and operational context

2. PURPOSE OF THIS DOCUMENT

The document contains an initial safety argument intended to be used by ANSPs in developing safety assurance for MSAW applications. The aim is to

aid ANSPs in reasoning about what is necessary by way of assurance to show that their MSAW will be acceptably safe in ATM operations and to reveal the logic behind such reasoning. The logic of the argument is presented graphically to make it clear and mutually understandable. The evidence required to support the argument is identified. The safety argument and associated evidence are essential content for a safety case¹.

ANSPs may find it useful to develop their argument in a stand-alone document initially, as with this document. One advantage of doing so is that it could be used as an early deliverable to their regulator when seeking prior approval for their planned assurance strategy. However, the argument will ultimately form part of the safety case document and the stand-alone version will then become defunct.

3. SCOPE

The safety argument encompasses all stages of the MSAW lifecycle, and all elements of the MSAW system including people, procedures and equipment.

4. SAFETY ARGUMENT

4.1 Introduction

The safety argument structure is based on an adapted form of Goal Structuring Notation [GSN] as described in the EUROCONTROL Safety Case Development Manual (SCDM).

4.2 GSN Symbols Used

The argument is represented graphically using the following symbols:

¹ A Safety Case is defined by the EUROCONTROL SCDM [4] as "...the **documented** assurance (i.e. argument and supporting evidence) of the achievement and maintenance of safety. It is primarily the means by which those who are accountable for service provision or projects assure **themselves** that those services or projects are delivering (or will deliver), and will continue to deliver, an acceptable level of safety"

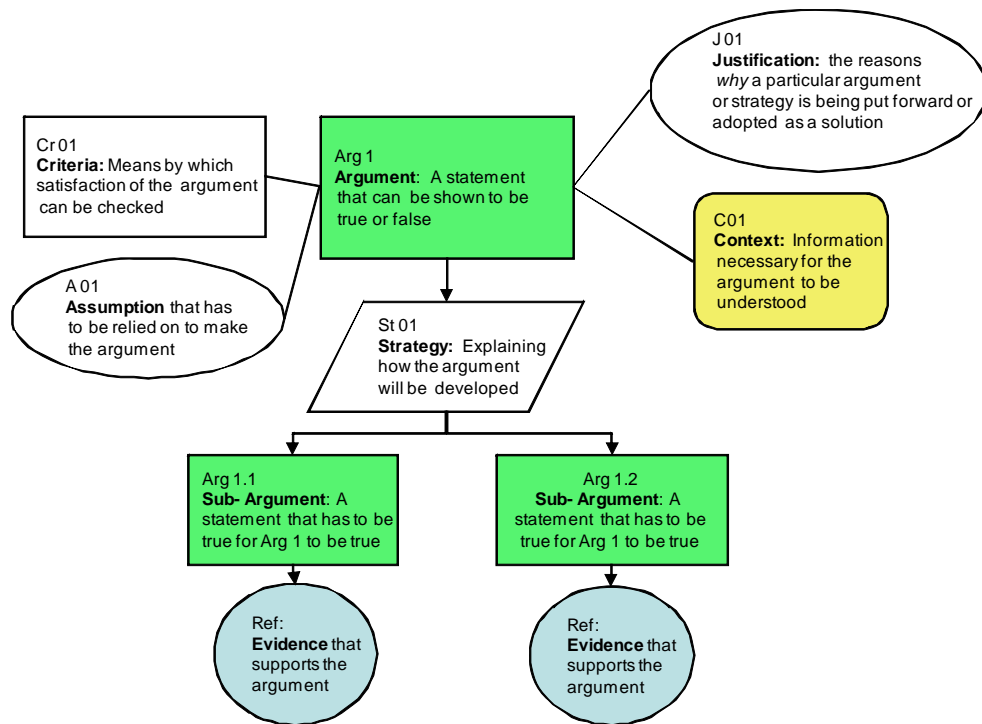


FIGURE 1: GOAL-STRUCTURING NOTATION SYMBOLS

4.3 Overall Argument structure

The overall safety argument is structured as shown in Diagram A below. The sub-arguments are mapped on to the MSAW development phases from definition through to operation and maintenance. This is to enable the planned safety assurance activities to be linked closely to the MSAW development and the safety case development. Each of the arguments has to be satisfied in order to make a safety case.

Arg 0, the top-level argument, is dependent on the following four-part argument comprising Arg 1 to Arg 4: The sub-arguments are developed in Diagrams B1 to B4, as indicated.

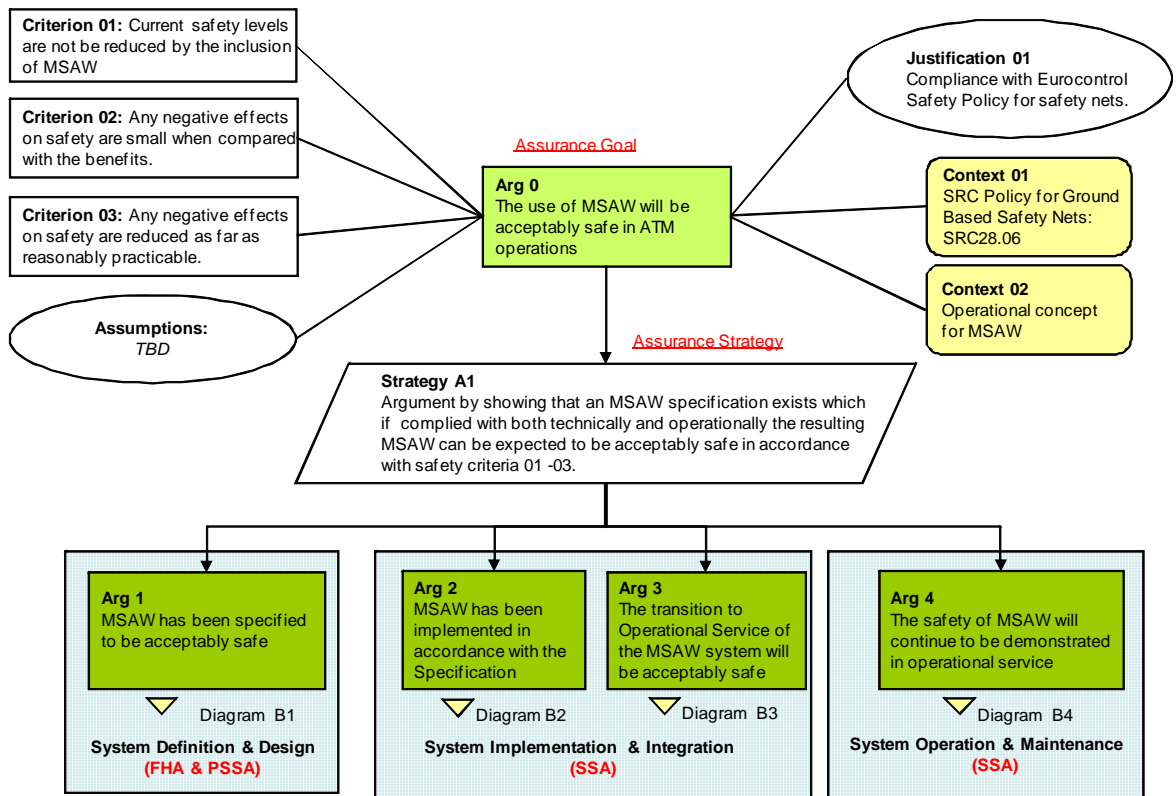


DIAGRAM A MAIN ARGUMENT STRUCTURE

4.4 Top Level Argument [Arg 0]

The top-level argument is that “MSAW will be acceptably safe in ATM operations”. The underlying argument structure is the means by which the supporting evidence is linked to the top-level argument.

4.5 Safety Criteria²

The criteria for deciding what will constitute “acceptably safe” in making the argument have to be established at the outset [Ref Safety Plan 7.1.1].

The first safety criterion (CRITERION 01) adopted is that “current levels of safety are not reduced by the inclusion of MSAW” *i.e. there is no net increase in the number of incidents above current levels as result of installing and operating MSAW.*

Note: Criterion 01 cannot be shown to be met until MSAW has been implemented.

² The specification of what is acceptable or tolerable in terms of risk [Ref EUROCONTROL SCDM]

The second safety criterion, (**CRITERION 02**) is that “any negative effects on safety shall be small compared with the safety benefit *i.e. that the number of incidents contributed to by MSAW is small compared to the number resolved by ATC as a result of an MSAW Alert.*

The third safety criterion, (**CRITERION 03**) is that “any negative effects on safety are reduced as far as reasonably practicable *i.e. this criterion points to the need to include mitigation means to ensure that the number of incidents contributed to by MSAW is small, and consistent with the requirements of criterion 02.*

These safety criteria provide a basis for a relative safety argument whereby the safety benefit should significantly outweigh the negative effects. It is a matter for ANSPs to determine what is acceptable in this regard for their implementation of MSAW.

4.6 Context

In addition to meeting the above safety criteria, MSAW will also need to be deemed acceptably safe in relation to the SRC Policy for Safety Nets [Ref Safety Plan 7.1.2].

4.6.1 Context 01 Safety Policy for MSAW

The EUROCONTROL Safety Regulation Commission (SRC) acknowledges that ground based safety nets are part of the ATM system and contribute positively to its safety. As MSAW is classed as a ground based safety net, this policy is relevant to ANSPs planning to implement MSAW.

4.6.2 Context 02 Concept of Operation for MSAW

An essential prerequisite for developing a safety argument for MSAW is the existence of a documented Concept of Operation (Conops) which describes the functionality, performance and uses of MSAW. The argument for MSAW is developed taking account of the Conops and the associated requirements specified in the EUROCONTROL Specification

4.7 Assumptions

Any assumptions on which the safety case is dependent should be stated e.g. the host surveillance system is acceptably safe [Ref Safety Plan 7.1.3].

4.8 Justification 01

Arg 0 is justified on the basis that MSAW should comply with EUROCONTROL safety policy for safety nets.

4.9 Strategy

The main strategy adopted to meet Arg 0 is based on showing that if a correct MSAW specification exists, and is complied with both technically and operationally, the resulting MSAW can be expected to be acceptably safe in accordance with safety criteria 01 - 03. This is dependent on satisfying four Arguments (Arg 1 to Arg 4). The four arguments are decomposed into sub-arguments as shown in Diagrams B1 to B4.

4.10 Assurance Objectives

Each of the sub-arguments in Diagrams B1 to B4 points to a Table which contain a set of assurance objectives to be addressed³ and for which evidence is required in order to satisfy the related Argument [Note this format is different to conventional GSN diagrams where the sub-arguments terminate in an evidence bubble - as shown in figure 1. In this document the assurance objectives are used to link the arguments to the evidence]. An example of the evidence required is given in each Table. [Note these are provisional lists, and ANSPs will need to adapt them for their own use]

5. MSAW SPECIFICATION AND SAFETY REQUIREMENTS

5.1 Introduction

The basic operational requirements for MSAW are established during the system definition phase.

- The Conops 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 requirements⁴ to enable the Conops are specified and a preliminary design of the system is determined which can reasonably be expected to meet them. The functional and non-functional requirements are regarded as safety requirements in this argument as they relate to how safe MSAW needs to be in the absence of failure. Note: These safety requirements are distinct from and in addition to those derived under Arg 1.5.

³ Assurance issues based on the EUROCONTROL document Safety Assessment Made Easier [Ref 6]

⁴ **Functional requirements** specify what the system should do. **Non-functional requirements** specify how a system must behave; they are a constraint upon the systems behaviour. Typical non-functional requirements are performance, throughput, utilisation etc.

- A Functional Hazard Assessment FHA and risk assessment is carried out to identify hazards that might impact on the design of the system. Safety objectives and safety requirements are derived for the system and mitigation for identified hazards determined.
- Human factor issues are highlighted and training requirements are identified. ATC and Engineering procedures are specified.

5.2 MSAW has been specified to be acceptably safe [Arg 1]

Evidence is required from the system definition and design phase to demonstrate that **Arg 1** can be considered to be true i.e. that MSAW has been specified to be acceptably safe; “acceptably safe” in this context means that it will satisfy criteria 01 - 03.

The strategy followed to show that **Arg 1** can be considered to be true is shown in **Diagram B1**, together with sub arguments (Arg 1.1 to Arg 1.7) for which supporting evidence are required. Note: Diagram B1 does not represent a sequential set of lifecycle activities; it is a diagram of the argument structure.

Arguments 1.1 to 1.4 are concerned with the *success* of MSAW in contributing to ATM safety i.e. in addressing pre-existing hazards. The specified functional and non-functional requirements for MSAW determine how safe it needs to be in the absence of failure and are therefore regarded as MSAW safety requirements. Note: As stated previously, these safety requirements are distinct from, and in addition to, those derived under argument 1.5 below.

Argument 1.5 is concerned only with the consequences of failure of MSAW (i.e. new hazards) and leads mainly to a specification of Safety Objectives⁵ and Safety Requirements⁶ for the integrity of the system.

⁵ Safety Objectives is a term used in ESARR 4 and in EUROCONTROL Safety Assessment Methodology to describe the maximum tolerable occurrence rate of hazards.

⁶ Safety Requirements refer to the mitigation means for hazards

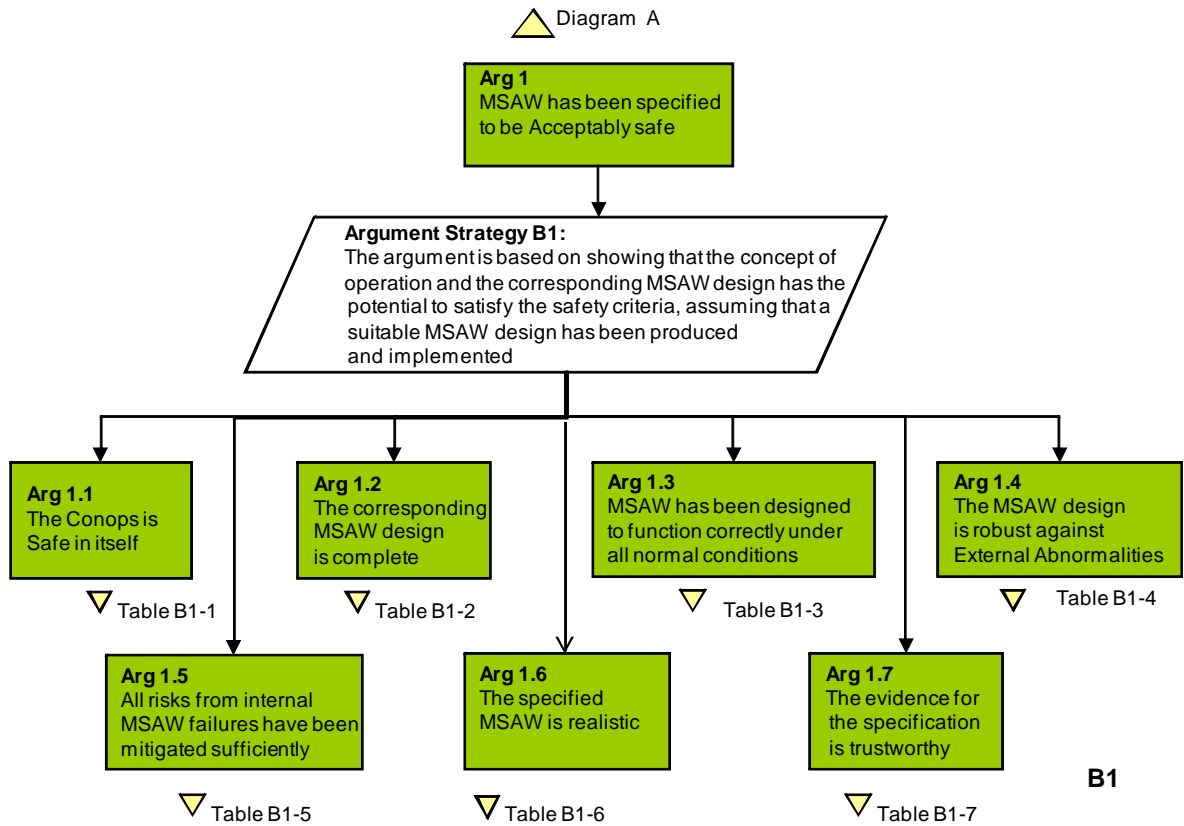


DIAGRAM B1 MSAW SPECIFICATION ARGUMENT

5.3 The Conops is safe in itself [Arg 1.1]

The issue here is whether the basic idea underlying the Concept has the potential to be safe – i.e. whether the Concept is capable of satisfying the safety criteria, assuming that a suitable system design could be produced and implemented – and what the minimum parameters are that would enable it to be safe. The following assurance objectives should be addressed and evidence to support them provided:

Arg 1.1: Assurance Objectives	Example Evidence
(1) Show that initial safety issues have been identified and addressed.	A draft Conops has been subject to formal review and modified to mitigate any hazards identified.
(2) Show that the minimum functionality has been defined and shown to be compatible with safety criteria 02 and 03.	Functionality to mitigate any negative effects on safety has been specified to reduce these as far as reasonably practicable e.g. alert inhibition function.
(3) Show that any differences from the existing Conops have been described, in	The “existing operation” referred to here is the non-MSAW ATM operation. The

terms of what MSAW will do when introduced into the ATM system.	Conops describes what MSAW will do when introduced into the system e.g. the ATC procedures are changed to specify controller action when an MSAW alert is received.
(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 safety criteria 02 and 03.	A draft Conops has been subject to formal review and modified to take in to account interfaces with adjacent systems and airspace e.g. coordination procedures with adjacent sectors.

TABLE B1-1: Arg 1.1 – Assurance Objectives

5.4 The corresponding MSAW design is complete [Arg 1.2]

The issue here is whether everything necessary to achieve a safe implementation of the Conops has been specified. The following assurance objectives should be addressed and evidence to support them provided [Ref Safety Plan 7.1.5]:

Arg 1.2: Assurance Objectives	Example Evidence
(1) Show that everything necessary to achieve a safe implementation of the Conops – related to the human, procedure, equipment and airspace design - has been specified.	A formal review has been carried out to ensure that the specification is complete and covers all aspects of the MSAW design e.g. Traceability to the Conops can be demonstrated.
(2) Show that all the requirements on, and assumptions about, external elements of the MSAW have been captured.	The MSAW specification has been formally reviewed to ensure that it covers external elements of MSAW, e.g. the host Radar Data Processing system.

TABLE B1-2: Arg 1.2 – Assurance Objectives

5.5 MSAW has been designed to function correctly under all normal conditions [Arg 1.3]

The ultimate aim is to show that all the functional and non functional safety requirements have been translated into design requirements and implemented successfully. Some ANSPs may have a complete MSAW design available at this phase of the development lifecycle; others may only have an outline design and MSAW description, with the intention of carrying out the detailed design during the Implementation and Integration phase. In either case, the following assurance objectives should be addressed and supporting evidence should be provided [Ref Safety Plan 7.1.6]. Note: For the purposes of this guidance material it is assumed that only an outline design is available at this

stage, but that the level of detail is sufficient to support the FHA process, and the derivation of safety objectives for the overall design.

Arg 1.3: Assurance Objectives	Example Evidence
(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.	Results of analysis of a documented description of the design.
(2) Show that the level of detail is sufficient to support the FHA process and the derivation of safety objectives for the overall design.	Results of analysis of a documented description of the design.

TABLE B1-3: Arg 1.3 – Assurance Objectives

5.6 The MSAW design is robust against external abnormalities [Arg 1.4]

The assurance issue here is whether MSAW can continue to operate effectively under abnormal conditions in the operational environment or can such conditions cause the system to behave in a way that could actually induce a risk that would otherwise not have arisen. The following assurance objectives should be addressed and supporting evidence provided [Ref Safety Plan 7.1.7].

Arg 1.4: Assurance Objectives	Example Evidence
(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.	This is under the scope of the FHA activities carried out under Arg 1.5 and may extend to the ATM boundary e.g. Errors in published charted IFR minimum altitudes.
(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.	A scenario-analysis has been carried out to identify the abnormal conditions that MSAW might encounter e.g. effect of radar ghosting whereby a multipath signal return incorrectly appears to the radar receiver as a valid target.

TABLE B1-4: Assurance Objectives

5.7 All risks from internal MSAW failures have been mitigated sufficiently [Arg 1.5]

Argument 1.5 leads mainly to a specification of safety objectives and safety requirements for the integrity of the MSAW. The assurance issue is to ensure that any negative effects on safety are reduced as far as reasonably

practicable (safety criterion 03). To do this it is first of all necessary to identify the hazards, if any, which can result from functional failures of MSAW. The process involves taking each of the specified functional requirements and subjecting them to a Functional Hazard Assessment FHA. The requirements for conducting an FHA are clearly set out in the EUROCONTROL SAM. The results of the FHA are used to determine the safety objectives. [Ref Safety Plan Table 7.1.8]

The next step is to derive the safety requirements. These are derived by taking each of the hazards identified and investigating how they might be caused. The causes will likely include some or all of the following:

- hardware and software failures,
- human error – errors of omission and commission by ATCOs and engineers
- Procedure failures – errors in design or application.

Fault Tree Analysis (FTA) is one formal method for investigating the causes of hazards. The following assurance objectives should be addressed and supporting evidence provided:

Arg 1.5: Assurance Objectives	Example Evidence
(1) Show that all reasonably foreseeable hazards, at the boundary of the MSAW, have been identified	Results of the FHA Process [Ref EUROCONTROL SAM ⁷] e.g. Hazard: MSAW does not reliably capture and direct controllers attention to potentially hazardous situations
(2) Show that the severity of the effects from each hazard has been correctly assessed, taking account of any mitigation that may be available / could be provided external to the MSAW.	Results of the FHA Process e.g. Effect: The controller may not become aware of some potential CFIT and there may be a proportionate increase in the number of CFIT resolved by the pilot or providence.
(3) Show that the Safety Objectives have been set for each hazard such that the corresponding aggregate risk is within the specified safety criteria	Results of the FHA Process for setting Safety Objectives. e.g. The probability of impaired functionality affecting the reliability MSAW shall be no greater than <i>TBD per year/flight hour</i>
(4) Show that all reasonably foreseeable causes of each hazard have been identified	Results of the FTA Process e.g. The potential cause of (2) above: Alerts inadvertently inhibited in relevant airspace.

⁷ EUROCONTROL Safety Assessment Methodology

(5) Show that 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	Preliminary results from the PSSA process e.g. Safety Requirement: The probability that the alert inhibition process compromises the MSAW function shall be <i>TBD per year/flight hour</i>
(6) Show that the safety requirements have been verified and validated.	Results from PSSA process e.g. The Human Machine Interface (HMI) for the alerting mechanism has been validated by controllers in the operational environment.
(7) Show that all external and internal mitigations have been captured as either safety requirements or assumptions as appropriate	Results from PSSA process e.g. The safety requirements have been shown to be consistent with the mitigations derived during the FHA e.g. (2) & (5) above.
(8) Show that MSAW can actually operate safely under all degraded modes of operation identified under this Argument	Results of scenario modelling in the PSSA e.g. the effects of loss of mode C radar or mode S where used.

TABLE B1-5: Arg 1.5 – Assurance Objectives

5.8 The specified MSAW is realistic [Arg 1.6]

The assurance issue here is to verify and validate the requirements with a view to determining the required integrity for the MSAW elements concerned. This is only feasible if the requirements are realistic. The following assurance objectives should be addressed and supporting evidence provided [Ref Safety Plan 7.1.9]:

Arg 1.6: Assurance Objectives	Example Evidence
(1) Show that all hazard related aspects of the MSAW design have been captured as safety requirements or (where applicable) as Assumptions	Review of the design with respect to the safety requirements
(2) Show 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.	Suitable test cases have been designed to show the effectiveness of the alerting mechanism.
(3) Show that all safety requirements are capable of being satisfied in a typical implementation in hardware, software, people and procedures.	Expert opinion that the alerting mechanism design and operation is similar to that proven for use in other MSAW systems.

(4) Show that all assumptions have been shown to be valid.	Assumptions made at the outset of the project can be confirmed in practice e.g. radar coverage.
--	---

TABLE B1-6: Arg 1.6 – Assurance Objectives

5.9 The evidence for the safety specification is trustworthy [Arg 1.7]

The assurance issue is to provide backing evidence that the evidence supporting the arguments 1.1 to 1.6 is trustworthy. The following assurance objectives should be addressed and supporting evidence provided [Ref: Safety Plan 7.1.10]

Arg 1.7: Assurance Objectives	Example Evidence
(1) Confirm that the assurance processes, tools and techniques used were adequate for the task	Expert opinion that the modelling scenarios used were consistent with those described EUROCONTROL Guidance Material for Minimum Safe Altitude Warning Appendix A: Reference MSAW System [Ref.2]
(2) Confirm that the competence of the people using them was adequate for the task	Confirmed by expert opinion and review of the analytical results.

TABLE B1-7: Arg 1.7 – Assurance Objectives

6. MSAW COMPLIANCE WITH THE SAFETY REQUIREMENTS

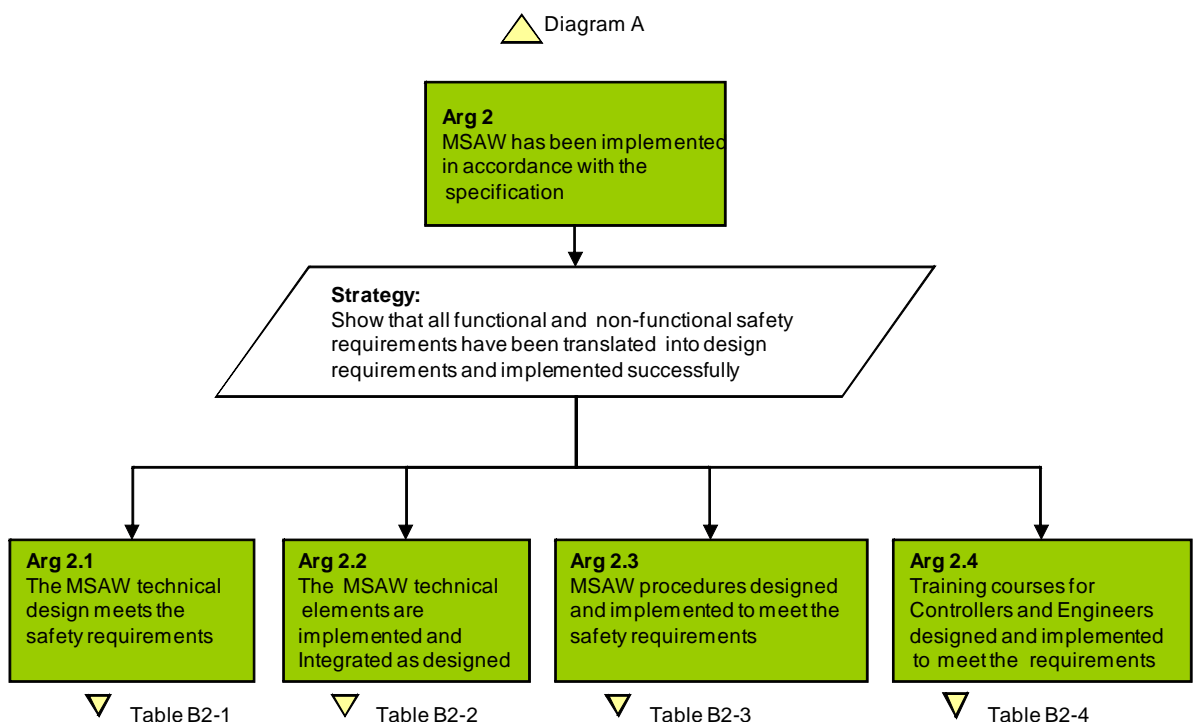
6.1 Introduction

The detailed design of MSAW is completed during the system implementation and integration phase of the lifecycle. All the elements of MSAW are developed and integrated into the ATM system i.e. people, procedures and equipment. Any hazards arising from the planned transfer of MSAW to operation are identified and appropriate mitigation put in place. All the resources necessary to operate MSAW are put in place.

6.2 MSAW has been implemented in accordance with the specification [Arg 2]

6.2.1 Strategy

The strategy is to show that all functional, non-functional and safety requirements have been translated into design requirements and implemented successfully. This requires that evidence is available to satisfy the sub arguments 2.1 to 2.4 as shown in Diagram B2 below:



B2

DIAGRAM B2 – SYSTEM IMPLEMENTATION AND INTEGRATION ARGUMENT

6.3 The MSAW technical design meets the safety requirements [Arg 2.1]

The assurance issue is to show that that the design is complete and correct. The design can only be reviewed for completeness and correctness if it is fully documented. The following assurance objectives should be addressed and supporting evidence provided [Safety Plan Ref: 7.2.1]:

Arg 2.1: Assurance Objectives	Example Evidence
(1) Confirm that the design requirements interpret the specification completely and correctly.	Results of review showing that all the safety requirements can be traced in the design requirements.
(2) Confirm that the design is documented and under configuration control.	Results of review showing that the design is documented to a known build state and version number.
(3) Confirm that the design incorporates all the safety requirements, completely and correctly.	Results of review showing that all the design requirements can be traced in the design.

TABLE B2-1: Arg 2.1 – Assurance Objectives

6.4 The MSAW technical elements are implemented and integrated as designed [Arg 2.2]

Assurance that the technical elements have been implemented in accordance with the design will be intimately dependent on the actual design, the implementation and the processes. Assurance is likely to be made up of evidence from the engineering processes followed, the results of testing, and controller-in-the-loop simulations. The following assurance objectives should be addressed and supporting evidence provided [Safety Plan Ref: 7.2.2]:

Arg 2.2: Assurance Objectives	Example Evidence
(1) Confirm that the MSAW meets the specified functional and non functional safety requirements.	Evaluation results (tracing to evidence for each Functional and Non-Functional requirement) show that the number of nuisance alerts identified during functional testing is within acceptable limits.
(2) Confirm that the MSAW functions correctly and coherently under all normal conditions.	Results of test cases and controller-in-the-loop simulations confirm that MSAW operates in accordance with the Conops under all reasonably foreseeable normal conditions.
(3) Confirm that the MSAW is robust against external abnormalities.	Evaluation results e.g. simulation of loss of mode s radar.

TABLE B2-2: Arg 2.2 – Assurance Objectives

6.5 MSAW procedures are designed and implemented to meet the safety requirements [Arg 2.3]

Procedures should be designed taking full cognisance of the operator's point of view and related human factor issues and with limited scope for ambiguity in understanding. Poorly designed ATC operational procedures and engineering maintenance procedures can be a contributory factor in incidents. The following assurance objectives should be addressed and supporting evidence provided:

Arg 2.3: Assurance Objectives	Example Evidence
(1) Confirm that the Procedures have been designed to meet the safety requirements	A documented procedure to ensure that Controllers shall be advised of any changes to the ATM system that might degrade the performance of MSAW identified during the FHA e.g. relocation of holding patterns.
(2) Confirm that the procedures have been implemented.	Procedure is formally published and acknowledged by those affected by it.
(3) Confirm that the Controllers and Engineers are trained and competent to operate MSAW and procedures.	As evidenced from training records.

TABLE B2-3: Arg 2.3 – Assurance Objectives

6.6 Training Courses for Controllers and Engineers designed and implemented to meet the safety requirements [Arg 2.4]

The assurance issue is to show that any training necessary for controllers or engineers to be able to operate and maintain the MSAW equipment has been identified, appropriate training courses developed and that staff has successfully completed those courses [Safety Plan 7.2.4]. The following assurance objectives should be addressed and supporting evidence provided:

Arg 2.4: Assurance Objectives	Example Evidence
(1) Confirm that the Training Courses have been designed to meet the safety requirements	Review of ATC Training course material on operation of MSAW
(2) Confirm that the Training Courses have been implemented.	Records showing all relevant ATC staff trained

TABLE B2-4: Arg 2.4 – Assurance Objectives

6.7 Transition to operational service of MSAW will be acceptably safe [Arg 3]

The strategy is to show that the existing ATM system will not be put at risk during the transition to operation of MSAW and that all the resources necessary for the safe operation of the MSAW are in place – people, procedures and equipment. It is important therefore that an assessment is made to identify any potential hazards that might need to be mitigated during that phase of activity. [Ref Safety Plan 7.3.1]

The ANSP will want assurance that MSAW is reliable; it should be at least as reliable as the host radar system in order to maximise the safety benefit. The ANSP will also want assurance that ATC is happy with it; that the necessary staff are trained and competent; that the regulator will approve it and that there are no outstanding issues that could impact on the safety of operations. Such assurance should be readily available in the safety case.

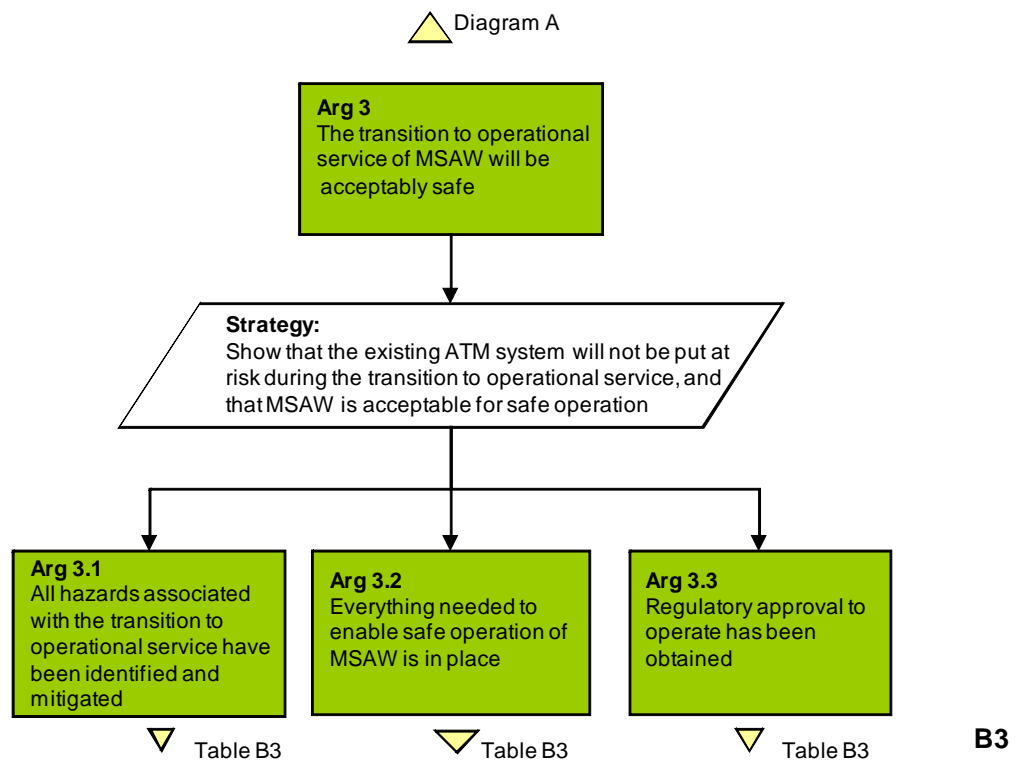


DIAGRAM B3 - SAFE TRANSITION TO OPERATIONAL SERVICE

The following assurance objectives should be addressed and supporting evidence provided:

Arg 3: Assurance Objectives	Example Evidence
(1) Confirm that the Safety requirements for the transfer to operation have been specified	Table of Safety Requirements derived during transition-in-to-operations hazard analysis e.g. The safety of ATC surveillance operations shall not be compromised during the installation of MSAW in the ATM system.
(2) Confirm that the System reliability and integrity accepted as meeting the safety requirements.	The results of functional and non functional testing and analysis are consistent with the safety requirements and are accepted.
(3) Confirm that the HF and HMI accepted as satisfactory	Verified by ATC during operational trials (Results).
(4) Confirm that the sufficient trained staff available to operate and maintain the system.	As agreed between management, ATC and engineering.
(5) Confirm that the Procedures published and promulgated to all relevant staff.	Confirmed by publication records.
(6) Confirm that the Operational validation trials satisfactory	Confirmed by trials reports
(7) Confirm that the System shortcomings highlighted and accepted for operation.	Current performance not sufficient to support MSAW operations in holding patterns e.g. shortcomings are documented and accepted by ATC management.
(8) Confirm that the Regulatory approval to operate obtained.	Written approval received

TABLE B3: Arg 3 – Assurance Objectives

7. SYSTEM OPERATION AND MAINTENANCE

7.1 The safety of MSAW will continue to be demonstrated in operational service (Arg 4)

The strategy is to show that the operating and maintenance procedures are followed correctly, the system is maintained and its performance is monitored to ensure that the safety objectives continue to be met. MSAW performance monitoring and analysis is a key issue in ensuring that MSAW meets and continues to meet the safety criteria set down at the outset. Managers must ensure that the system remains optimised for its role and keeps pace with ever changing operational requirements. They should also ensure that ATC behaviour in operating the system is consistent with ANSP MSAW policy as well as not being compromised by system performance. [Ref Safety Plan 7.4.1]

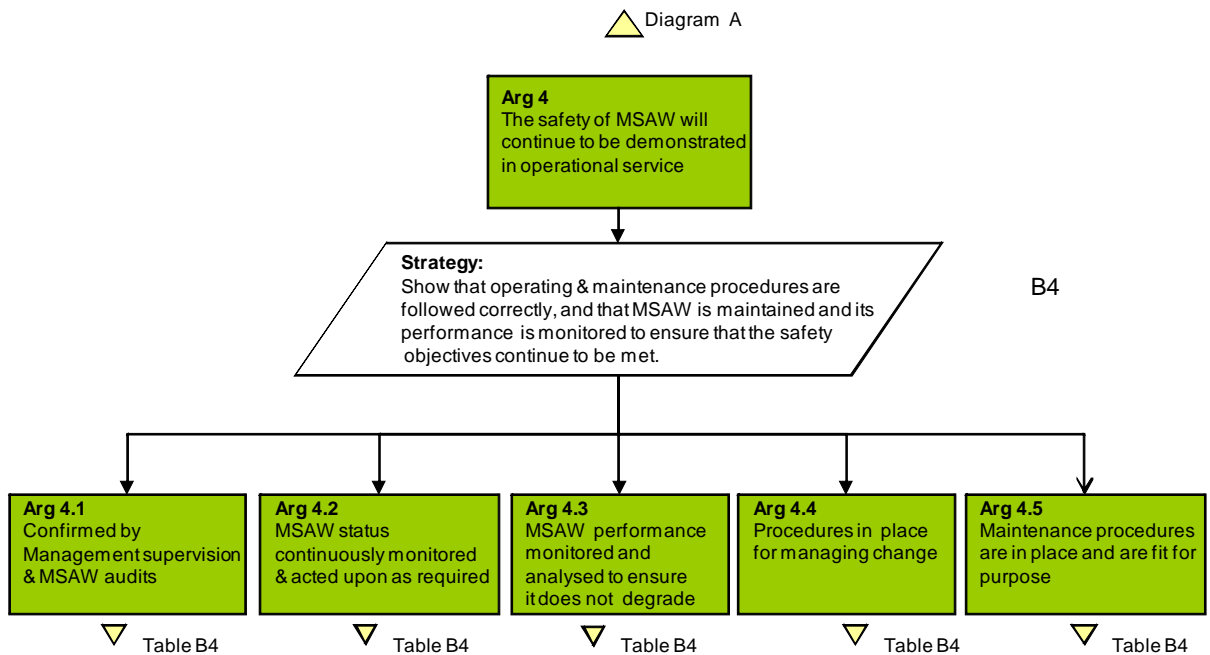


DIAGRAM B4 - SAFETY IN OPERATIONAL SERVICE

The following assurance objectives should be addressed and supporting evidence provided:

Arg 4: Assurance Objectives	Example Evidence
(1) Confirm that the Staff have been assigned with the responsibility for management of MSAW (to fulfil the above functions)	ANSP organisation: Engineering staff member assigned responsibility for managing MSAW design and for changes to MSAW data sets and algorithms.
(2) Confirm that the a formal process exists for monitoring MSAW Status	Manual of ATC: The ATC supervisor is alerted about all MSAW failures and takes action accordingly.
(3) Confirm that the a formal process exists for monitoring MSAW and analysing the results	Documented Procedure: Recorded MSAW data is subjected to periodic off-line analysis in order to determine if the performance has degraded.
(4) Show that the MSAW remains optimised for its ATM role and keeps pace with changing operational requirements.	Documented MSAW data sets are consistent with current operational environment.
(5) Show that ATC are advised of any MSAW changes that might affect the safety performance	Manual of ATC: ATC supervisor to promulgate changes and to advise ATC how these might impact on operations.
(6) Show that MSAW maintenance procedures are in place and are fit for purpose	Documented procedures for updating MSAW software.

TABLE B4: Arg 4 – Assurance Objectives

8. 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

9. REFERENCES

1. EUROCONTROL Specification for Minimum Safe Altitude Warning.
2. EUROCONTROL Guidance Material for Minimum Safe Altitude Warning; Appendix A: Reference System.
3. Generic Safety Plan for MSAW implementation.
4. SCDM: EUROCONTROL Safety Case Development Manual, Edition 2.2.
5. SRC Action paper SRC28/06. SRC Policy on Ground Based Safety Nets.
6. Safety Assessment Made Easier Version 0.92
7. EUROCONTROL ESARR 4 – Risk Assessment and Mitigation, Edition 1.0

END OF DOCUMENT