EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

A-SMGCS Levels 1 & 2 Guidance Material in support of the Preliminary Safety Case

Edition Number	**:**	**1.0**
Edition Date	**:**	**September 2005**
Status	**:**	**Released Issue**
Intended for	**:**	**General Public**

EUROPEAN AIR TRAFFIC MANAGEMENT PROGRAMME

DOCUMENT CHARACTERISTICS

TITLE		
A-SMGCS Levels 1 & 2 Guidance Material in support of the Preliminary Safety Case		
	EATMP Infocentre Reference:	07/01/09-02
Document Identifier	**Edition Number:**	1.0
	Edition Date:	September 2005

Abstract

This documents presents guidance on the use of the EUROCONTROL preliminary safety case for the A-SMGCS Levels 1 and 2 concept.

Keywords

Surveillance Airport Multi-lateration Safety

Contact Person(s)	Tel	Unit
Paul ADAMSON	+32 2 729 3308	DAP/AOE

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

ELECTRONIC SOURCE		
Path:	C:\Documents and Settings\dupwood\Desktop On HBRUWA52A	
Host System	Software	Size
Windows_NT	Microsoft Word 10.0	375 Kb

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

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

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

DOCUMENT APPROVAL

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

AUTHORITY	NAME AND SIGNATURE	DATE
Please make sure that the EATMP Infocentre Reference is present on page ii.		
Project Manager	Chris MACHIN	
A-SMGCS Project Manager	Paul ADAMSON	
Airport Operations Programme Manager	Eric MIART	
Head of AOE Division	Paul WILSON	

DOCUMENT CHANGE RECORD

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

EDITION NUMBER	EDITION DATE	INFOCENTRE REFERENCE	REASON FOR CHANGE	PAGES AFFECTED
1.0	Sep 2005		Project Team Review	All

CONTENTS

DOCUMENT CHARACTERISTICS ii

DOCUMENT APPROVAL iii

DOCUMENT CHANGE RECORD iv

1. INTRODUCTION 1

1.1 Background 1

1.2 EUROCONTROL A-SMGCS Safety Activities 1

1.3 Aim 2

1.4 Scope and Limitations 2

1.5 Structure of the Document 2

1.6 Points of Contact 3

2. SAFETY ROLES AND RESPONSIBILITIES – EUROCONTROL AND STATES 4

2.1 Introduction 4

2.2 Safety Lifecycle 4

2.3 Roles and Responsibilities by Lifecycle Stage 6

3. GUIDANCE TO A-SMGCS IMPLEMENTERS ON THE USE OF EUROCONTROL FHA/PSSA 8

3.1 Introduction 8

3.2 Derivation of a Target Level of Safety for A-SMGCS 9

3.3 Derivation of Severity Classification Scheme 10

3.4 Definition of Architecture and Operating Procedures 11

3.5 Identify Hazards 13

3.6 Safety Objective Development 15

3.7 Safety Requirements Development 17

4. SYSTEM SAFETY ASSESSMENT 18

4.1 Introduction 18

4.2 SSA 18

4.3 Avionics 19

4.4 Sensor Performance 20

4.5 Historical Evidence 20

4.6 Reliability Analysis 21

4.7 Monitoring of System Performance....21
4.8 Incident Reporting and Analysis 21

5. GUIDANCE TO A-SMGCS IMPLEMENTERS ON THE DEVELOPMENT OF A FULL SAFETY CASE 22

5.1 Introduction 22
5.2 A-SMGCS Safety Argument 22

6. REFERENCES....28

1. INTRODUCTION

1.1 Background

1.1.1

Safety Cases provide documented assurance (i.e. argument and supporting evidence) of the achievement and maintenance of safety. They are primarily the means by which those who are accountable for **service provision** (and/or projects that introduce **change** to that service or underlying systems) assure themselves that those services (or projects) are delivering (or will deliver), and will continue to deliver, an acceptable level of safety.

1.1.2

As the main objective of safety regulation is to ensure that those who are accountable for safety discharge their responsibilities properly, then it follows that Safety Cases which serves the above primary purpose should also (but secondarily) provide an adequate means of obtaining regulatory approval for the service or project concerned.

1.2 EUROCONTROL A-SMGCS Safety Activities

1.2.1

EUROCONTROL has carried out a safety assessment (FHA and PSSA) of A-SMGCS (Level 1 and 2) and has produced a Preliminary Safety Case to show that the A-SMGCS (Level 1 and 2) Concept is acceptably safe in principle – ie subject to complete and correct implementation of the related set of Safety Requirements.

1.2.2

Of necessity, the EUROCONTROL FHA/PSSA is based on a generic application of A-SMGCS, and the associated Preliminary Safety Case **[1]** is limited to EUROCONTROL's sphere of responsibility – i.e. to demonstrating that the A-SMGCS Concept is inherently safe for that generic application.

1.2.3

Responsibility for the safety of the implementation of the A-SMGCS Concept for specific applications rests with the State ANSPs concerned, and this Guidance document has been produced to aid ANSPs in discharging their safety responsibilities and to ensure, as far as practicable, the consistent implementation of the A-SMGCS Concept.

1.2.4

The document is intended for use by those who have to:

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

1.3 Aim

1.3.1

The aim of this document is to provide guidance to States on conducting a safety assessment of, and producing a full Safety Case for, A-SMGCS Level 1 and 2.

1.4 Scope and Limitations

1.4.1

This document provides:

- an amplification of the scope of the A-SMGCS Preliminary Safety Case – i.e. what is, and what is not included;
- a delineation of the responsibilities between EUROCONTROL and the organisation(s) responsible for Implementation;
- instructions for the A-SMGCS Implementers concerning the use of the safety assessment results and other information in the Preliminary Safety Case
- guidance on the additional work needed to cover the Implementation, Migration and Operational phases in the full Project Safety Case.

1.4.2

It is assumed that users of this Guidance Material have an understanding of the EUROCONTROL SAM **[3]** and a technical and operational knowledge of A-SMGCS.

1.4.3

Whereas it will aid the process of developing and presenting a Safety Case, this document cannot give assurance of the validity of the end product, and it does not, therefore, relieve its users of their responsibility to provide such assurance.

1.5 Structure of the Document

1.5.1

Section 2 explains the relative roles and responsibilities, of EUROCONTROL and the States in the safety assessment and assurance of A-SMGCS, in relation to a typical project safety lifecycle.

1.5.2

Section 3 provides guidance to the Implementers of A-SMGCS on how to use the EUROCONTROL FHA and PSSA. It explains what they do and what the Implementer needs to review and revise and what can be reused.

1.5.3

Section 4 provides an overview of the activities required to complete a local system safety assessment. The PSC verified that the safety requirements are achievable using LHR as an example implementation. Implementers will need to complete a System Safety Assessment (SSA) as part of the local implementation.

1.5.4

Section 5 provides guidance to A-SMGCS Implementers on the development of a full Safety Case. It provides a top level safety argument and describes how the Eurocontrol PSC can be used to support the development of a local Safety Case.

1.5.5

Section 6 provides references to the Guidance Material.

1.6 Points of Contact

1.6.1

Should you require further information regarding the A-SMGCS Preliminary Safety Case or this Guidance material please contact:

Mr Paul Adamson
A-SMGCS Project Manager
EUROCONTROL Headquarters
96 Rue de la Fusee
B-1130 Brussels

Tel: +32 (0)2 729 3308
Fax: +32 (0)2 729 9193
Email: paul.adamson@EUROCONTROL.int

2. SAFETY ROLES AND RESPONSIBILITIES – EUROCONTROL AND STATES

2.1 Introduction

2.1.1

This section explains the relative roles and responsibilities of EUROCONTROL and the States in the safety assessment and assurance of A-SMGCS, in relation to a typical project safety lifecycle.

2.2 Safety Lifecycle

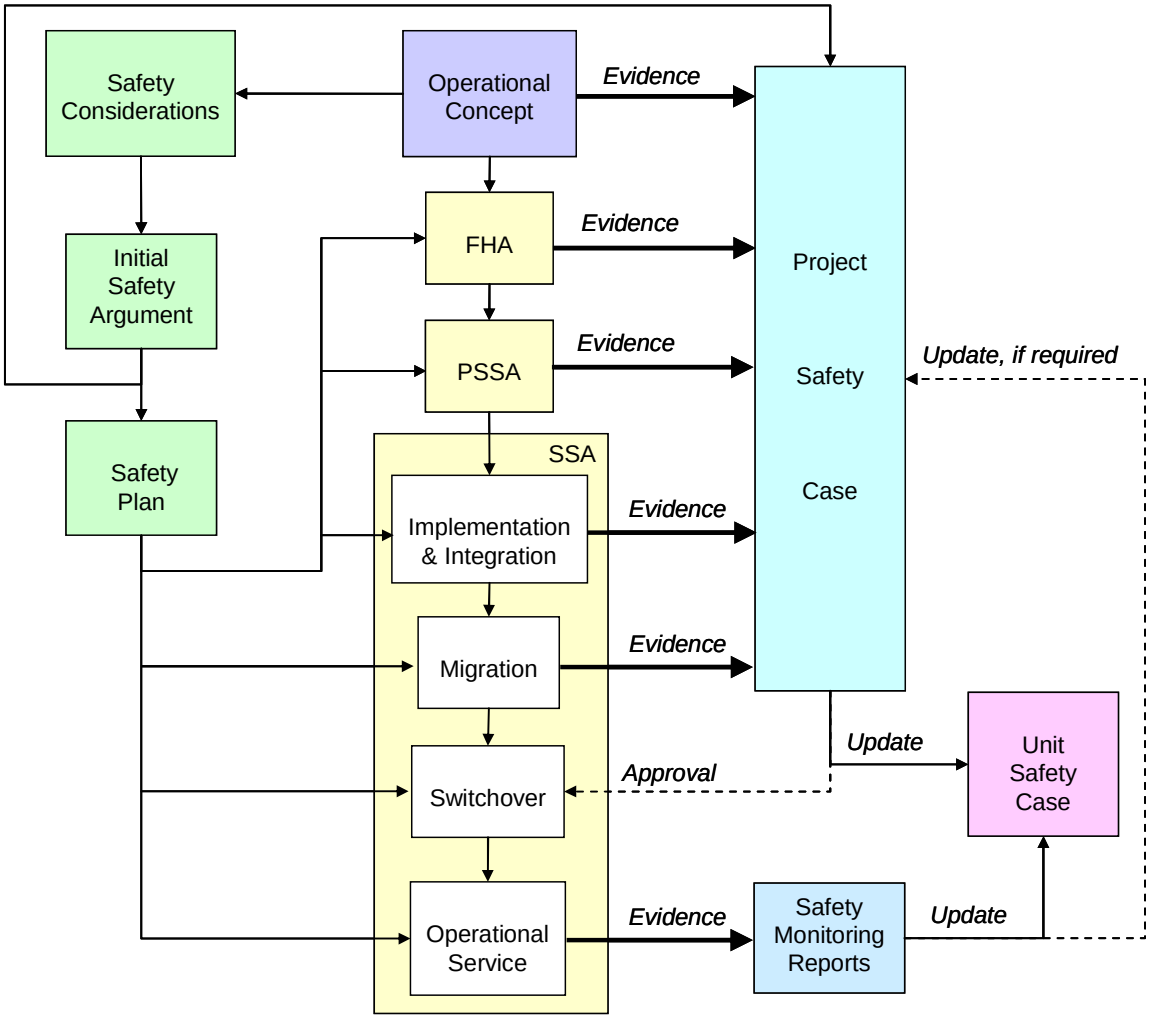

Figure 2-1: Stages in the Development of a Safety Case

2.2.1

A simplified view of a typical project lifecycle is shown in Figure 2-1 above.

2.2.2

Safety Considerations are the documented results of a EUROCONTROL process to identify, as soon as possible after a mature *Operational Concept* has been developed, the main safety issues associated with a Project and to help in deciding whether a full Safety Plan and Safety Case are required.

2.2.3

Building on the Safety Considerations, the initial *Safety Argument* should be as complete as possible and at least sufficient to form the basis of the Safety Plan. It also provides the starting point, and framework, for the development of the *Project Safety Case* – i.e. a Safety Case for a significant to the ATM service and/or underlying system.

2.2.4

The *Safety Plan* specifies the safety activities (mainly the gathering and assessment of Evidence) to be conducted throughout the project lifecycle and the allocation of responsibilities for their execution.

2.2.5

The three main phases of safety assessment – *Functional Hazard Assessment* (FHA), *Preliminary System Safety Assessment* (PSSA) and initial stages of *System Safety Assessment* (SSA) - provide much of the Evidence needed for the Project Safety Case.

2.2.6

Migration is the phase that covers all the preparation needed in order to bring the new / modified system – i.e. the subject of the Project Safety Case – into operational service, including risk assessment and planning for the moment of Switchover. Switchover of the operational service to the new/modified system would normally be preceded by finalisation and, where applicable, regulatory approval of the Project Safety Case.

2.2.7

Because most, if not all, of the preceding safety assessment work is predictive in nature, it is important that further assurance of the safety is obtained from what is actually achieved in operational service. If the operational experience differs significantly from the results of the predictive safety assessment, it may be necessary to review and update the Project Safety Case.

2.2.8

Once a satisfactory steady state has been achieved, it would be appropriate to update the Unit Safety Case (if one exists) with the information from the Project Safety Case thus establishing a new safety baseline for the on-going service.

2.2.9

Decommissioning of a system, at the end of its operational life, is not shown explicitly on Figure 2-1, but may be thought of as a special case of a change.

2.2.10

For many EUROCONTROL EATM Programmes, of which A-SMGCS is an example, EUROCONTROL is not responsible for implementation of the concept concerned. In those cases, EUROCONTROL would carry out a safety assessment up to and include the PSSA stage and would document the resulting assurance in a subset of the eventual Project Safety Case, known as a *Preliminary* Safety Case. The implementing authority would then be responsible for development of a full Project Safety Case, including carrying out all the steps in the SSA process.

2.3 Roles and Responsibilities by Lifecycle Stage

2.3.1

Table 2-2 below shows the division of roles and responsibilities between EUROCONTROL, as developer of the Concept at a generic level, and the States, as implementers of the Concept at a local level. It also provides internal and external references to where the related guidance can be found.

Activity	EUROCONTROL	States	Remarks
Safety Considerations	☒	☒	This is an internal EUROCONTROL process[1]
Safety Argument	☑	☑	The EUROCONTROL Preliminary Safety Case (see below) contains the structured Safety Argument for the initial safety assessment (FHA / PSSA) but only an outline for the SSA. The Implementer should confirm the former, and expand the latter, in relation to the specific implementation. Further guidance is given in section 5 and in **[1]**

[1] The early stages of the EUROCONTROL A-SMGCS Programme predated the introduction of this process – a Safety Considerations report was not therefore produced in the case of A-SMGCS

Safety Plan	☑	☑	EUROCONTROL produced a Safety Plan for its own purposes – the Implementer should do the same in relation to the specific implementation. Some guidance on this may be found in **[1]**
FHA	☑	☑	EUROCONTROL has completed an FHA for a 'generic' application of A-SMGCS. The Implementer should confirm the results including the Safety Objectives in the context of the specific implementation – see section 3.
PSSA	☑	☑	EUROCONTROL has completed PSSA, and produced a complete set of Safety Requirements, for a 'generic' application of A-SMGCS. The Implementer should confirm the results, including the Safety Requirements, in the context of the specific implementation – see section 3.
SSA – Implementation & Integration	☒	☑	Implementation & Integration are entirely the Implementer's responsibility; however, some guidance is given in section 4.
SSA – Migration	☒	☑	Planning and execution of the migration from the pre-A-SMGCS state to a fully operational A-SMGCS is entirely the Implementer's responsibility
SSA – Switchover	☒	☑	Planning and risk management of the switchover from the pre-A-SMGCS state to a fully operational A-SMGCS is entirely the Implementer's responsibility
SSA – Safety Monitoring in Operational Service	☑	☑	Some guidance is given in section 4.
Project Safety Case	☑	☑	EUROCONTROL has produced a Preliminary Safety Case containing the Safety Argument (see above) and Evidence for the generic FHA and PSSA (see above). The Implementer should confirm the information

			presented in the Preliminary Safety Case, and modify / expand it as necessary to produce a full Safety Case for the specific implementation – see section 5
Unit Safety Case	☒	☑	Unit Safety Cases, if produced, are entirely the Implementers' responsibility; however, some guidance on this is given in **[1]**

Table 2-2: Allocation of Roles and Responsibilities

3. GUIDANCE TO A-SMGCS IMPLEMENTERS ON THE USE OF EUROCONTROL FHA/PSSA

3.1 Introduction

3.1.1

This section describes guidance to the Implementers of A-SMGCS on how to use the EUROCONTROL A-SMGCS FHA / PSSA **[1]**. Further Guidance material on how to apply the process can be found in the EUROCONTROL Safety Assessment Methodology **[3]** and EUROCONTROL Safety Case Development Manual **[2]** although other processes may be applied as appropriate.

3.1.2

The use of the EUROCONTROL A-SMGCS FHA/PSSA includes a number of key aspects that require adapting to reflect local implementation and operations, as follows:

- The acceptable risk of an accident influenced by the A-SMGCS at the airport
- The relations between the different severity classes in the risk classification scheme
- The logical architecture of A-SMGCS
- The procedures applied for the use of A-SMGCS
- Safety Objectives development
- Safety Requirements development

3.1.3

The following flow chart depicts the FHA/PSSA process and provides references to the sections of the FHA/PSSA where relevant information is provided and to the subsequent paragraphs of the guidance material containing explanatory notes.

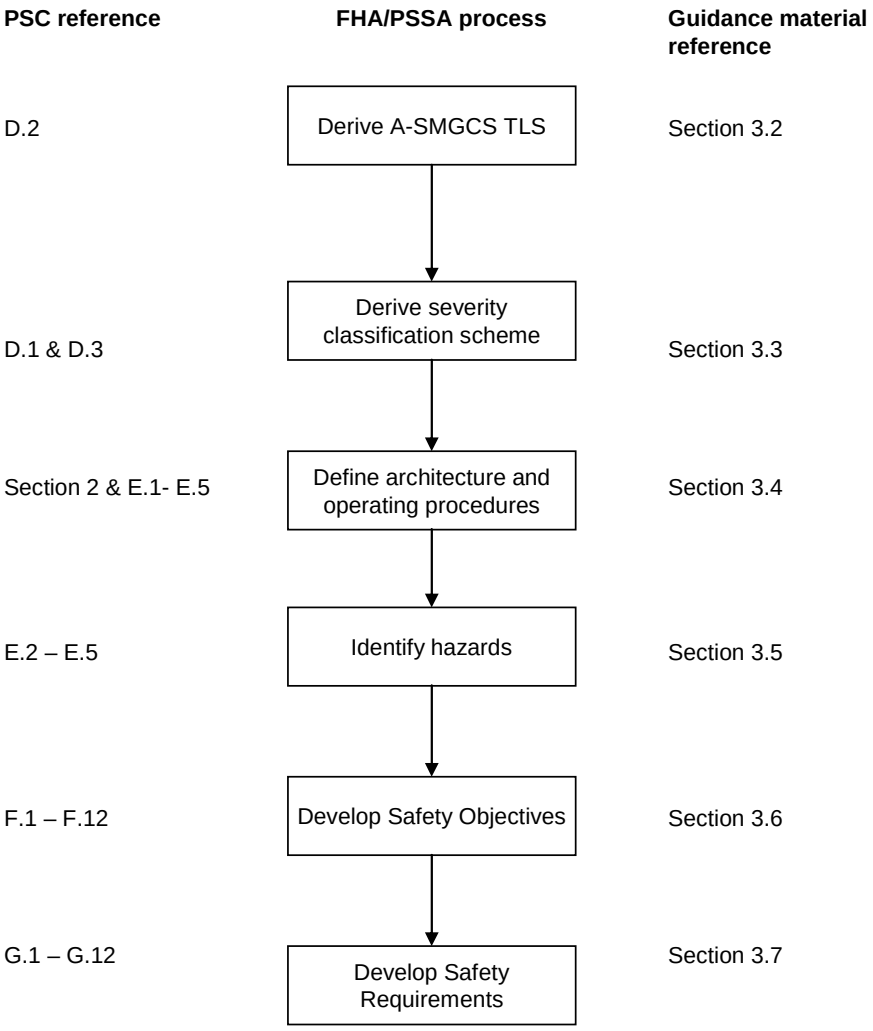

Figure 3-1: FHA/PSSA Process

3.1.4

Each of these items is discussed in the following paragraphs, with reference to the relevant sections of the EUROCONTROL FHA / PSSA Report.

3.2 Derivation of a Target Level of Safety for A-SMGCS

3.2.1

The target level of safety derived in the FHA/PSSA is based on SRC recorded accident rates for ECAC and was based upon the following assumptions:

- 90% of accidents occur at an aerodrome (taxi, missed approach, take-off, landing)
- 94% of accidents on the aerodrome are within the scope of SMGCS.

- 50% of accidents during take-off, missed approach and landing occur under the control of A-SMGCS
- The proportion of accidents per flight that A-SMGCS may influence in the future is 15%

3.2.2

The following figure shows the relationship between the maximum acceptable probability of ATM directly contributing to an accident of a commercial Air Transport aircraft and the TLS for A-SMGCS.

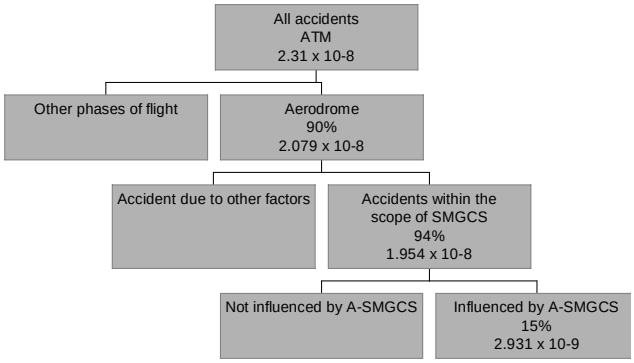

Figure 3-2: Derivation of A-SMGCS TLS

3.2.3

The TLS should be reviewed and aligned with the local aerodrome operations. The assumptions regarding proportion of accidents that occur within the scope of SMGCS and the proportion of those which may be influenced by A-SMGCS should be considered and validated or modified according to the local aerodrome operations.

3.2.4

Note that the units used to derive the TLS are probability of an accident per flight.

3.3 Derivation of Severity Classification Scheme

3.3.1

The severity classification scheme used in the PSC is derived from the EUROCONTROL SAM.

3.3.2

The relationship between each severity class is applied as illustrated in Table 3-1. The definitions used and accident probabilities were agreed by stakeholders participating in the safety workshops. A-SMGCS implementers should follow a similar process to develop a severity classification scheme or verify that this is applicable to their local airport.

Severity Class	Description	Relationship between classes	Probability of an accident if the incident occurs
5	No impact on safety		Not credible to discuss
4	Minor impact on workload or system functionality but all participants (i.e. controllers and aircrew) still believed the situation to be 'safe'	100	1 in 1000000 or 10^{-6}
3	Higher impact on workload or system functionality but one or more participants (i.e. controllers and aircrew) believed the situation to have moved from 'safe' to a less safe situation.	100	1 in 10000 or 10^{-4}
2	Significant impact on safety with a high probability of an accident.	100	1 in 100 or 10^{-2}
1	Accident (i.e. loss of life or collision between mobiles)		1

Table 3-3: Relationship between accident risk per severity classification

3.4 Definition of Architecture and Operating Procedures

3.4.1

The PSC was based upon a generic application of A-SMGCS. In order to use evidence to demonstrate safety requirement achievability, the Safety Requirements were based upon the Heathrow A-SMGCS implementation and figure 3-3 shows its logical architecture.

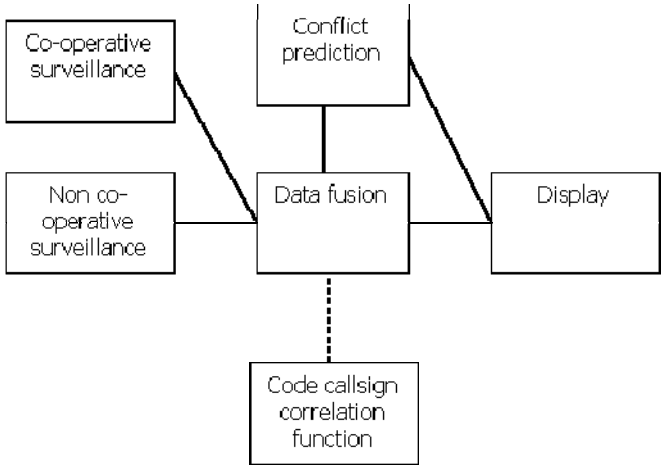

Figure 3-4: Logical architecture for A-SMGCS

3.4.2

A more detailed description of the Heathrow system is provided in section 2 of the PSC. Implementers must base their FHA/PSSA upon the functional and logical architectures, and the SAA on the physical architecture, of their specific implementations.

3.4.3

The PSC has been applied to the EUROCONTROL specification and procedures **[4-7]**. Implementers should ensure that the procedures applied at the airport are compliant with these specifications or address any differences with these specifications as part of their FHA/PSSA.

3.4.4

The FHA/PSSA contains a number of assumptions concerning A-SMGCS operations that shall be verified by the stakeholders. These are:

- All participating mobiles are cooperative.
- Current procedures are not changed through the use of A-SMGCS in normal visibility conditions.
- Should the A-SMGCS fail then the controller will revert to visual and procedural methods. When the A-SMGCS cooperative identification system fails there would be no automatic labelling of traffic. However, there may be variations within operating procedures such that already acquired aircraft identification may be maintained.
- Access to and operation on the runway for all vehicles is based on clearances from the tower.
- Only authorised drivers and suitably equipped vehicles are allowed to operate on the manoeuvring area. Service vehicles operating near aircraft stands and on dedicated roads are uncontrolled. However, such traffic may be restricted when Low Visibility Procedures (LVP) are in force.
- In some SMGCS installations, the function of certain taxiway, runway, holding point and stop bar lights are automated to mitigate the impact of the need to control by visual reference when visibility is low.
- Visibility conditions affect the controller's ability to observe and control traffic. Visibility conditions affect also the flight crew's ability to see and avoid other traffic during taxi, takeoff, and final approach and landing. Current procedures permit aircraft to take off and land on suitably equipped runways in conditions of runway visual range (RVR) down to below 100 m visibility. Therefore, advanced capabilities are needed to ensure spacing on the aerodrome surface when visual means are not adequate, and in order to maintain airport capacity in all weather conditions.
- VHF voice is the principal communications means for controlling aircraft and vehicle movements on the aerodrome surface. Multiple channels are usually used to control traffic on different parts of a large airport. UHF is used to communicate with airport vehicles at some airports.

- Availability of communications systems are outside the scope of the FHA/PSSA, as are lighting equipment and stopbars.
- Entry of aircraft into restricted areas is not considered
- Level 2 does not change roles of controllers, flight crew and drivers. Implementers must ensure that the controller shall not rely on A-SMGCS to detect conflicts.

3.4.5

A number of statements based on the operations at Heathrow are used during the derivation of the safety requirements, these were:

- A failure of the system does not immediately result in a 'safety significant event'. A failure will only become safety relevant after 3 seconds.
- The Multi-lateration update rate is 1 second;
- The rotation rate of SMR is 1 second;
- There are 100 movements per hour at Heathrow;
- A Movement (at Heathrow) is 10 minutes.
- Position information is considered corrupt if it is more than 30m from the actual position

3.5 Identify Hazards

3.5.1

The local FHA/PSSA must identify the failure modes to be considered. As part of the EUROCONTROL FHA/PSSA, the potential failure modes of the A-SMGCS functions were considered, ie:

- Position
- Identification
- Conflict detection

3.5.2

The potential failure modes were considered and consolidated as:

- Loss of information provided by a function;
- Corruption of the information provided by a function (eg inconsistent or delayed information).

3.5.3

The severity of failure of the A-SMGCS functions was assessed over a number of FHA workshops. In conducting this analysis, it was assumed that failures occurred under the following conditions:

- High traffic density;
- Complex;
- Peak time.

3.5.4

The severity of an A-SMGCS failure may be dependent on the region of the aerodrome the aircraft or vehicle is located at the time of the failure. The FHA assumed that hazards would be more severe in the vicinity of the runway and therefore hazard severity was assessed for the Runway Strip and elsewhere in the airport. Assumptions were made concerning the proportion of time the aircraft was on the runway (defined as the proportion of time that the aircraft is on the runway strip from push-back until the aircraft is at 100ft agl, or on landing, it is the proportion of time from 100ft above the runway threshold to arrival at the stand).

3.5.5

The severity of failures was also considered to be dependent upon the visibility conditions and estimates were made for the proportion of time for which each visibility condition occurred.

3.5.6

It was further assumed that a short term failure of up to 12 seconds would have not impact on operational safety for Level 1, and therefore the analysis assumed that failures persisted for more than 12 seconds.

3.5.7

The failure severity was also assessed according to whether it was detected by a controller or not. In some cases, undetected failures were not considered credible – for example the case of a total loss of A-SMGCS was considered to be always detected – and these failures were not considered further in the hazard analysis.

3.5.8

A further consideration was that not all failures of the A-SMGCS would result in an incident because at the time of failure, there may be no possibility of a safety significant event. The concept of ‘fail to safe’ was used to capture this aspect of the analysis.

3.5.9

The hazard analysis assessed the severity of each failure for each A-SMGCS failure according to aircraft location and visibility conditions as described above and the findings are

recorded in Annex E of the PSC. Implementers should follow a similar process and provide assumptions that are specific to the A-SMGCS and aerodrome. Detailed notes on the basis for allocating the severity are also provided in Annex E of the PSC.

3.6 Safety Objective Development

3.6.1

Event Trees are used to calculate the acceptable frequency of occurrence of a hazard - ie the Safety Objective. The PSC developed Event Trees for each hazard which allocated probabilities to the factors that could influence the severity of the hazard (see figure 3-4 below).

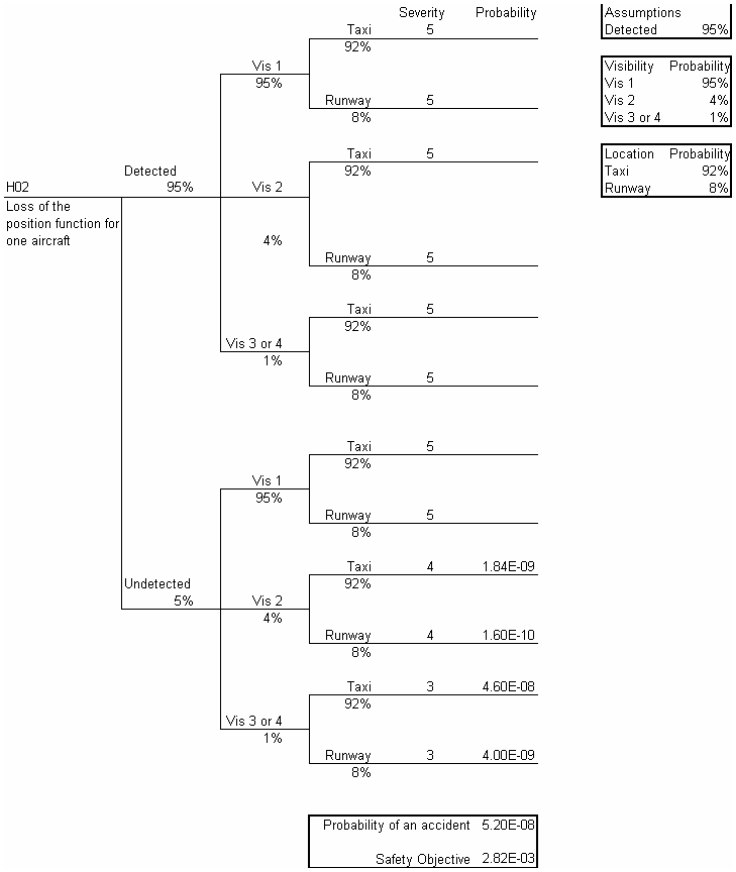

Figure 3-5: Example of Event Tree

3.6.2

In the case of the PSC the assumptions made were:

- the proportion of time which each visibility condition occurs at the aerodrome, namely:

  - visibility condition 1 95%;

- visibility condition 2 4%;
- visibility condition 3/4 1%.

- the proportion of time which an aircraft is on the runway (defined as the proportion of time that the aircraft is on the runway strip from push-back until the aircraft is at 100 ft above the runway datum or, on landing, the total time from 100 ft to arrival at the stand). The FHA/PSSA estimates 8% of time on the runway strip under all visibility conditions
- All failures occurred during high traffic density, in a complex situation and at peak time
- Probability that the failure would be detected by a controller (see table below);
- Probability of an incident occurring if the hazard occurs (probability of failing to safe – see table below).

		On the runway	Taxiway (vis1)	Taxiway (vis 2,3,4)
H01	Total loss of A-SMGCS	100.00%	100.00%	100.00%
H02	Loss of the position function for one aircraft	95.00%	95.00%	95.00%
H03	Loss of the position function impacting multiple aircraft	95.00%	95.00%	95.00%
H04	Corruption of the position function impacting one aircraft	95.00%	98.00%	99.80%
H05	Corruption of the position function impacting multiple aircraft	100.00%	100.00%	100.00%
H06	Total loss of the identification function	100.00%	100.00%	100.00%
H07	Loss of the identification function impacting multiple aircraft	100.00%	100.00%	100.00%
H08	Corruption of the identification function for one aircraft	99.00%	98.00%	99.80%
H09	Corruption of the identification function for multiple aircraft	99.00%	99.80%	99.98%
H10	Corruption of the conflict prediction function	100.00%	N/A	N/A

Table 3-6: Assumptions regarding detection rates of A-SMGCS failures

		'Fail to safe' probability
H04	Corruption of the position function impacting one aircraft	99.00%
H08	Corruption of the identification function for one aircraft	99.00%
H09	Corruption of the identification function for multiple aircraft	99.00%
H10	Corruption of the conflict prediction function	99.90%

Table 3-7: Assumptions regarding the probability of an incident should a failure occur

3.6.3

Implementers should follow a similar process using information for the specific aerodrome and also:

- ensure that all hazards have been identified
- customise the Event Trees with any specific additional conditions which would impact the safety consequence.
- re-validate the severity consequence for each branch of the Event Tree.
- Re-validate the assumptions regarding the detection probability with which a controller will detect a failure.

3.7 Safety Requirements Development

3.7.1

Safety Requirements are developed using Fault Trees. This enables the safety requirements to be partitioned between the components which contribute to each Safety Objective. The process involves dividing the acceptable failure rate between these components enabling Safety Requirements for each component to be identified.

3.7.2

For the PSC, the key assumptions for the Fault Trees are:

- Acceptable risk is spread evenly over each hazard in order to determine safety requirements – in practice this would be revisited once actual performance information for components was available
- Total loss of A-SMGCS is always detected
- A probability of loss or corruption of information from avionics of 10-4 per movement is assumed
- Regarding avionics failure, 90% are assumed to result in loss of data, 9% in corruption of data and 1% in corruption of position information

3.7.3

These assumptions should be re-validated for each local implementation.

3.7.4

The PSC verified that the safety requirements were achievable by using the implementation at LHR as an example. However this is not required in the local safety case.

4. SYSTEM SAFETY ASSESSMENT

4.1 Introduction

4.1.1

This section provides an overview of the activities required to complete a local safety assessment. The PSC verified that the safety requirements are achievable using LHR as an example implementation. Implementers will need to complete an SSA as part of the local implementation. Further information can be found in the EUROCONTROL SAM **[3]** and the EUROCONTROL Safety Case Development Manual **[2]**.

4.2 SSA

4.2.1

Evidence is required to support the argument that A-SMGCS Safety Requirements have been implemented consistently and correctly. This element of the safety case is addressed through the system safety assessment (SSA). The SSA demonstrates that the system as implemented achieves an acceptable risk and consequently satisfies its Safety Objectives and the system elements meet their safety requirements specified in the PSSA.

4.2.2

The SSA process is conducted throughout the system implementation and integration, transfer into operation, operation, maintenance and decommissioning phases of the system lifetime. Detailed guidance is provided in the EUROCONTROL SAM.

4.2.3

For A-SMGCS, evidence can be collected from the following sources:

- System specification: the design criteria used by the manufacture;
- Reliability modelling;
- Site acceptance tests undertaken following the installation of the system to determine that the system meets its original purchase specification and can be used operationally.

- Historical, to determine that the system is still performing to meet requirements;
- Interviews: where physical evidence is not obtainable, particularly with reference to the ability of the controller to meet the required error detection rates, interviews can be used to determine whether the requirement is achievable;
- Trials and modelling results.

4.2.4

Evidence should be gathered to support achieving safety requirements for each A-SMGCS component. These are:

- Display;
- Data fusion;
- Conflict prediction;
- Code callsign correlation;
- Surveillance (Multi-lateration and SMR).

4.2.5

Where the architecture of the local implementation differs, evidence should be gathered for the components of the local architecture

4.2.6

The SSA process requires sufficient evidence to be gathered to provide confidence that the local implementation will meet its safety requirements. Following transfer to operations, the SSA needs to be supported by monitoring of system performance to augment the evidence collected during the implementation phase.

4.2.7

The following notes provide details of specific issues that may need to be addressed during the implementation phase.

4.3 Avionics

4.3.1

The surveillance performance is dependent upon failures rates of Mode S transponders and no firm evidence is available. The PSC SSA used the following:

- EUROCONTROL Mode S programme Enhanced Surveillance FHA and PSSA presented to the SRC (awaiting approval);
- JAA CNS/ATM Steering Group on enhanced surveillance with SSR Mode S No. and Revision pp025_76 17th April 2003;
- FAA/JAA Ac/AMJ No>25.1309 dated 6/10/2002/

4.3.2

The transponder failure rate should be converted into operational hours for the specific airport based upon the number of movements per hour at the airport and the duration of each movement.

4.3.3

Assumptions are also required concerning the effects of transponder failures. In the example of the PSC, the following assumptions were used:

- 90% of transponder failures result in a loss of data with the consequence that the aircraft is not detected by the ground system;
- 9% result in corruption of data content (eg Mode A or aircraft identification);
- 1% result in corruption of position information.

4.4 Sensor Performance

4.4.1

It is likely that SMR will already be installed at the airport and probability of target detection already measured. Performance parameters are required to assess the probability of detection and display. In the case of the PSC, the parameters used were the probability of detection and display of a target with a radar cross section of $1m^2$, with a probability of 95% per scan. Multi-lateration system performance can be measured as part of site acceptance testing to determine accuracy and loss of position.

4.4.2

In the case of the PSC, it was assumed that three consecutive track drops would constitute a safety event.

4.5 Historical Evidence

4.5.1

Historical evidence was used to provide evidence of the mean time between failures (MTBF) of the overall A-SMGCS and the display system in the PSC. Historical performance information may be available from manufacturers to support evidence that the procurement specifications can be achieved. However, the reliability of historical evidence should be checked because it may not record all failures.

4.6 Reliability Analysis

4.6.1

Reliability analysis can be used to product the MTBF and mean time to repair (MTTR) of the system and its components. In the case of the Heathrow system, RAM4 was used to model the A-SMGCS system and its subsystems. For the failure and repair distributions a lognormal distribution was used. The lognormal distribution is usually used to describe repair times. The distribution value is always 0.6 which is associated with a modular repair policy (replacement of Line Replaceable Units (LRUs) on failure.

4.7 Monitoring of System Performance

4.7.1

Continuous safety monitoring should be performed to ensure that the Safety Requirements are met, Safety Objectives are satisfied and assumptions on the operational environment and its external mitigation means and assumptions made during the safety assessment process are correct while the system is in operation. Safety monitoring also allows identification of any trends in the evolution of safety performance[2].

4.7.2

Fault data should be collected for all of the A-SMGCS elements. The failure rates and repair times should be monitored to determine whether the overall system safety requirements are being met.

4.7.3

Note that it may not be feasible to monitor system performance relating to all safety requirements. Where requirements relate to the loss or corruption of a function for an individual aircraft, routine performance monitoring may not be a practical approach due to the volumes of data that would need to be gathered an analysed.

4.8 Incident Reporting and Analysis

4.8.1

Safety occurrence reporting and assessment should be carried out routinely as part of overall safety management process. This should consist of events detection and notification, factual information gathering and event reconstruction, event analysis, issue of recommendations, assessment of their effectiveness by monitoring over time the effect of their implementation, and reporting and exchange[2].

4.8.2

Details of requirements for compliance with the European ANS safety legislation concerned with incident reporting and analysis is contained with ESARR2, Reporting and Assessment of Safety Occurrences in ATM. It requires incidents and accidents to be recorded together with the contribution of ground-based ATM and identification of system inadequacies and areas for system improvement.

5. GUIDANCE TO A-SMGCS IMPLEMENTERS ON THE DEVELOPMENT OF A FULL SAFETY CASE

5.1 Introduction

5.1.1

This section describes guidance to the Implementers of A-SMGCS on how to use the EUROCONTROL A-SMGCS Preliminary Safety Case **[1]** in the development of a full Project Safety Case for a specific implementation of A-SMGCS. Further Guidance material on how to apply the process can be found in the EUROCONTROL Safety Case Development Manual **[2]**.

5.2 A-SMGCS Safety Argument

5.2.1

The following figure provides a top-level safety argument for A-SMGCS. This is a set of statements that is used to assert that the system is safe. The safety argument below is based upon the safety argument used in development of the EUROCONTROL A-SMGCS Preliminary Safety Case.

5.2.2

The shaded items in the safety argument are the responsibility of the States. The other items show where information in the PSC may be re-used to support the States' Safety Argument. Where information in the PSC is reused, it must be validated in the context of the local implementation and specific Safety Objectives and Safety Requirements derived for that implementation.

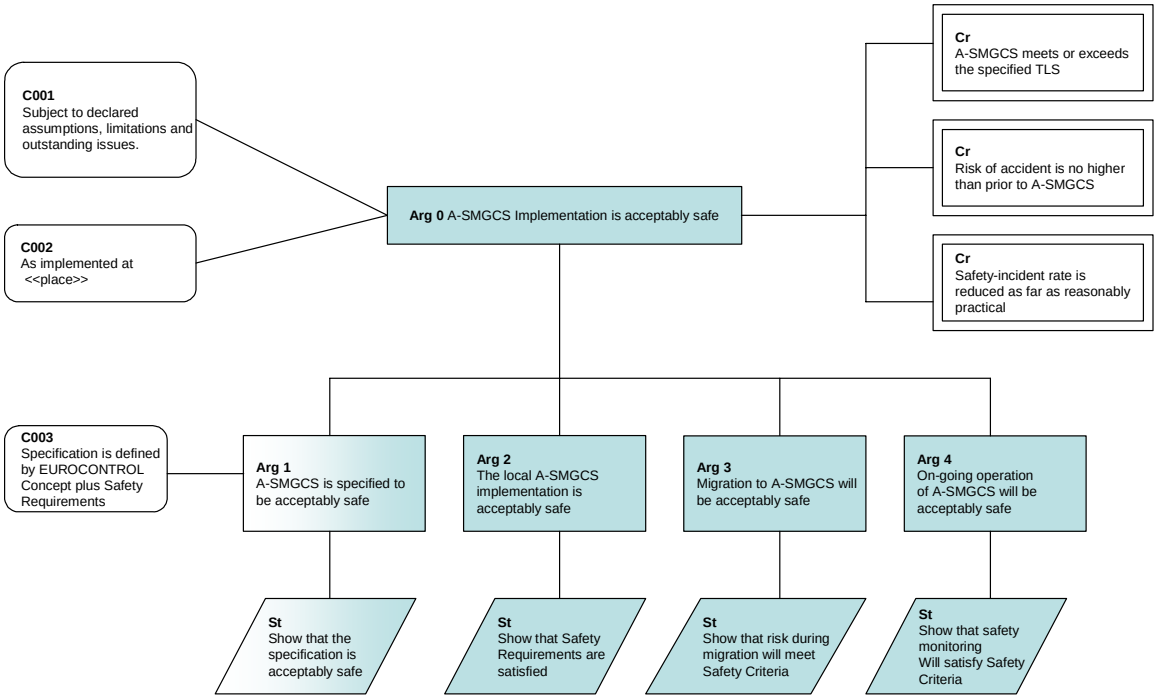

Table 5-1: Overall Safety argument for A-SMGCS in ECAC

5.2.3

Arg 1 shows that the EUROCONTROL A-SMGCS concept is acceptably safe subject to complete and correct implementation of the Safety Requirements. This argument is based upon the findings of the EUROCONTROL Preliminary Safety Case **[1]**, in relation to the generic application of A-SMGCS described therein. It decomposed in the following figure.

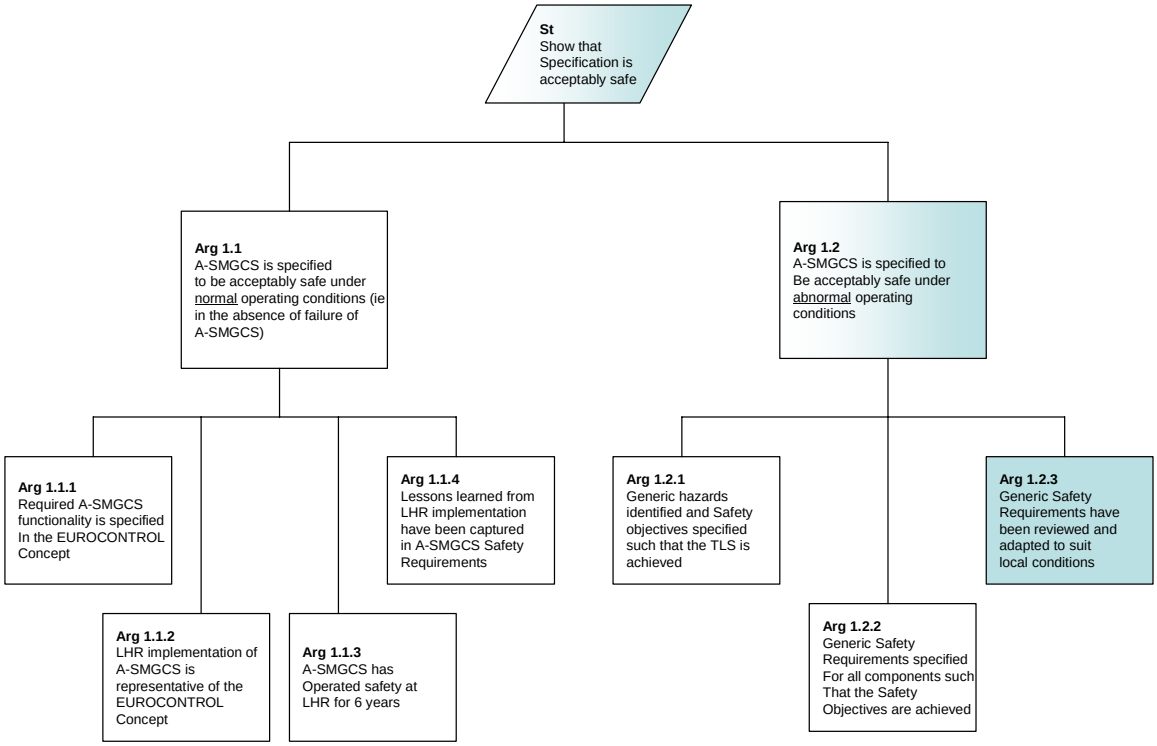

Figure 5-1: Specification of Safety Requirements

5.2.4

Arg 1 asserts that A-SMGCS is specified to be acceptably safe and this is broken down into arguments that it is acceptably safe during normal operating conditions (**Arg 1.1**, the success case) and that is acceptably safe under abnormal operating conditions (**Arg 1.2**, the failure case).

5.2.5

The following paragraphs describe arguments supporting **Arg 1.1** (normal operations):

5.2.6

Arg 1.1.1 asserts that the system is consistent with the EUROCONTROL definition of A-SMGCS as specified in **[4-7]**.

5.2.7

The case for acceptably safe normal operations in the PSC was based upon the argument that the LHR implementation is consistent with the EUROCONTROL A-SMGCS concept (**Arg 1.1.2**) and that is has been operating safely since 1999 (**Arg 1.1.3**). The success case is further supported by evidence of operating methods adopted at Heathrow to ensure safety under normal operations (Arg 1.1.4). These are detailed in section 4 of the PSC and include:

- ensuring the professional competence of controllers through appropriate training;
- communicating with airlines and aircrew to ensure correct transponder setting procedures are followed;
- operation of the system is subject to a safety management system.

5.2.8

Arg 1.2 asserts that A-SMGCS is acceptably safe under abnormal operating conditions. This argument is supported by **Arg 1.2.1** which states that hazards have been identified and Safety Objectives specified to meet the TLS. This requires all hazards to be correctly identified and analysed and the safety objectives adequately specified. This relates to the output of the FHA and further guidance is provided in section 3 of this report.

5.2.9

Arg 1.2.2 asserts that Generic Safety Requirements have been specified for all components such that the Safety Objectives are achieved. This process relates to the PSSA elements of the PSC and further guidance is provided in section 3 of this report.

5.2.10

The Safety Objectives and Safety Requirements were developed on a generic basis and any implementation specific details based upon LHR as a representative implementation. As part of the safety case for a specific A-SMGCS implementation, these generic Safety Requirements would need to be adapted for meet local conditions (**Arg 1.2.3**). Section 3 of this report provides further guidance on conducting a local FHA/PSSA.

5.2.11

Arg 2 asserts that the local implementation of A-SMGCS is acceptably safe and is further expanded in Figure 3-2 below.

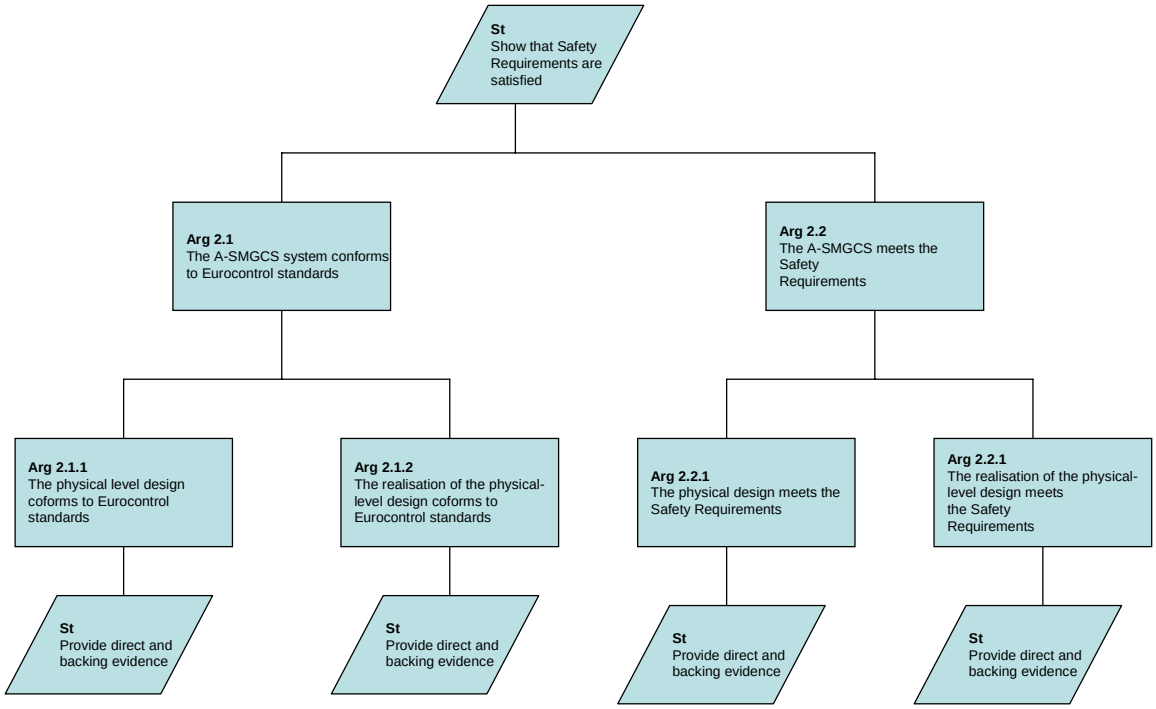

Table 5-2: Local safety case argument for A-SMGCS

5.2.12

Arg 2 shows that the local implementation is acceptably safe. In order to achieve this the supporting arguments assert that the system conforms to EUROCONTROL standards and that the system meets its Safety Requirements.

5.2.13

Arg 2.1 asserts that the system conforms to EUROCONTROL specifications. The Preliminary Safety Case has been applied to the EUROCONTROL specifications and procedures. Evidence that the system conforms to EUROCONTROL standards is required to verify that the system functions and procedures are consistent with the functions and procedures that the PSC was based upon. It is further broken down into:

5.2.14

Arg 2.1.1 asserts that the physical design conforms to EUROCONTROL standards **[4-7]**.

5.2.15

Arg 2.2.2 asserts that the realization of the physical design conforms to EUROCONTROL standards **[4-7]**.

5.2.16

Arg 2.2 asserts that the A-SMGCS meets the Safety Requirements and is further broken down into:

5.2.17

Arg 2.2.1 asserts that the physical level design shall meet the related safety requirements. Whilst this is outside the scope of the PSC, a process to verify that the Safety Requirements were achievable was conducted using London Heathrow as an example. For the local safety case, the Implementer should conduct an SSA. Further guidance on this is provided in the EUROCONTROL SAM **[3]** and Safety Case Development Manual **[2]**.

5.2.18

Arg 2.2.2 asserts that the realization of the physical level design meets the Safety Requirements. Whilst this is outside the scope of the PSC, a process to verify that the Safety Requirements were achieved was conducted using London Heathrow as an example. For the local safety case, the Implementer should conduct an SSA. Further guidance on this is provided in the EUROCONTROL SAM **[3]** and Safety Case Development Manual **[2]**.

5.2.19

Arg 3 asserts that the migration to A-SMGCS operations will not endanger the on-going operational service. This is outside the scope of the Preliminary Safety Case and although some guidance concerning the process and techniques required to provide evidence to support Arg 3 is provided in the Safety Case Development Manual **[2]**, it is the implementers responsibility to show that the decomposition of the argument, and the evidence to support it, are adequate.

5.2.20

Arg 4 asserts that the monitoring of the on-going operational service will be sufficient to show that A-SMCGS is acceptable safe. This is outside the scope of the Preliminary Safety Case and although some guidance concerning the process and techniques required to provide evidence that on-going operations will be acceptably safe is provided in the Safety Case Development Manual **[2]**, it is the implementers responsibility to show that the decomposition of the argument, and the evidence to support it, are adequate.

6. REFERENCES

[1] A-SMGCS Preliminary Safety Case, Edition 1.1, October 2005

[2] Safety Case development manual v2.0 document number DAP/SAF/091

[3] EUROCONTROL Safety Assessment Methodology, document number SAF.ET1.ST03.1000-MAN-00-00

[4] Functional Specifications for A-SMGCS Implementation Level I, Edition 1, 30/9/2003

[5] Functional Specifications for A-SMGCS Implementation Level II, Edition 1, 17/5/2004

[6] Operational Concept and Requirements for A-SMGCS Implementation Level I, Edition 1, 30/9/2003

[7] Operational Concept and Requirements for A-SMGCS Implementation Level II, Edition 1, 17/5/2004