EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

A-SMGCS Levels 1 & 2 Preliminary Safety Case

Edition Number	:	2.0
Edition Date	:	November 2006
Status	:	Released Issue
Intended for	:	General Public

EUROPEAN AIR TRAFFIC MANAGEMENT PROGRAMME

DOCUMENT CHARACTERISTICS

TITLE		
A-SMGCS Levels 1 & 2 Preliminary Safety Case		
	EATMP Infocentre Reference:	07/01/09-01
Document Identifier	**Edition Number:**	2.0
	Edition Date:	November 2006

Abstract

This document presents the preliminary safety case for the A-SMGCS Level 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	2290 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 Airport Operations and Environment 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
0.1	June 2005		Project Team review	All
0.2	August 2005		EUROCONTROL review	All
0.3	August 2005		APR review	All
0.4	September 2005		Stakeholder review comments (PRG 06/09/05)	All
1.0	October 2005		Formal release	All
1.1	November 2005		Editorial corrections (from Skyguide)	All
1.2	August 2006		Updates to A-SMGCS Level II performance	All
1.3	October 2006		Updates following Level II workshop	All
1.4	October 2006		Final draft	All

CONTENTS

FIGURES

TABLES

EXECUTIVE SUMMARY

The A-SMGCS preliminary safety case evaluates whether the EUROCONTROL Levels 1 and 2 A-SMGCS concept and specifications can be safely implemented. This is to support the EUROCONTROL Airports Programme in the validation of the Concept. The A-SMGCS preliminary safety case has been developed based on the generic EUROCONTROL concept and a representative A-SMGCS implementation in Europe (London Heathrow).

The safety analysis was performed by applying the EUROCONTROL Safety Assessment Methodology (SAM).:

Throughout the whole process, stakeholders have participated in a number of workshops to validate the approach, assumptions and results of the analysis.

Assumptions

The A-SMGCS preliminary safety case has been developed based on a number of assumptions. The results of the A-SMGCS preliminary safety case are only valid if these assumptions are valid. As such, when stakeholders develop their local safety cases then all the assumptions shall be validated.

The key assumptions relate to:

- Weather (the proportion of time an airport is in visibility condition 1, 2, 3 or 4);
- Airport layout (the proportion of time an aircraft is on the taxiway or runway);
- Controller performance (the detection rate of an A-SMGCS failure);
- The architecture and performance of a typical A-SMGCS (in this case LHR).

The evidence to support the argument has been developed, in part, based on a ‘case-study’ (London Heathrow). Stakeholders should review all the assumptions regarding LHR evidence to ensure it remains valid for their local implementation.

Conclusions

The A-SMGCS preliminary safety case has shown that the safety requirements for A-SMGCS Level 1 and 2 can be implemented.

It should be noted that this Preliminary Safety Case demonstrates that A-SMGCS can operate within a tolerable risk. As part of the overall case for A-SMGCS, it should be demonstrated that A-SMCGS provides operational and safety benefits and this is addressed separately in the EUROCONTROL Generic Cost Benefit Assessment of A-SMGCS (reference 11).

CAUTIONARY NOTE

The preliminary safety case has been developed based on a generic concept and a representative A-SMGCS implementation in Europe.

A great number of assumptions have been made during the analysis relating to operational aspects of A-SMGCS and the implementation decisions which have been made at Heathrow. It is unlikely that all of these assumptions and implementation details will be valid at other airports in Europe and should be re-validated on a ‘case-by-case’ basis.

This document is not intended to replace the safety cases that shall be performed by stakeholders for their local implementation.

1. INTRODUCTION

1.1 Scope and Context

1.1.1

The A-SMGCS preliminary safety case examines the safety aspects of the EUROCONTROL Levels 1 and 2 A-SMGCS concept and specifications. It presents evidence whether the A-SMGCS concept, as defined by the EUROCONTROL Airport Operations Programme, can be implemented such that safety requirements are achieved or exceeded.

1.1.2

The A-SMGCS preliminary safety case examines the concept of A-SMGCS. It is not intended to replace the safety cases that shall be performed by stakeholders for their local implementation.

1.1.3

The preliminary safety case focuses on developing safety requirements and showing that these are achievable. The full case for implementation of A-SMGCS should also address the operational and safety benefits offered by A-SMGCS. A generic cost benefit analysis for A-SMGCS has been developed by EUROCONTROL that addresses this issue (reference 11).

1.1.4

National Air Traffic Services (NATS) Ltd and Helios Technology Ltd. have developed this document for the EUROCONTROL Airport Programme.

1.2 Stakeholder Validation

1.2.1

The A-SMGCS preliminary safety case was conducted with the participation of a wide set of stakeholders who participated in a number of workshops. The workshops developed and validated the:

- scope of the A-SMGCS Operational concept assessed;
- the evidence presented in the safety case including the hazards, failures and the consequences of the failure on aerodrome operations caused by A-SMGCS or other systems at the aerodrome which interface to the A-SMGCS;
- safety objectives and requirements;
- set of assumptions.

1.2.2

The participants at the workshop included active aerodrome controllers, engineers and safety experts, consisted of the following stakeholders:

- Belgocontrol
- IFATCA
- Skyguide
- AIG
- ENAV S.P.A
- LVNL
- EUROCAE
- NATS
- Oslo
- Czech ANS
- ADP
- EUROCONTROL
- Helios Technology

1.2.3

Stakeholders who have participated in the development and validation of the Preliminary Safety Case are identified in Annex L

2. A-SMGCS CONCEPT AND THE LHR IMPLEMENTATION

2.1 Introduction

2.1.1

This section describes the scope of the A-SMGCS concept and the London Heathrow implementation of that concept. It describes the people, procedures and equipment that constitute the scope of the preliminary safety case.

2.2 Concept

2.2.1

The main functions provided by the A-SMGCS Level 1 are illustrated in **Figure 1**. These are:

- Position: the presentation to a controller of the location of an aircraft or vehicle;

- Identification:
- the presentation to the controller of the automatic identity (aircraft identification or registration) of cooperative aircraft and vehicles;
- the presentation to the controller of non-cooperative aircraft or vehicles.
-

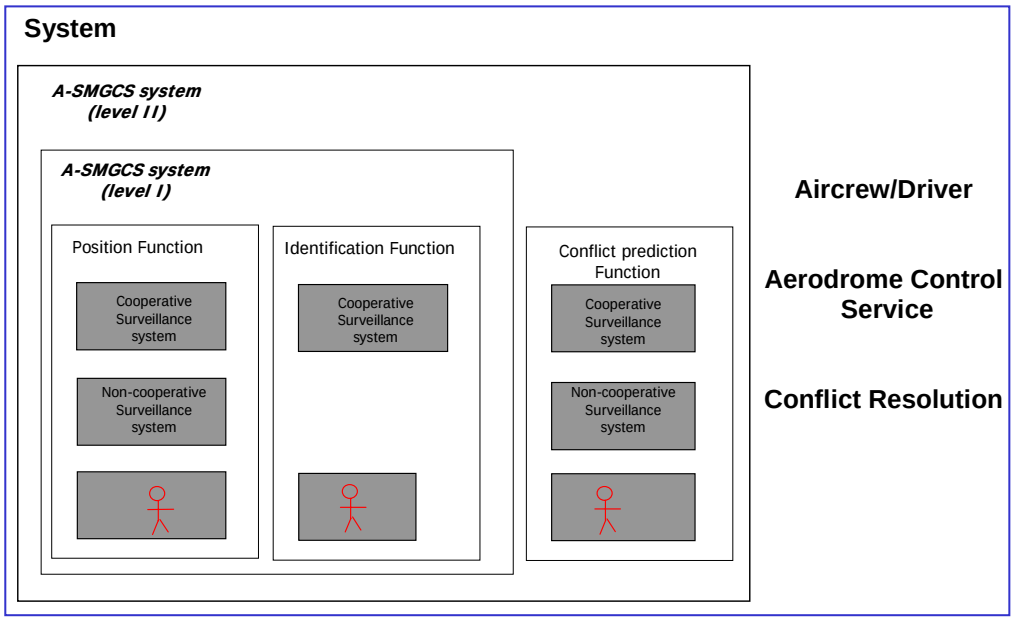


Figure 1: Functions of A-SMGCS

2.2.2

Level 1 A-SMGCS provides a prediction function to alert the controller of:

- potential collisions (between aircraft/vehicle or aircraft/aircraft) on the runway surface or protection area;
- potential entry of aircraft or vehicles into restricted areas.

2.2.3

This applies to arriving and departing movements and all transit movement on runways and restricted areas

A-SMGCS Level 1

Definition

2.2.4

Level 1 (reference 1) A-SMGCS displays the position and identity of all cooperative aircraft in the movement area; in addition, it displays the position of all vehicles, and the identity of co-operative vehicles, in the manoeuvring area.

2.2.5

This surveillance information is shown on a screen with the aerodrome traffic context (e.g. airport layout, reference points).

2.2.6

Control (including runway incursion alerting), Guidance and Planning functions are not included in implementation Level 1.

Concept of Operation

2.2.7

The operational concept for A-SMGCS at Level 1 has been defined by EUROCONTROL (reference 2). The primary intention is to enhance safety and efficiency of surface operations through the introduction of the A-SMGCS.

2.2.8

It is expected that all participating mobiles are co-operative, and therefore automatically labelled in the movement or manoeuvring area. Non-cooperative mobiles are the exception processed by special procedures. One or more co-operative surveillance systems are necessary to detect and identify these co-operative targets. Since there may be non co-operative targets present, a surveillance system that does not rely on co-operation is also required.

2.2.9

EUROCONTROL has defined the A-SMGCS operating procedures (reference 3). These ATC procedures define how the surveillance information provided by A-SMGCS will be used. The Identification procedure is defined, for various operating conditions, as is the use of the information provided by A-SMGCS at various stages of movement on the airfield.

2.2.10

A-SMGCS Level 1 does not change the current roles of controllers, flight crew or vehicle drivers.

2.2.11

During normal visibility conditions, the information provided by the A-SMGCS will serve as a supplementary means of information to the controller for regular visual ‘out-the-window’ surveillance. In a situation with restricted visibility (e.g. due to distance, obstructions or bad weather) then A-SMGCS surveillance data may be used instead of visual observation.

2.2.12

It is assumed that the current procedures are not changed through the use of A-SMGCS in normal visibility conditions:

System Description

2.2.13

EUROCONTROL has defined the functional requirements for A-SMGCS Level 1 (reference 4). These can be summarised as follows:

- Acquisition of traffic information from non co-operative targets;
- Acquisition of traffic information from co-operative targets;
- Acquisition of traffic information from approaching targets;
- Acquisition of other information about traffic;
- Data Fusion;
- Acquisition of traffic context;
- Interface with user;
- Service monitoring.

2.2.14

Acquisition of traffic information from Non co-operative targets: this typically requires one or more Surface Movement Radars (SMR) to provide surveillance of non co-operative targets.

2.2.15

Acquisition of traffic information from Co-operative targets: a number of technologies may be used to provide surveillance of targets. The most common implementation option used today is based on the use of multi-lateration using the Mode S transponder on an aircraft. The position of the mobiles are calculated based on the time difference between the receipt of spontaneous emissions from the target. Identification information (aircraft identification or call sign) is obtained through active interrogation of the transponder. Vehicles do not have a standard means of detection, such as Mode S. Therefore it is necessary, either to provide them with Mode S type transmitters, capable of detection by multi-lateration, or a bespoke vehicle tracking system.

2.2.16

Acquisition of traffic information from Approach targets: primary and secondary surveillance radars are the current standard means of detecting approaching aircraft. Wide Area multi-lateration may also be used. Data from the approach radar may be distributed through a radar data processing system.

2.2.17

Data Fusion: the various elements of surveillance and other information are collected in a data fusion system. This ensures that all information regarding a target is available to the user.

2.2.18

Traffic Context: information regarding runway status, LVP, system status, etc, may be provided either automatically or as a manual input.

2.2.19

Interface with User: each user typically requires traffic information displayed on a map showing relevant information about the airfield. The user should be able to modify the display presentation, and information displayed, to fit the operational conditions.

2.2.20

Service monitoring: the various elements of the A-SMGCS should be monitored, such that relevant status information can be supplied to users, and technicians, and to allow performance information to be derived.

2.2.21

Figure 2 shows a typical architecture for an A-SMGCS. It may be possible to achieve the required performance without some elements shown in the diagram, and other systems may be used instead. The service monitoring element is not shown in the diagram.

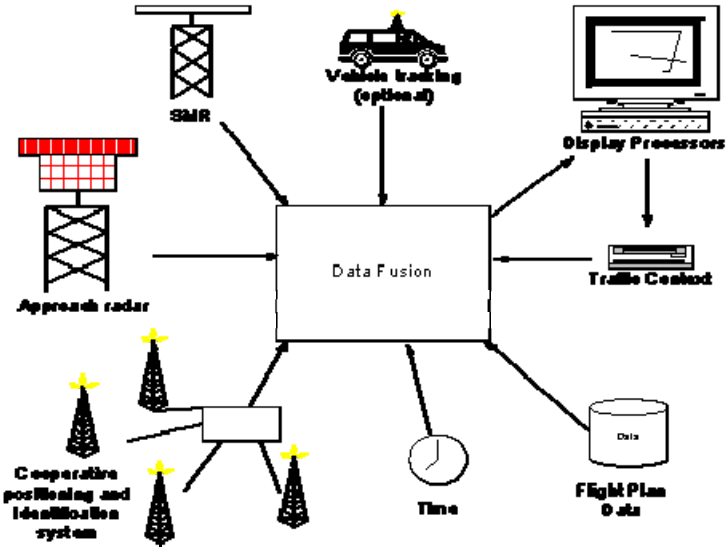


Figure 2: Typical A-SMGCS architecture

Constraints and Assumptions

2.2.22

Should the A-SMGCS fail, then the controller will revert to visual and procedural (which may be supported by flight progress strips) methods.

2.2.23

When the A-SMGCS co-operative identification system fails there would be no automatic labelling of traffic. However, depending on local procedure, already acquired aircraft identification may be maintained.

2.2.24

There are no safe distance minima defined in terms of distance or time on the aerodrome surface except for runway operations of aircraft. Traffic on the aerodrome manoeuvring area (defined as runways and taxiways) is controlled by the tower through the issuance of a taxi clearance and progressive instructions such as “Taxi behind”, “Hold short of” and “Behind landing line up and wait” that assume visual acquisition and correlation of traffic by the flight crew and continuous position awareness of the ‘own-ship’ position. The priority between aircraft operating on the aerodrome surface is at the discretion of the controller.

2.2.25

Traffic on the apron may be managed either by:

- an ATS provider;
- a dedicated apron management service.

2.2.26

Access to and operation on the runway for all vehicles is based on clearances from the tower.

2.2.27

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.

2.2.28

In some A-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.

2.2.29

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.

2.2.30

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.

2.2.31

Figure 3 illustrates normal voice communication exchange procedures between tower and aircraft at various stages during departure and arrival operations.

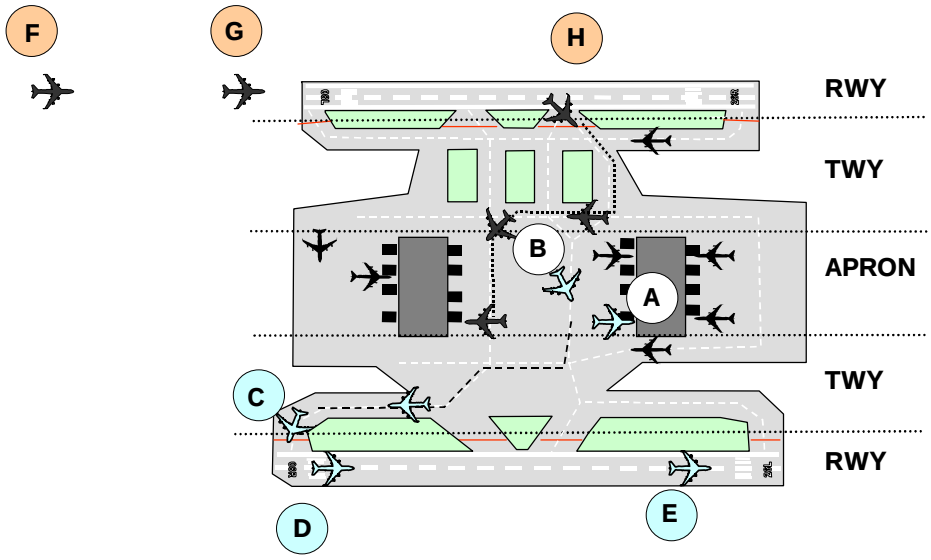


Figure 3: Example airport operations scenario

A 1/ Pilot requests ATC clearance, typically 10 min prior to off block time;

2/ Pilot requests engine start and confirms having received latest ATIS or has been cleared to start with the ATC clearance;

3/ Pilot requests pushback (engine start and pushback are normally requested at the same time).

B Pilot requests taxi clearance. The controller issues a clearance. If applicable, instructions to hold short of intersections and give way to conflicting traffic may be included. In the illustrated case: “Behind aircraft [type] from left taxi to holding Point RWY 08R”.

C Pilot will report ready and will be given line-up clearance or conditional line up clearance with or without constraints, such as: “Behind first landing”, “Behind departing”, “Line up RWY 01R” etc.

D Take-off clearance will be issued with wind and RVR info, if needed. The clearance is given when safe distance (radar or procedural) to a preceding aircraft is assured after take-off.

E After take-off and when free of any local traffic, aircraft will be shifted to departure frequency.

F Pilot checks in on TWR frequency after handoff from approach control and reporting on final.

G Controller issues landing clearance with wind and other essential information.

H After landing, pilot will receive taxi instructions to stand including, for instance: “Hold short of…”, “Give way to..” and “Taxi behind…” and guidance, if needed.

Systems outside the scope of the analysis

2.2.32

The availability of communication systems (e.g. VHF) are outside of the scope of the safety assessment and are assumed to be always available. In addition lighting, including stop bars are not considered in this analysis.

A-SMGCS Level 2

Definition

2.2.33

A-SMGCS Level 2 consists of the introduction of automated surveillance (identical to Level 1) complemented by an automated service capable of detecting conflicts and infringements of some ATC rules involving aircraft or vehicles on runways and restricted areas. Whereas the detection of conflicts identifies a possibility of a collision between aircraft and/or vehicles, the detection of infringements focuses on dangerous situations because one or more mobiles infringed ATC rules. A-SMGCS Level 2 will not address conflicts between two vehicles, but only between an aircraft and another mobile.

2.2.34

The conflicts / infringements considered at Level 2 are related to the most hazardous ground circulation incidents or accidents. They could be defined as follows:

- conflicts / infringements on runway caused by aircraft or vehicles;

- restricted areas incursions caused by aircraft (i.e. incursions on a closed taxiway or runway).

2.2.35

This analysis does not consider the alert for aircraft entering restricted areas because this is very specific to each airport and their local operations.

2.2.36

Two stages of alert are recommended, these are:

- Stage 1 alert is used to inform the controller that a situation which is potentially dangerous may occur, and he/she needs to be made aware of. According to the situation, the controller receiving a stage 1 alert may take a specific action to resolve the alert if needed. This is called INFORMATION step;
- Stage 2 alert is used to inform the controller that a critical situation is developing which needs immediate action. This is called ALARM step.

2.2.37

A-SMGCS Level 2 does not change the current roles of controllers, flight crews and vehicle drivers. Even if provided with the A-SMGCS control service, the controller shall not rely on it to detect conflict / infringement, but shall continue the analysis of the traffic situation to detect conflict / infringement himself as in SMGCS or A-SMGCS Level 1.

2.3 London Heathrow A-SMGCS

Introduction

2.3.1

London Heathrow (LHR) implemented the A-SMGCS concept in 1998 and have been using the system operationally since then. This section describes the operational and technical implementation at LHR.

Operational implementation at Heathrow

General

2.3.2

This section describes the A-SMGCS operations at Heathrow.

2.3.3

LHR has implemented the EUROCONTROL A-SMGCS procedures as far as practical. There are a few modifications to resolve local issues, which are identified below.

2.3.4

The A-SMGCS at LHR is in operation 24 hours each day. The exceptions to this are:

- Routine Maintenance;
- Modification to the airfield map (both temporary and permanent);
- System Upgrades.

Identification Procedures

2.3.5

The identification procedures in use at Heathrow vary slightly from those in the EUROCONTROL draft procedures document. This is due to the fact that, following hazard analysis it was determined that, identification on stand had two inherent risks.

2.3.6

The integrity of the A-SMGCS at Heathrow does not provide an accuracy of better than 7.5 metres in terms of position accuracy within stand areas. Therefore, within these areas, there is the potential for the position of two adjacently parked aircraft to be transposed on the HMI and to be displayed on the wrong stands.

2.3.7

Another issue is that the controllers have very little control over when an aircraft will actually enter their assigned Mode A code, or when they will physically switch the transponder on. With the increased use of Data Clearance Link (DCL) this may become even more of an issue. Until such time as there are laid down procedures for transponder setting following parking, there can be no guarantee that aircraft parked in close proximity will not be transmitting the same Mode A code.

2.3.8

Furthermore, to prevent clutter and label overlap caused by the proliferation of ground vehicles that carry transponders (or similar co-operative devices), the stand areas are suppressed from the controller's display.

Outbound Aircraft

2.3.9

Due to the above reasons it was decided that aircraft identification, for outbound traffic, should be carried out once aircraft had left their parking position. The procedures very closely emulate the United Kingdom, Manual of Air Traffic Services (Part 1), procedures for establishing SMR identification which are reproduced below:

Methods of establishing SMR Identification

2.3.10

Before providing guidance to an aircraft/vehicle based on SMR-derived information, positive radar identification shall be established by the use of one of the methods specified below:

a) By correlating the position of a visually observed aircraft/vehicle to that displayed on the SMR; or

b) By correlating an identified SMR position from another radar source; or

c) By correlating an SMR position complying with an ATC instruction for a specified manoeuvre; or

d) By correlating a displayed SMR position to an aircraft/vehicle as reported by radio or

e) By correlating a displayed SMR position to an aircraft/vehicle position e.g. entering a runway or taxiway, holding point or any position marked on the video map.

2.3.11

The GMC controller is responsible for identifying outbound aircraft as soon as is practicable following pushback.

Inbound Aircraft

2.3.12

As the UK National Airspace System (NAS) feeds data via the central Code Callsign Distribution System (CCDS) into both the Aerodrome Traffic Monitor (ATM) and A-SMGCS it was determined that the integrity of this data would allow transfer of identification between the two systems.

2.3.13

Therefore the Air controller may validate the code/callsign pairing by recognising a pairing previously observed on the ATM.

Towing Traffic and Vehicles

2.3.14

As integrity trials are ongoing into the equipment that may be available/fitted to other vehicles using the airfield, as yet there are no procedures associated with towing or vehicular traffic

Decision Making Based on Identified Traffic

2.3.15

Based on position information provided by the A-SMGCS, controllers are able to issue the following types of instructions/clearances:

- Pushback instructions (including conditional);
- Taxi instructions (including conditional);
- Line-up clearance;
- Take off clearance;
- Landing clearance.

Future Procedures

2.3.16

At present there are no advanced procedures for the use of the A-SMGCS in operation, however following approval from NATS Airports Headquarters (AHQ) and the Civil Aviation Authority, Safety Regulation Group, Air Traffic Services Standards Department (CAA SRG ATSSD) it is envisaged that the following procedures will be developed for use in Visibility Condition 2:

- Conditional Line-up Clearance;
- Multiple Line-up Clearance;
- Land After.

Technical implementation at Heathrow

Introduction

2.3.17

This section provides a description of the A-SMGCS system in operation at Heathrow airport. The system architecture presented here forms the basis for the fault tree analysis of system safety requirements from the PSSA. **Figure 4** presents the architecture of the Heathrow A-SMGCS system.

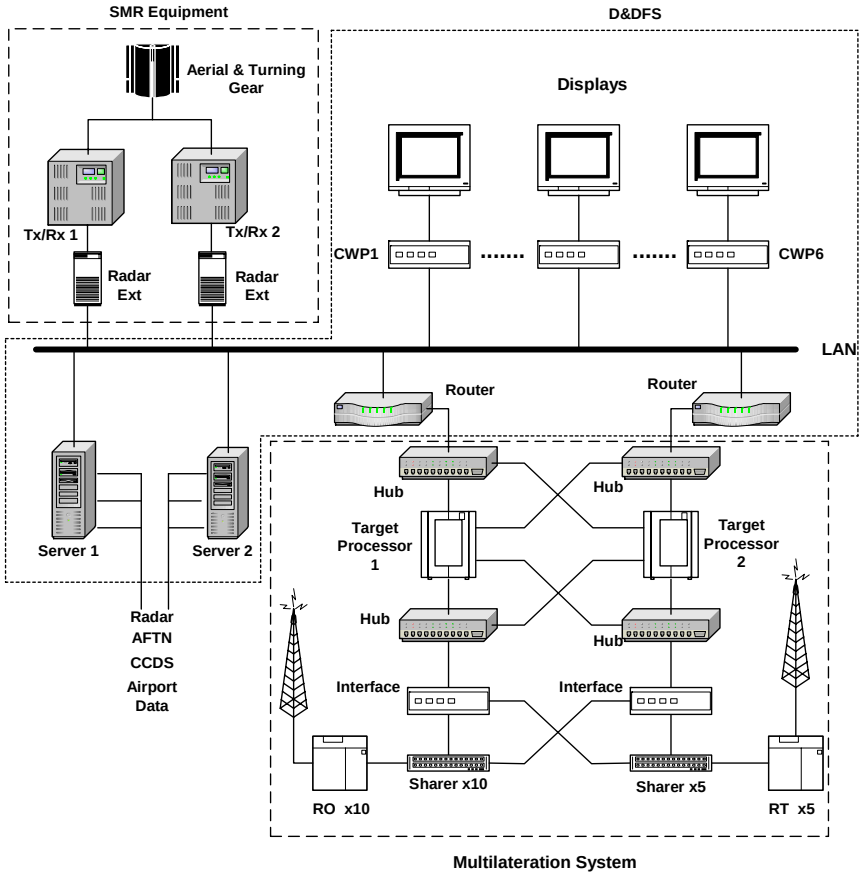


Figure 4: Heathrow A-SMGCS architecture

SMR system

2.3.18

The main elements of the SMR are as follows:

- Reflector antenna;
- Turning gear;
- Radome;
- Transmitters;
- Receivers;
- Processing.

2.3.19

Monitoring – the system monitors various elements to indicate the state of the system, as follows:

- Transmitted power;

- Noise figure;
- Magnetron state;
- 48V power supply state;
- High voltage state;
- Low voltage state;
- Turning gear state;
- Radome state;
- Cabin temperature and fire alarm state;

2.3.20

Control – control can be effected by the system itself (in the event of partial failure), or manually using the control and monitoring system. The following automatic control functions are available:

- Transmitter trip – in the event that the system detects situations that may cause damage to the system or personnel, the Security Card will stop transmission. Note that, normally only one transmitter would trip. The other transmitter would continue to function and provide a service;
- Master/slave changeover – when a transmitter trips, it is necessary to ensure that the remaining transmitter is master.

2.3.21

Control can also be effected manually using the control and monitoring PC or the front panel of the transmitters.

Display and Data Fusion Systems

2.3.22

Within the implementation at London Heathrow, the functions of the display and the Data fusion system considered in the FHA and PSSA are a single system. This analysis assesses the performance of this single system against the safety requirements.
The implementation at London Heathrow consists of:

- two servers;
- six display processors;
- a control and monitoring processor;
- two routers and three LAN switches.

Display system

2.3.23

The Display Processors overlay the digitised radar video onto maps of the airfield. Additionally they label the blips with their callsign, display the callsign of impending arrivals, and warn the user of runway incursions. A control panel and rollerball driven menu system is used to control the configuration of the display. The operator can set the displayed range, screen centre, map selection, brightness, radar trails etc.

2.3.24

Six Display Processors are used at Heathrow. The picture is displayed on liquid crystal displays in the VCR. The video distribution system will allow operators to view any other's screen (but not to control it). This provides a fall-back, so that the operator can still see a picture in the event of a display processor fault.

Data Fusion system

2.3.25

The servers are responsible for:

- carrying out multi-sensor tracking on data received from the MDS and radar extractor, and controlling how the radar extractors track the blips (for example initiating and terminating tracks);
- gathering data from the external sources and associating it with the tracks produced by the radar extractors, allowing labelling to take place;
- detecting situations where tracked targets may be in conflict with each other.

2.3.26

One server is master, whilst the other is in hot standby. The master server constantly updates the slave with the system status, so that it can take over as master at any time. Note that the servers play no part in the display of SMR video.

2.3.27

Each server receives track data from the active MDS processor, the approach radar and the active radar extractor. A track fusion process in the master server combines these sources of data, to produce a best track position. Each sensor is weighted according to the known performance.

2.3.28

The servers receive data from the following sources: AFTN, Code Call sign system, station time source and airport database. The AFTN and airport database are used to compile a flight information database. Targets are normally identified using the Mode A code to interrogate CCDS to obtain the callsign. The callsign is then used as the key to extract data from the flight information database.

2.3.29

The servers carry out runway incursion monitoring. When the server determines that an aircraft is at a predetermined time or distance from touchdown, it searches the runway area for any tracked targets. If any are found, a stage one alert is raised on the display, causing the labels of the landing and intruding targets to turn amber. If after a second, shorter time or distance from touchdown the tracked target is still in the runway area a stage two alert is raised, causing the labels to turn red. An audible alarm can also be sounded. Similarly the system can also detect when two or more targets are on a departure runway (stage one) and it will detect if one target starts accelerating towards the other. All the parameters associated with runway incursion monitoring can be configured via password protected menus on the Control and Monitoring system.

3. SAFETY ARGUMENT

3.1 Introduction

3.1.1

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 shaded items in the safety argument are the responsibility of the States. The other items show where the information in the PSC supports the safety argument.

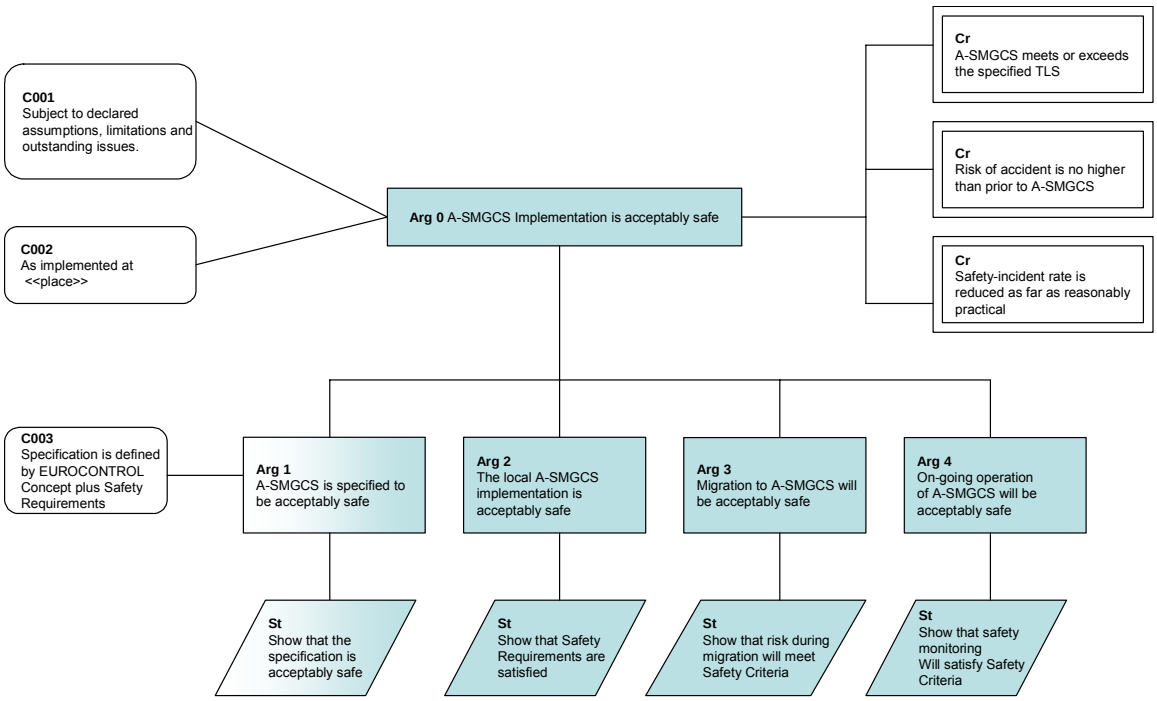


Figure 5: Overall Safety argument for A-SMGCS in ECAC

3.1.2

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 Preliminary Safety Case. It decomposed in the following figure.

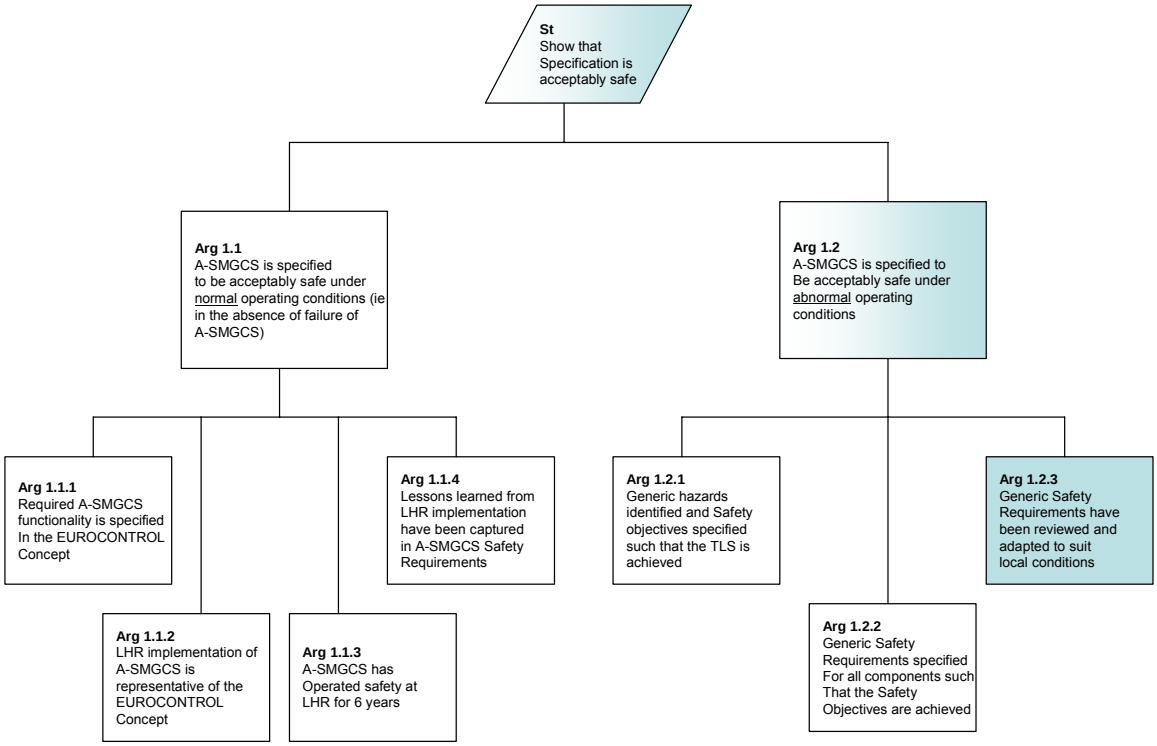


Figure 6: Specification of Safety Requirements

3.1.3

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).

3.1.4

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

3.1.5

Arg 1.1.1 asserts that the system is consistent with the EUROCONTROL definition of A-SMGCS as specified in references 1-4.

3.1.6

The case for acceptably safe normal operations is 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)** and are detailed in section 5 of the PSC.

3.1.7

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 is addressed in section 6 of the PSC.

3.1.8

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 is addressed in section 6 of the PSC.

3.1.9

The Safety Objectives and Safety Requirements have been 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**).

3.1.10

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

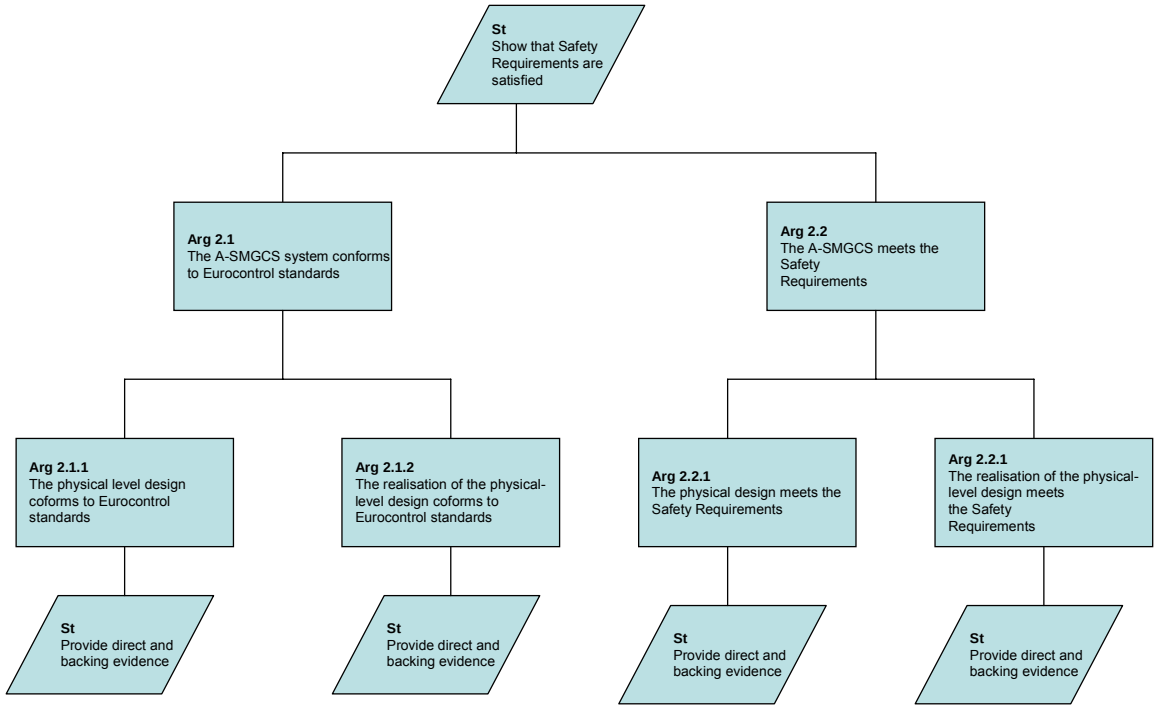


Figure 7: Local safety case argument for A-SMGCS

3.1.11

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.

3.1.12

Arg 2.1 asserts that the system conforms to EUROCONTROL specifications. The Preliminary Safety Case has been applied to the EUROCONTROL specifications and procedures. It is further broken down into:

3.1.13

Arg 2.1.1 asserts that the physical design conforms to EUROCONTROL standards (references 1-4).

3.1.14

Arg 2.1.2 asserts that the realization of the physical design conforms to EUROCONTROL standards (references 1-4).

3.1.15

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

3.1.16

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 and details are provided in section 6.

3.1.17

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 and details are provided in section 6.

3.1.18

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 it is the implementers responsibility to show that the decomposition of the argument, and the evidence to support it, are adequate.

3.1.19

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 it is the implementers responsibility to show that the decomposition of the argument, and the evidence to support it, are adequate.

4. NORMAL OPERATIONS (ARGUMENT 1.1)

4.1 Introductions

4.1.1

The evidence that A-SMGCS is acceptably safe, in principle, when working normally (ie in the absence of failure is developed as follows:

- That the required functionality is specified in the EUROCONTROL Concept for A-SMGCS and that the system being assessed is consistent with the EUROCONTROL definition for A-SMGCS;
- That a system conforming to the EUROCONTROL Concept for A-SMGCS has been operated safety for six years (as in the case of London Heathrow);

- That lessons learned from the operation of A-SMGCS have been addressed as part of the Safety Case;

4.1.2

The following sub-sections provide evidence supporting the measures undertaken for safe operation and evidence of the Safety Benefits offered by A-SMGCS Level II.

4.2 Measures Undertaken for Safe Operation

4.2.1

This section describes some of the measures undertaken to ensure safe operations of the A-SMGCS at Heathrow. These measures include:

- Ensuring the professional competence of controllers;
- Communication with airlines and aircrew;
- The implementation of a safety management system.

4.3 Technical Training of Controllers

4.3.1

The identification procedures for A-SMGCS were basically the same as those that were already established for SMR so no formal training in this aspect of the A-SMGCS was given to controllers.

4.3.2

Training was however given into the use of the revised HMI. This took the form of “cascade training” whereby the Watch Training Officer (WTO [a controller responsible for the administration of controller training within the watch]) was given specific instruction into the operation of the HMI. The WTO would then pass this information down to the remaining controllers on their watch who would then be tested to ensure their understanding.

4.4 Communication with Airline Operators / Aircrew

<u>UK AIP Entry</u>

4.4.1

The transponder setting procedures that were required for operations at Heathrow were published in the United Kingdom Air Pilot (UK AIP) approximately 12 months prior to the implementation of A-SMGCS procedures. These have since been modified in line with EUROCONTROL requirements and will very shortly be modified again to include transponder procedures to be applied following parking.

Letters to Airlines

4.4.2

In November 2002, all airlines that operate into Heathrow were sent a letter reminding them of the required transponder setting procedure along with a request for them to highlight these to their crews.

4.5 Safety Management

Unit Safety Case (USC)

4.5.1

Under the NATS Safety Management System (SMS), each ATSU is required to have a USC which contains reasoned argument intended to prove the safety integrity of the unit. The USC contains details of all equipment in use, its safety case and the purpose for which it is used, both as a stand alone item together with how it is used within the ATS system as a whole. The SMS tracks any shortcomings of the equipment and its associated procedures.

4.5.2

A thorough safety case was developed for A-SMGCS at Heathrow

A-SMGCS Accident/Incident History

4.5.3

Although the A-SMGCS may have been the subject of Mandatory Occurrence Reports (MOR) due to system failures, none of these have resulted in an accident or incident.

5. ABNORMAL OPERATIONS (ARGUMENT 1.2)

5.1 Objective

5.1.1

This section develops evidence that A-SMGCS is acceptably safe in ‘abnormal’ operations. This is proved by demonstrating that A-SMGCS meets or exceeds the specified Target Level of Safety.

The argument is developed as follows:

- Define a target level of safety for A-SMGCS (details of how the TLS was defined can be found in annex D);
- Apply the EUROCONTROL Safety Assessment Methodology (SAM) to develop safety objectives such that the TLS is achieved;

- Developing safety requirements for the A-SMGCS components such that the safety objectives are satisfied;
- Providing evidence that a 'typical' implementation of A-SMGCS meeting the safety requirements is achieved by using the LHR implementation as a case study.
- Review the allocation of the TLS to safety objectives if required to demonstrate that the safety requirements have met.

5.2 Hazards and Safety Objectives (Argument 1.2.1)

5.2.1

Hazards and safety objectives are defined for the three A-SMGCS functions, namely Position, Identification and Conflict Prediction functions.

5.2.2

Event trees are used to calculate the acceptable probability of a hazard occurring, i.e. the safety objective.

5.2.3

Supporting information can be found in:

- Annex E presents details of the process and results of the hazard analysis;
- Annex F presents all the event trees for each A-SMGCS Hazard. **Table 1** summarises the safety objectives for A-SMGCS.

5.2.4

The total credible failures[1] with safety consequences and their severity classification are illustrated in **Table 1**. These are grouped into a set of common Hazards (labelled H01 through H10).

[1] During the validation workshop (Oslo, December 2004) it was agreed that all possible hazards had been identified.

HZ	Hazard	Safety Objective (per movement)
H01	Total loss of A-SMGCS	2.96E-06
H02	Loss of the position function for one aircraft	2.82E-04
H03	Loss of the position function impacting multiple aircraft	1.51E-05
H04	Corruption of the position function for one aircraft	1.54E-04
H05	Corruption of the position function impacting multiple aircraft	1.83E-04
H06	Total loss the identification function	1.83E-04
H07	Loss of the identification function impacting multiple aircraft	1.83E-04
H08	Corruption of the identification function for one aircraft	7.90E-05
H09	Corruption of the identification function impacting multiple aircraft	5.52E-05
H10	Corruption of the conflict prediction function	1.22E-03

Table 1: Summary of credible failures for each hazard and their associated safety objective

5.2.5

Note that *delay* is treated as a special case of *corruption* and not listed in **Table 1**.

5.2.6

The ten hazards occur at the boundary of each function, as illustrated in **Figure 5**

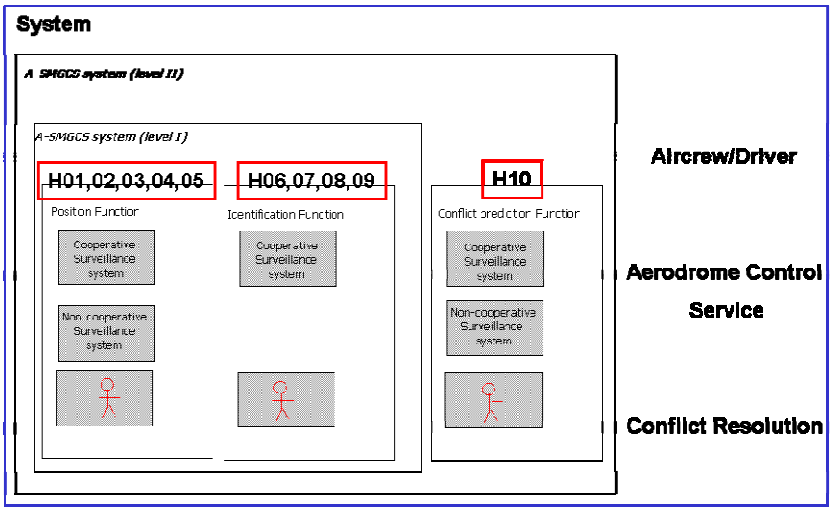


Figure 5: Hazards occur at functional boundaries

5.3 Safety Requirements (Argument 1.2.2)

5.3.1

Safety requirements are defined for each system element. Supporting information can be found in Annex G which presents the detailed fault tree for each safety objective. The safety requirements are summarised in **Table 2**

HZ	Hazard	Safety Objective (per movement)	System safety requirements (per movement)				
			Display	Data Fusion	Sensors	Code Callsign	Conflict Prediction
H01	Total loss of A-SMGCS	2.96E-06	9.75E-07	9.75E-07	1.00E-06	N/A	N/A
H02	Loss of the position function for one aircraft	2.82E-04	9.30E-05	9.30E-05	9.58E-05	N/A	N/A
H03	Loss of the position function impacting multiple aircraft	1.51E-05	4.97E-06	4.97E-06	5.12E-06	N/A	N/A
H04	Corruption of the position function for one aircraft	1.54E-04	5.09E-05	5.09E-05	5.25E-05	N/A	N/A
H05	Corruption of the position function impacting multiple aircraft	1.83E-04	6.05E-05	6.05E-05	6.23E-05	N/A	N/A
H06	Total loss the identification function	1.83E-04	6.05E-05	6.05E-05	6.23E-05	N/A	N/A
H07	Loss of the identification function impacting multiple aircraft	1.83E-04	6.05E-05	6.05E-05	6.23E-05	N/A	N/A
H08	Corruption of the identification function for one aircraft	7.90E-05	1.97E-05	1.97E-05	1.97E-05	1.97E-05	N/A
H09	Corruption of the identification function impacting multiple aircraft	5.52E-05	1.38E-05	1.38E-05	1.38E-05	1.38E-05	N/A
H10	Corruption of the conflict prediction function	1.22E-03	N/A	N/A	N/A	N/A	1.22E-03

Table 2: Safety requirements per system components (per movement)

5.3.2

The relationship of the safety requirements between cooperative and non-cooperative sensors is summarised in **Table 3**.

HZ	Hazard	Cooperative Sensor	Non Cooperative sensor
H01	Total loss of A-SMGCS	1.00E-03	1.00E-03
H02	Loss of the position function for one aircraft	9.79E-03	9.79E-03
H03	Loss of the position function impacting multiple aircraft	2.26E-03	2.26E-03
H04	Corruption of the position function for one aircraft	2.62E-05	2.62E-05
H05	Corruption of the position function impacting multiple aircraft	3.11E-05	3.11E-05
H06	Total loss the identification function	6.23E-05	N/A
H07	Loss of the identification function impacting multiple aircraft	6.23E-05	N/A
H08	Corruption of the identification function for one aircraft	1.97E-05	N/A
H09	Corruption of the identification function impacting multiple aircraft	1.38E-05	N/A
H10	Corruption of the conflict prediction function	N/A	N/A

Table 3: Safety requirements per sensor type (per movement)

5.4 Safety Requirements Achievability in a Typical Implementation (Argument 2)

5.4.1

The performance of the LHR A-SMGCS system is used to validate that the safety requirements defined for the A-SMGCS Concept are achievable. Each safety requirement is assessed individually, by gathering evidence from LHR for each component. Evidence is provided through the following means:

- Site acceptance tests, which were undertaken following the installation of the system to determine that the system performance achieves the original purchase specification and can be used operationally;
- Historical, where evidence exists at the LHR implementation. Data is examined as part of this analysis to determine whether the current system is still performing to the requirements;
- System specifications: where the system was required to achieve a certain level of performance. These requirements may have existed either through the original NATS system specification, or the design criteria used by the manufacture in the system architecture;
- Interviews: where physical evidence is not obtainable, particularly with reference to the ability of the controller to meet the required detection rate from the PSSA, interviews will be used to determine whether the requirement is achievable;

- Trials carried out previously at LHR.

Operational parameters at LHR

5.4.2

A number of statements based on the operations at Heathrow are used during the conversion of units, these are:

- A failure of the system does not immediately result in a 'safety significant event'. A failure will only become safety relevant after 12 seconds. This was agreed during the FHA workshops by operational aerodrome controllers (however on subsequent discussion with London Heathrow controllers this was reduced to the more stringent 3 seconds for this safety assessment);
- 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.

Heathrow Safety Requirements

5.4.3

In order to use the generic requirements for the Heathrow Case, the number of movements per hour should be taken into account to derive safety requirements per hour. Heathrow safety requirements are presented in **Table 4**.

HZ	Hazard	Safety requirements (per hour)						
		Display and data fusion	Sensors	Code Callsign	Conflict Prediction		MLAT	SMR
H01	Total loss of A-SMGCS	3.25E-05	1.67E-05	N/A	N/A		1.67E-02	1.67E-02
H02	Loss of the position function for one aircraft	3.10E-03	1.60E-03	N/A	N/A		1.63E-01	1.63E-01
H03	Loss of the position function impacting multiple aircraft	1.66E-04	8.54E-05	N/A	N/A		3.77E-02	3.77E-02
H04	Corruption of the position function for one aircraft	1.70E-03	8.74E-04	N/A	N/A		4.37E-04	4.37E-04
H05	Corruption of the position function impacting multiple aircraft	2.02E-03	1.04E-03	N/A	N/A		5.19E-04	5.19E-04
H06	Total loss the identification function	2.02E-03	1.04E-03	N/A	N/A		1.04E-03	N/A
H07	Loss of the identification function impacting multiple aircraft	2.02E-03	1.04E-03	N/A	N/A		1.04E-03	N/A
H08	Corruption of the identification function for one aircraft	6.58E-04	3.29E-04	3.29E-04	N/A		3.29E-04	N/A
H09	Corruption of the identification function impacting multiple aircraft	4.60E-04	2.30E-04	2.30E-04	N/A		2.30E-04	N/A
H10	Corruption of the conflict prediction function	N/A	N/A	N/A	2.03E-02		N/A	N/A

Table 4: Safety requirements (per hour) for Heathrow airport

Performance of LHR relating to the technical system

5.4.4

Annex H presents the detailed evidence for the contributing technical elements for each hazard.

5.4.5

The primary source of evidence is based on the fact that, at LHR, detailed system specifications were defined to meet or exceed the safety requirements specified for each element. The delivered system was thoroughly tested during Factory and Site Acceptance Testing.

5.4.6

In many cases, secondary supporting evidence is presented based on reliability modelling and historical operational experience from the use of the A-SMGCS system over the previous five years.

5.4.7

The evidence associated with each safety requirement is summarized in **Table 5**.

HZ	Hazard	Order of magnitude for the evidence at LHR						
		Display and data fusion	Sensors	Code Callsign	Conflict Prediction		MLAT and avionics	SMR
H01	Total loss of A-SMGCS	1.00E-06	1.30E-10	N/A	N/A		1.00E-04	1.30E-06
H02	Loss of the position function for one aircraft	2.00E-05	1.88E-05	N/A	N/A		1.50E-03	1.25E-02
H03	Loss of the position function impacting multiple aircraft	2.00E-05	3.52E-10	N/A	N/A		2.25E-06	1.56E-04
H04	Corruption of the position function for one aircraft	Not Credibl	2.79E-04	N/A	N/A		4.90E-05	2.30E-04
H05	Corruption of the position function impacting multiple aircraft	Not Credibl	5.43E-07	N/A	N/A		4.90E-07	5.29E-08
H06	Total loss the identification function	1.00E-04	N/A	N/A	N/A		N/A	N/A
H07	Loss of the identification function impacting multiple aircraft	1.00E-04	1.00E-06	N/A	N/A		1.00E-06	N/A
H08	Corruption of the identification function for one aircraft	2.00E-05	1.50E-04	1.00E-06	N/A		1.50E-04	N/A
H09	Corruption of the identification function impacting multiple aircraft	2.00E-05	1.00E-06	1.00E-06	N/A		1.00E-06	N/A
H10	Corruption of the conflict prediction function	Not Credibl	N/A	N/A	1.79E-02		N/A	N/A

Note that the avionics failure is included in the MLAT failure

Table 5: Performance of the LHR A-SMGCS implementation

Conclusions of LHR relating to the technical system

5.4.8

Table 6 indicates the safety margin between the performance of the NATS system and the safety requirements.

5.4.9

The results of the analysis are:

- The safety requirements for the A-SMGCS Level 1 and 2 concepts are achieved at LHR.

HZ	Hazard	Results of LHR assessment (order of magnitude difference between requirement and perfromance						
		Display and data fusion	Sensors	Code Callsign	Conflict Prediction		MLAT	SMR
H01	Total loss of A-SMGCS	1	5	N/A	N/A		2	4
H02	Loss of the position function for one aircraft	2	1	N/A	N/A		2	1
H03	Loss of the position function impacting multiple aircraft	0	5	N/A	N/A		4	2
H04	Corruption of the position function for one aircraft	Not Credible	0	N/A	N/A		0	0
H05	Corruption of the position function impacting multiple aircraft	Not Credible	3	N/A	N/A		3	3
H06	Total loss the identification function	1	N/A	N/A	N/A		N/A	N/A
H07	Loss of the identification function impacting multiple aircraft	1	3	N/A	N/A		3	N/A
H08	Corruption of the identification function for one aircraft	1	0	2	N/A		0	N/A
H09	Corruption of the identification function impacting multiple aircraft	1	2	2	N/A		2	N/A
H10	Corruption of the conflict prediction function	Not Credible	N/A	N/A	0		N/A	N/A

Note that the avionics failure is included in the MLAT failure

safety requirement not achieved
order of magnitude same or less that 10 times greater
order of magnitude between 10 and 100 times greater
order of magnitude greater than 100 times

Table 6: Order of magnitude difference between each safety requirement and the performance at LHR

6. CONCLUSIONS

6.1 Assumptions and Issues

6.1.1

The A-SMGCS preliminary safety case has been developed based on a number of assumptions. These results of the A-SMGCS preliminary safety case are only valid if these assumptions are valid. When stakeholders develop their local safety cases then all the assumptions shall be validated.

6.1.2

The key assumptions relate to:

- Weather (the proportion of time an airport is in visibility condition 1, 2, 3 or 4);
- Airport layout (the proportion of time an aircraft is on the taxiway or runway);
- Controller and pilot performance (the detection rate of an A-SMGCS failure).

6.1.3

The evidence to support the argument has been developed, in part, based on a 'case-study' (London Heathrow). Stakeholders should review all the assumptions regarding LHR evidence to ensure it remains valid for their local implementation.

6.2 Conclusions

6.2.1

The A-SMGCS preliminary safety case has shown that the safety requirements for A-SMGCS Level 1 and 2 can be implemented.

6.2.2

The level 2 performance was assessed following a programme of improvements at LHR involving two new SMRs being added together with upgrades to the data fusion system, so that false targets from the sensors do not generate runway incursion monitoring false alert. This has resulted in an improved performance of the Level II alerting function.

6.2.3

The preliminary safety case has focussed on developing safety requirements and showing that these are achievable. The full case for implementation of A-SMGCS should also address the operational and safety benefits offered by A-SMGCS. A generic cost benefit analysis for A-SMGCS has been developed by EUROCONTROL that addresses this issue (reference 11).

6.2.4

A great number of assumptions have been made during the analysis relating to operational aspects of A-SMGCS and the implementation decisions that have been made at Heathrow. These assumptions and implementation details are very unlikely to be valid at other airports in Europe and should be re-validated on a 'case-by-case' basis.

6.2.5

This document is not intended to replace the safety cases that shall be performed by stakeholders for their local implementation.

A References

1. EUROCONTROL Definition of A-SMGCS Implementation Levels (Edition 1.0, 30/9/03)

2. EUROCONTROL Operational Concept & Requirements for A-SMGCS Implementation Level 1 (Edition 1.0, 30/9/03)

3. EUROCONTROL A-SMGCS Operating Procedures (Edition 1.0, 25/2/04)

4. EUROCONTROL Functional Specification for A-SMGCS Implementation Level 1 (Edition 1.0, 30/9/03)

5. EUROCAE ED87a, Minimum Aviation System Performance Specification for A-SMGCS (December 2000)

6. EUROCONTROL Operational Concept & Requirements for A-SMGCS Implementation Level 12 (Edition 1.0, 30/9/03)

7. EUROCAE ED 117 - MINIMUM OPERATIONAL PERFORMANCE SPECIFICATION FOR MODE S MULTILATERATION SYSTEMS FOR USE IN ADVANCED SURFACE MOVEMENT GUIDANCE AND CONTROL SYSTEMS

8. EUROCAE ED 116 - MINIMUM OPERATIONAL PERFORMANCE SPECIFICATION FOR SURFACE MOVEMENT RADAR SENSOR SYSTEMS FOR USE IN ADVANCED SURFACE MOVEMENT GUIDANCE AND CONTROL SYSTEMS

9. ICAO Annex 11 ATS and Annex 14 ‘ Aerodromes’

10. SRC Document 2. 12 December 2002 version 3.0

11. EUROCONTROL Final Report on the Generic Cost Benefit Assessment of A-SMGCS, Version 0.2, 4th August 2006

B Acronyms and Abbreviations

ADS-B	Automatic Dependant Surveillance – Broadcast
A-SMGCS	Advanced Surface Movement, Guidance and Control System
ATM	Air Traffic Management
ATM	Air Traffic Monitor
ATS	Air Traffic Service
C	Constraint
Cr	Criteria
EATMP	European Air Traffic Management Programmes
ENAV	Ente Nazionale di Assistenza Al Volo
ESARR	EUROCONTROL Safety Regulatory Requirement
EUROCAE	European Organisation for Civil Aviation Equipment
FHA	Functional Hazard Assessment
IFATCA	International Federation of Air Traffic Controllers' Associations
LVNL	Luchtverkeersleiding Nederland
LVP	Low Visibility Procedures
MASPS	Minimum Aviation System Performance Specification
NATS	National Air Traffic Services
PSSA	Preliminary System Safety Assessment
SAM	Safety Assessment Methodology
SMR	Surface Movement Radar
SO	Safety Objective
SR	Safety Requirement
SRC	Safety Regulation Commission
SSA	System Safety Assessment
St	Strategy
TLS	Target Level of Safety
TMA	Terminal Manoeuvring Area
RIMCAS	Runway Intrusion Monitoring and Collision Avoidance System
CCDS	Code Callsign Distribution System
NAS	National Airspace System

C Approach to developing the failure case argument.

C.1 Overview of the EUROCONTROL safety assessment methodology used in this preliminary safety case

C.1.1 The project applies the EATMP Air Navigation System Safety Assessment Methodology (EAM 4/AMC 1).

C.1.2 The objective of the method is to define the means for providing assurance or evidence, that an Air Navigation System is safe for operational use.

C.1.3 This EUROCONTROL SAM process consists of three major steps as illustrated in **Figure 6**[2]:

- Functional Hazard Assessment (FHA), defining how safe the A-SMGCS should be;
- Preliminary System Safety Assessment (PSSA), resulting in a safe design;
- System Safety Assessment (SSA) results in a safe implementation and operational use.

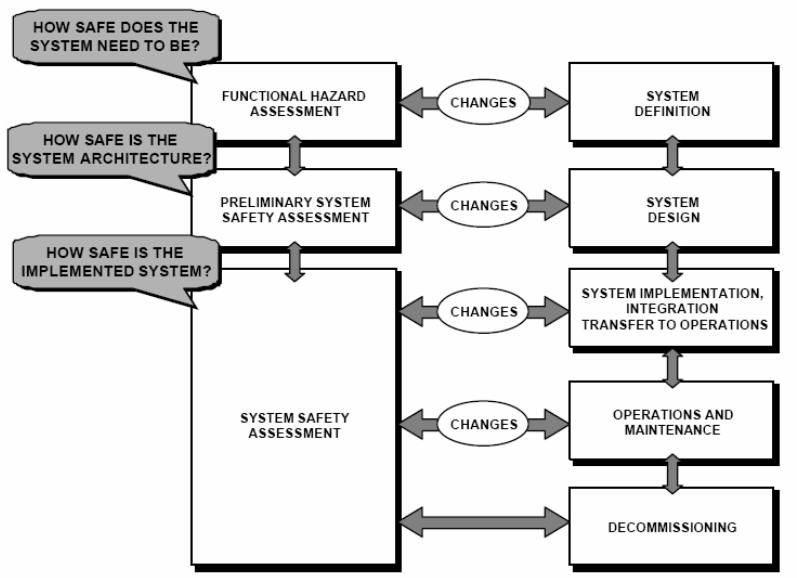


Figure 6: EUROCONTROL SAM

Functional Hazard Assessment

C.1.4 The FHA is[3] "…a top-down iterative process, initiated at the beginning of the development or modification of an Air Navigation System. The objective of the FHA process is to determine how safe does the system need to be. The process identifies potential failures and hazards. It assesses the consequences of their occurrences on the safety of aircraft operations, within a specified operational

[2] Source SAF.ET1.ST03.1000-MAN-00-00
[3] SAF.ET1.ST03.1000-MAN-01-00

environment. The FHA process specifies overall Safety Objectives of the system, i.e. specifies the risk level to be achieved by the system."

C.1.5 The objective of the FHA is to document potential hazards in the FHA process and estimate their potential consequences in order to derive a set of safety objectives.

C.1.6 The FHA for this project is described in this annexes E and F.

PSSA

C.1.7 The objective of performing a PSSA is to define, based on the safety objectives, a set of safety requirements[4] on the A-SMGCS system components so that it can reasonably be expected to achieve the Safety Objectives specified in the FHA.

C.1.8 The PSSA process apportions Safety Objectives into Safety Requirements allocated to the A-SMGCS elements and demonstrates that the safety requirements are achievable. Note that this is an iterative process in which the apportionment was reviewed and adjusted such that safety requirements could be achieved.

C.1.9 The PSSA for this project is described in annexes G and H.

SSA

C.1.10 The SSA is not performed in the Preliminary Safety Case

[4] A Safety Requirement is a risk mitigation means, defined from the risk mitigation strategy that achieves a particular safety objective. Safety requirements may take various forms, including organisational, operational, procedural, functional, performance and interoperability requirements or environmental characteristics.

D Risk classification scheme and target level of safety.

D.1 Severity classification scheme

D.1.1 The workshops used the severity classification scheme illustrated in Annex M. This was simplified to the following:

D.1.2

Severity Class	Description
5	No impact on safety
4	Minor impact on workload or system functionality but all participants (i.e. controllers and aircrew) still believed the situation to be 'safe'.
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.
2	Significant impact on safety with a high probability of an accident.
1	Accident (i.e. loss of life or collision between mobiles)

Table 7: Simplified severity classification scheme

D.2 Risk classification scheme

D.2.1 This section derives the acceptable incident rate for A-SMGCS failures.

D.2.2 **Table 8** presents the distribution of accidents by phase of flight (taken from SRC DOCUMENT 2[5]). This is used to derive the proportion of fatal accidents that occur at the aerodrome.

Phase of flight and region	Western Europe	North America	Total accidents world-wide	Accident rate by phase of flight*
Taxi	27	80	129	0.307
Missed approach / go-around	1		1	0.002
En route	3	11	21	0.050
Take off	2	5	11	0.026
Landing	3	8	14	0.033
Approach	1	8	17	0.040
Total accidents	37	112	193	0.460
Accident rate by region	0.530	0.450	0.460	

Table 8: Distribution of fatal accidents and accident rate (per million flights) by phase of flight

[5] See http://www.EUROCONTROL.int/src/documents/deliverables/srcdoc2_e30_ri_integrated.pdf

D.2.3 The proportion of accidents which occur at the aerodrome in Western Europe are the sum of taxi (27), Missed approach (1), Take off (2) and Landing (3). This shows that 90% of all Western European fatal accidents have occurred at the aerodrome, as illustrated in **Figure 7**

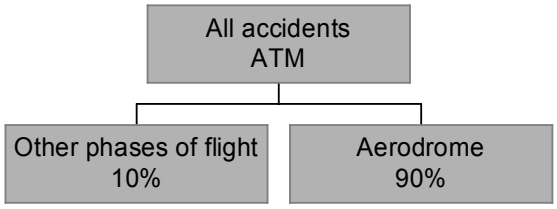


Figure 7: Deriving the proportion of accident at Aerodromes

D.2.4 For the purpose of this FHA, it is assumed that the 90% of all accidents occur at aerodromes.

Maximum acceptable probability of an accident at an aerodrome

D.2.5 ESARR 4 defines a maximum acceptable probability of ATM directly contributing to an accident of a commercial Air Transport aircraft of 2.31E-8 accidents per flight.

D.2.6 The ESARR 4 tolerability figure is used as a basis to derive the maximum acceptable probability of an accident per flight at aerodromes.

D.2.7 For aerodrome operations, it is estimated that the maximum acceptable probability of an accident is 2.079E-8 per flight (i.e. 90% of 2.31E-8 per flight) as illustrated in **Figure 8**

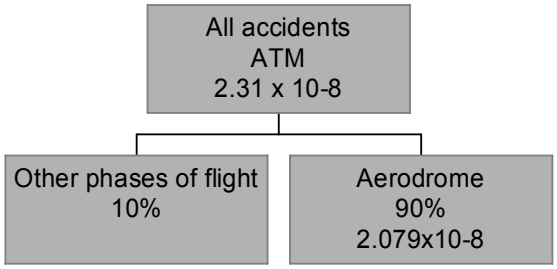


Figure 8: Deriving the accident frequency at Aerodromes for severity class 1

Maximum acceptable probability of an accident of SMGCS

D.2.8 The maximum acceptable probability of an accident of 2.079E-8 per flight for the complete aerodrome operations and was derived when A-SMGCS was not in operation.

Type of event	Fatal Accidents
Collision with Vehicle	1
Collision with standing aircraft on the ground	1
Collision with moving aircraft on the ground	6
Collision/near collision with aircraft – both airborne	14
Landing aids related	4
Aircraft encountered vortex/wake turbulence	0
Collision with Aircraft – on airborne	1
Total	27

Table 9: Distribution of accidents and accident rate (per million flight) by type of event during the taxi phase (extracted from SRC Document 2)

D.2.9 Data presented in **Table 9** provides an indication of the causes of accidents during the taxi phase The other significant aerodrome related accidents from **Table 8** (i.e. take-off, missed approach and landing) account for 6 of the accidents (i.e. 18% of accidents). Assuming 50% of these occur whilst the aircraft is under control using some form of SMGCS then this accounts for an additional 9%.

D.2.10 Data from **Table 8** and **Table 9** is used to estimate a maximum acceptable probability for severity class 1 for the SMGCS (i.e. the old system prior to A-SMGCS implementation). The data suggests that 94% of all past accidents at the aerodrome occurred within the influence or scope of the SMGCS.

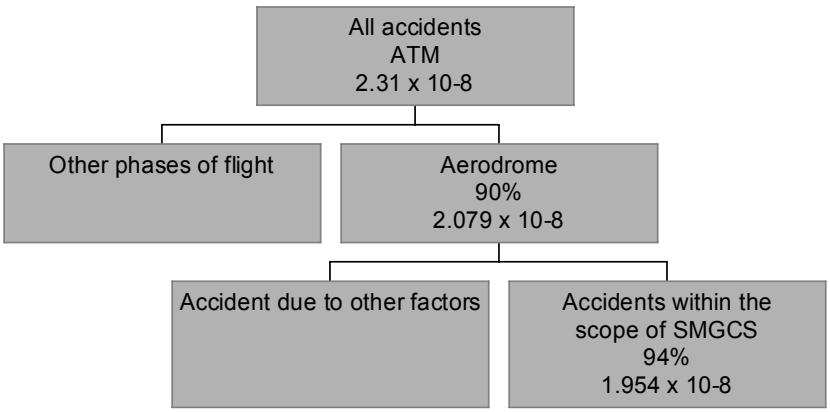


Figure 9: Deriving the accident frequency at Aerodromes for severity class 1

D.2.11 The target level of safety for accidents within the scope of SMGCS is 1.954E-8.

Maximum acceptable probability of an accident for A-SMGCS

D.2.12 In the future A-SMGCS will be implemented and contribute to the TLS for SMGCS. For the purpose of this FHA, it is assumed that the proportion of accidents per flight which A-SMGCS may influence in the future is 15% .

D.2.13 Therefore based on historical data and the assumptions outlined above, the acceptable probability of a severity Class 1 incident caused by the A-SMGCS shall be not more than 2.931E-9.

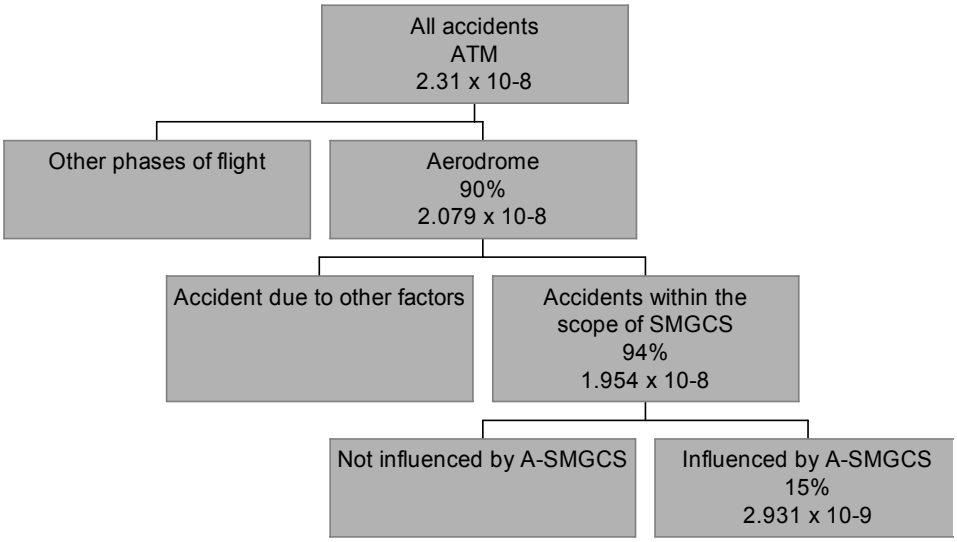


Figure 10: Deriving the accident frequency at Aerodromes for severity class 1

D.2.14 Therefore the acceptable accident rate caused by A-SMGCS is 2.931E-9 per flight.

D.2.15 A flight is two movements (take-off and landing). Therefore the acceptable risk of an accident caused by the A-SMGCS is 1.5E-9 per movement.[6]

D.3 Relationship between risk per severity classification

D.3.1 The relationship between the acceptable probabilities for each severity class is a factor of 100. Therefore the risk classification scheme for A-SMGCS failures per severity class is illustrated in **Table 10**.

D.3.2 Note that because safety objectives are only defined for those consequences of severity 1 to 4 (i.e. those consequence with no effect have no safety objectives defined in this document) then no acceptable probability for severity class 5 is defined.

6 Note that ICAO ASGCS Manual have defined (in section 4.2.1.1) the A-SMGCS TLS should be 1 x 10-8 (per operation) based on worldwide accident rates. The Function risk has been estimated as:

a) Guidance: 3.0 x 10-9 per operation;

b) Surveillance: 3.0 x 10-9 per operation;

c) Control: 3.0 x 10-9 per operation; and

d) Routing: 1.0 x 10-9 per operation.

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 10: Relationship between accident risk per severity classification

E Identifying Hazards

E.1 A-SMGCS assumptions used for developing safety objectives

E.1.1 A number of FHA workshops took place and were structured to identify the consequence on safety for an A-SMGCS failure if the failure occurred in different weather conditions and how many mobiles were impacted.

E.1.2 The consequence of a failure based on whether it occurred during:

- Visibility condition 1;
- Visibility condition 2;
- Visibility conditions 3,4.

E.1.3 Visibility conditions (as defined in A-SMGCS implementation levels 2.6.1) are described below.

- Condition 1: Visibility sufficient for the pilot to taxi and to avoid collision with other traffic on taxiways and at intersections by visual reference, and for personnel of control units to exercise control over all traffic on the basis of visual surveillance;
- Condition 2: Visibility sufficient for the pilot to taxi and to avoid collision with other traffic on taxiways and at intersections by visual reference, but insufficient for personnel of control units to exercise control over all traffic on the basis of visual surveillance;
- Condition 3: Visibility sufficient for the pilot to taxi but insufficient for the pilot to avoid collision with other traffic on taxiways and at intersections by visual reference with other traffic, and insufficient for personnel of control units to exercise control over all traffic on the basis of visual surveillance. For taxiing this is normally taken as visibilities equivalent to a RVR less than 400 m but more than 75 m;
- Condition 4: Visibility insufficient for the pilot to taxi by visual guidance only. This is normally taken as a RVR of 75 m or less.

E.1.4 The consequences on the failure for each of the three A-SMGCS functions, namely:

- Position;
- Identification;
- Conflict detection.

E.1.5 For each function a number of failure modes were considered. A failure mode is:

- Loss of Data;
- Misdirected Data;
- Delayed Data;
- Corruption of Data;
- Inconsistent Data;
- Spurious and Malicious Data.

E.1.6 If data is misdirected or delayed beyond a credible time and hence is not received by the appropriate Controller when required, it is treated as though it were lost. The effects would be the same as for the Loss of Data failure mode. Similarly, inconsistent, delayed, spurious and malicious data are examples of data corruption.

E.1.7 Therefore the failure modes can be consolidated into the following:

- Loss of the information provided by a function;
- Corruption of the information provided by a function, e.g. Inconsistent information or delayed;

E.1.8 The effect or consequence of a failure will impact on a number of systems within the aerodrome. The workshop participants assessed the effects on:

- the ability to provide a safe Service at the aerodrome;
- controllers working conditions (e.g. workload, ability to perform his/her tasks);
- Aircrew working conditions (e.g. workload, ability to perform his/her tasks);
- Aircrew and controllers ability to cope with adverse operational and environmental conditions;
- the functional capabilities of the aircraft (e.g. technology breakdown or inability to provide co-operative information);
- Effect on the functional capabilities of the ground part of the airport.

E.1.9 The FHA participants were asked to allocate a severity to a failure of a function if the failure were either Detected by the system or Undetected by the system

A-SMGCS operational assumptions.

E.1.10 During the Hazard analysis it was assumed that the failure occurred whilst operating under the following conditions:

- High traffic density;
- Complex;
- Peak Time;

E.1.11 The consequence of a A-SMGCS failure may be more severe dependent on the region of the aerodrome the aircraft or vehicle is at the time of the failure. The workshop participants agreed that hazards occurring on or in the immediate vicinity of the runway were likely to be of greater severity than hazards occurring elsewhere in the aerodrome and therefore hazard severity should be considered for the Runway Strip.

E.1.12 In addition, it was noted that the visual condition definitions do not take the time of day into account. The FHA workshop participants agreed that the most challenging time of day was during night operations in peak traffic (e.g. a winters evening)

E.1.13 The participants agreed that a short term system failure of up to 12 seconds would have no impact on operational safety for Level 1. Failures longer than 12 seconds will result in the consequence presented for each function.

Probabilities for calculating safety objectives

E.1.14 The workshop participants agreed a number of assumptions that are applied to all situations at the aerodrome. These 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 or, on landing, it is the proportion of time from 100 ft to arrival at the stand). The workshop agreed an estimate of 8% of time on the runway strip under visibility condition 1[7];
- the number of failures which would be detected by the controller. It was agreed this is 'context specific' and dependent upon the failure type, the visibility conditions and the location of the aircraft.

E.1.15 In addition it was noted that not all failures of the A-SMGCS would result in an incident, because at the time of the failure there may be no possibility of a safety significant event. For example an aircraft is taking off and the callsign becomes corrupted, or the aircraft is taxing back to the stand and is shown in the wrong position. At that particular time there is no safety impact and the controller does not need to intervene, however additional workload may be required to rectify the situation and the safety consequence is therefore 4.

E.1.16 It was agreed that a concept of 'fail to safe' should be included in the analysis to capture the fact that not all failures will automatically result in a safety incident. However, it was agreed that a significant event is context specific and dependent upon the failure type, visibility conditions and location of the aircraft.

E.2 Failure of the position function

E.2.1 This section presents the severity of the consequence of an A-SMGCS position function failure.

E.2.2 It was noted that when the position function fails the other two functions (identification and conflict prediction) also fail. Therefore this failure is equivalent to the complete A-SMGCS function failing.

Detected failure

E.2.3 The following table lists the results of the discussion at the workshop.

[7] Further discussion (December 2004 at Oslo) clarified that this proportion applies to Visibility condition 2, 3 and 4.

Ref.	Failure	Visibility Condition	Number of Mobile impacts	Discussion and Consequence	Severity Class	
					Taxi	RWY
P01	Detected total loss of A-SMGCS	1	All aircraft	Controller uses visual recognition and Aircrew will maintain safe distance. Flight Strips are available and are used to maintain situational awareness. Situation remains safe but a slight increase in workload is expected.	4	4
P02		2	All aircraft	Aircrew will maintain safe distance. Controller will request position reports and flight strips are still available and are used to maintain situational awareness. However in a high density complex environment, the situation may move to a less safe situation	3	3
P03		3 or 4	All aircraft	Aerodrome already handling reduced traffic and aircraft already under procedural control. Slight increase in workload of controllers but situation remains safe.	4	4
P04	Detected Partial Loss of the position function	1	=1	Controller uses visual recognition and Aircrew will maintain safe distance. Flight Strips still maintained. No effect	5	5
P05		2	=1	Aircrew will maintain safe distance. Flight Strips still maintained. Situation remains safe. No effect	5	5
P06		3 or 4	=1	Reduced traffic and aircraft already under procedural control. No effect	5	5
P07		1	>1	Consequence same as Total Loss of A-SMGCS (P02)	4	4
P08		2	>1	Consequence same as Total Loss of A-SMGCS (P01)	3	3
P09		3 or 4	>1	consequence same as Total Loss of A-SMGCS (P02)	4	4
P10	Detected Corruption of the position function	1	=1	Same as Partial Loss (P04)	5	5
P11		2	=1	Same as Partial Loss (P05)	5	5
P12		3 or 4	=1	Same as Partial Loss (P06)	5	5
P13		1	>1	Same as Partial Loss (P07)	4	4
P14		2	>1	Same as Partial Loss (P08)	3	3

Ref.	Failure	Visibility Condition	Number of Mobile impacts	Discussion and Consequence	Severity Class	
					Taxi	RWY
P15		3 or 4	>1	Same as Partial Loss (P09)	4	4

Table 11: Failure of Position – Detected Failure

Undetected failure

E.2.4 In many cases undetected failure of the position function is not credible because the controller would detect that the position and label were not present.

E.2.5 At the FHA workshop it was agreed that a controller would not notice that the position was missing unless he looked for it, in which case it would become a detected error. If the controller was not looking for it then it has no impact (because the aircraft was not being directly controlled at the time because control instructions at the time were not dependent on reference to the display). Therefore undetected loss is not credible failure modes

Ref.	Failure	Visibility Condition	Number of Mobile impacts	Discussion and Consequence	Severity Class	
					Taxi	RWY
P16	Undetected total loss of A-SMGCS	1	all aircraft	Not Credible; controller would recognize problem	N/A	N/A
P17		2	all aircraft	Not Credible; controller would recognize problem	N/A	N/A
P18		3	all aircraft	Not Credible; controller would recognize problem	N/A	N/A
P19	Undetected partial Loss of the position function	1	=1	A-SMGCS is a supplement to visual control and Aircrews are likely to contact tower if an unsafe instruction is issued. Aircraft also maintain own safe distance. Controller continues to use Flight Strips. No effect	5	5
P20		2	=1	Aircrews are likely to contact tower and will also maintain own safe distance. Controller continues to use Flight Strips. Not credible for long duration but will increase workload whilst remaining safe	4	4
P21		3 or 4	=1	Reduced traffic and Aircraft already under procedural control. However potential for unsafe situation to develop for one aircraft	3	3

Ref.	Failure	Visibility Condition	Number of Mobile impacts	Discussion and Consequence	Severity Class	
					Taxi	RWY
P22		1	>1	Aircrews are likely to contact tower if an unsafe instruction is issued and will also maintain own safe distance. Controller continues to use Flight Strips. Not credible for long duration	5	5
P23		2	>1	Aircrews are likely to contact tower and will also maintain own safe distance. Controller continues to use Flight Strips. Not credible for long duration but will increase workload whilst remaining safe	4	3
P24		3 or 4	>1	Reduced traffic and Aircraft already under procedural control. However potential for serious situation to develop.	2	2
P25	Undetected Corruption of the position function	1	=1	Controller will use visual acquisition of aircraft position but may not be able to determine exact position (e.g. at a large distance). Possible unsafe situation on the runway. No effect off the runway.	5	3
P26		2	=1	Possible unsafe situation on the runway. No effect off the runway.	5	2
P27		3 or 4	=1	More likely to remain undetected (this may also occur at the same time as an incorrect position report from pilot). If failure occurs near runway then no mitigations exist to prevent collision No effect off the runway	5	2
P28		1	>1	Not Credible; controller would recognize problem	N/A	N/A
P29		2	>1	Not Credible; controller would recognize problem	N/A	N/A
P30		3 or 4	>1	Not Credible; controller would recognize problem	N/A	N/A

Table 12: Failure of Position – Undetected Failure

E.3 Identification function

E.3.1 This section presents the severity of the consequence of an A-SMGCS identification function failure.

E.3.2 When the identification function fails the automatic track labeling no longer operates correctly and the mobile identification (aircraft identification or registration) is either not presented or is incorrect.

E.3.3 The loss or corruption of the identification function includes the scenario whereby the automatic labeling function fails and either the Mode A code is not available or the Mode A code is incorrect.

E.3.4 There are a number of potential causes of the loss of automatic labeling. These include human error (e.g. Aircrew enters incorrect information) and system failure (e.g. failure of the correlation function).

E.3.5 Note that, as per procedure, it is assumed that identification is confirmed prior to push-back.

Detected failure

E.3.6 The loss of the label does not necessarily mean the controller has lost the identification of the aircraft (because the mental picture is maintained and strips are still available). When the Loss or corruption is detected, possible actions available to the controller are:

- to not start up any more aircraft;
- gradually reduce traffic level;
- to stop any taxiing aircraft.

E.3.7 When any of these actions are taken, then the situation is still considered safe but a slight increase in workload may be required if the failure occurs for more than one aircraft (i.e. severity class 4).

Ref.	Failure	Visibility Condition	Number of Mobile impacts	Discussion and Consequence	Severity Class	
					Taxi	RWY
I01	Detected complete Loss of the identification function	1	all aircraft	Controller still retains identification however a slight increase in workload is predicted but condition still considered safe	5	4
I02		2	all aircraft	Controller still retains identification however an increase in workload is predicted but condition still considered safe. The controller will regulate traffic according to local rules and may stop outbound traffic if required	5	4

Ref.	Failure	Visibility Condition	Number of Mobile impacts	Discussion and Consequence	Severity Class	
					Taxi	RWY
I03		3 or 4	all aircraft	Controller still retains identification however an increase in workload is predicted but condition still considered safe. The controller will regulate traffic according to local rules and may stop outbound traffic if required	5	4
I04	Detected partial Loss of the identification function	1	=1	No impact. Controller retains identification of aircraft and may revert to strips	5	5
I05		2	=1	No impact. Controller retains identification of aircraft and may revert to strips	5	5
I06		3 or 4	=1	No impact. Controller retains identification of aircraft and may revert to strips	5	5
I07		1	>1	Same consequence as detected complete loss (I01)	5	4
I08		2	>1	Same consequence as detected complete loss (I02)	5	4
I09		3 or 4	>1	Same consequence as detected complete loss (I03)	5	4
I10	Detected corruption of the identification function	1	=1	No impact. Controller retains identification of aircraft and may revert to strips	5	5
I11		2	=1	No impact. Controller retains identification of aircraft and may revert to strips	5	5
I12		3 or 4	=1	No impact. Controller retains identification of aircraft and may revert to strips	5	5
I13		1	>1	Same consequence as detected complete loss (I01)	5	4
I14		2	>1	Same consequence as detected complete loss (I02)	5	4
I15		3 or 4	>1	Same consequence as detected complete loss (I03)	5	4

Table 13: Failure of Identification – Detected Failure

Undetected failure

E.3.8 At the workshops it was agreed that a controller would not notice that the label was missing unless he looked for it, in which case it would become a detected error. If the controller was not looking for it then it has no impact (because the aircraft was not being directly controlled at the time or because control instructions at the time were not dependent on reference to the display). Therefore undetected loss and partial loss are not credible failure modes.

E.3.9 A number of credible identification corruption examples were discussed at the FHA workshop. These were:

- Label swapping (i.e. at least two aircraft labels are transposed);
- Duplicate labels (i.e. at least two aircraft labels are identical);
- Incorrect aircraft identification.

E.3.10 Although the undetected corruption of aircraft identification was considered credible, the workshop participants considered it very unlikely a failure of this type (e.g. label swap) would always lead to a dangerous situation. It was suggested that, in the majority of cases it would result in aircrew querying a wrong clearance. Aircrews would mitigate most of the risk generated from mis-directed clearances issued as a result of the labels being wrong.

E.3.11 A number of scenarios were identified which may have serious safety consequences when a credible corruption occurs. These include:

- Multiple line-ups where the complete runway is not visible in visibility conditions 1 and 2. If the labels were swapped, it would be possible to clear the wrong aircraft for takeoff resulting in a potential collision8 ;
- When a controller has cleared an aircraft onto a runway and then a label swap occurs, then potentially the controller may clear the wrong aircraft to take-off first.

E.3.12 The workshop participants agreed that:

- undetected corrupted identification was one of the most dangerous situations that could occur on the aerodrome surface in particular the runway;
- there is no guarantee that aircrew will have situational awareness especially at night or in low visibility to mitigate this failure;
- when the corruption is detected (even for one aircraft) then confidence in the function would reduce;
- undetected delay has the same consequences as undetected loss.

E.3.13 The following table lists the results of the workshop discussion.

Ref.	Failure	Visibility	Number	Discussion and Consequence	Severity Class

[8] It is noted that the recent European Action Plan for the prevention of runway incursions recommends such procedures are not implemented.

					Taxi	RWY
I16	Undetected complete Loss of the identification function	1	all aircraft	Not Credible; controller would detect failure	N/A	N/A
I17		2	all aircraft	Not Credible; controller would detect failure	N/A	N/A
I18		3 or 4	all aircraft	Not Credible; controller would detect failure	N/A	N/A
I19	Undetected partial Loss of the identification function	1	=1	Not Credible; controller would detect failure	N/A	N/A
I20		2	=1	Not Credible; controller would detect failure	N/A	N/A
I21		3 or 4	=1	Not Credible; controller would detect failure	N/A	N/A
I22		1	>1	Not Credible; controller would detect failure	N/A	N/A
I23		2	>1	Not Credible; controller would detect failure	N/A	N/A
I24		3 or 4	>1	Not Credible; controller would detect failure	N/A	N/A
I25	Undetected corruption of the identification function	1	=1	Serious incident possible (e.g. E.3.11)	2	2
I26		2	=1	Serious incident possible (e.g. E.3.11)	2	2
I27		3 or 4	=1	Serious incident possible (e.g. E.3.11)	2	2
I28		1	>1	Serious incident possible (e.g. E.3.11)	2	2
I29		2	>1	Serious incident possible (e.g. E.3.11)	2	2
I30		3 or 4	>1	Serious incident possible (e.g. E.3.11)	2	2

Table 14: Failure of identification – Undetected Failure

E.4 Conflict prediction function

E.4.1 This section presents the severity of the consequence of an A-SMGCS Conflict Prediction function failure.

E.4.2 Two levels of alert are defined in the A-SMGCS concepts. These are:

- Stage 1 alert is used to inform the controller that a situation which is potentially dangerous may occur, and he/she needs to be made aware of. According to the situation, the controller receiving a stage 1 alert may take a specific action to resolve the alert if needed. This is called INFORMATION step;
- Stage 2 alert is used to inform the controller that a critical situation is developing which needs immediate action. This is called ALARM step.

E.4.3 Two types of failure of the function are defined, these are[9]

[9] EUROCAE Working Group 41, MASPS for A-SMGCS, Edition ED-87A, January 2001

- False alert: an alert which does not correspond to an actual alert situation;
- Nuisance alert: an alert correctly generated according to the rule set, but inappropriate to the desired outcome. In addition, the EATM defines a nuisance alert as an 'alert which is not considered necessary by the controller';

E.4.4 The safety impact of nuisance alerts is that controllers become desensitised and therefore when a real conflict occurs, they may not take any notice of it. Nuisance alerts, by their very nature have no impact on safety however, the consequence of the desensitisation may be that when a real alert is generated then the controller may not react on this alert. However in this case it is no longer a nuisance alert and becomes an undetected alert.

E.4.5 The analysis presented in this section relates to false alerts and particularly during the critical take off stage.

E.4.6 Failures of this function are only applicable for more than one aircraft. An alert for one aircraft is not a credible failure because two aircraft will always be involved (even if one aircraft is actually a false target).

Detected false alerts

E.4.7 The conflict prediction function is considered as a safety net and is not used to control aircraft and therefore any detected failure will have no impact on the safety of the system but does represent a reduction in aerodrome safety nets. The fundamental method of aerodrome control does not change if the conflict prediction function is not available.

Undetected false alerts

E.4.8 A scenario was identified which may have serious safety consequences when a credible corrupted false alarm occurs. An alert may be generated when a false target is on the runway (e.g. from a reflection) and an aircraft is on final approach or take off. The conflict prediction function would generate an alert because of the perceived collision between the false target and a real target. This could cause the controller to issue a go around or abort take-off instruction that may result in severe consequences. The pilot may react to avoid the (false) collision by exiting the runway into a potentially dangerous situation.

E.4.9 This situation may be mitigated in visibility conditions 1 and 2, however in such a stressful situation there is no guaranteed mitigation against such a scenario.

E.4.10 Severity tables were generated to identify the consequences of a stage 1 and a stage 2 false alert during take-off.

E.4.11 The following table lists the results of the workshop discussion relating to stage 1 (information) alerts.

Ref.	Failure	Visibility Condition	Number of Mobile impacts	Discussion and Consequence	Severity Class	
					Taxi	RWY
C01	Undetected complete Loss of the conflict prediction function	1	all aircraft	No impact because not used at a control tool	N/A	5
C02		2	all aircraft	No impact because not used at a control tool	N/A	5
C03		3 or 4	all aircraft	No impact because not used at a control tool	N/A	5
C04	Undetected partial Loss of the conflict prediction function	1	=1	Not credible for one aircraft	N/A	N/A
C05		2	=1	Not credible for one aircraft	N/A	N/A
C06		3 or 4	=1	Not credible for one aircraft	N/A	N/A
C07		1	>1	No impact because not used at a control tool	N/A	5
C08		2	>1	No impact because not used at a control tool	N/A	5
C09		3 or 4	>1	No impact because not used at a control tool	N/A	5
C10	Undetected corruption of the conflict prediction function	1	=1	Not credible for one aircraft	N/A	N/A
C11		2	=1	Not credible for one aircraft	N/A	N/A
C12		3 or 4	=1	Not credible for one aircraft	N/A	N/A
C13		1	>1	Controller would be able to visually check is the alarm is correct, therefore not a credible failure.	N/A	N/A
C14		2	>1	No impact. If the aircraft is in take-off and no stage 2 alert is generated then time window permits aircraft to continue to take-off. Otherwise if the aircraft are on line up, the controller may revoke clearance to investigate possible conflict.	N/A	5
C15		3 or 4	>1	No impact. If the aircraft is in take-off and no stage 2 alert is generated then time window permits aircraft to continue to take-off. Otherwise if the aircraft are on line up, the controller may revoke clearance to investigate possible conflict.	N/A	5
C16	Undetected delay of the	1	=1	Not credible for one aircraft	N/A	N/A
C17		2	=1	Not credible for one aircraft	N/A	N/A

Ref.	Failure	Visibility Condition	Number of Mobile impacts	Discussion and Consequence	Severity Class	
					Taxi	RWY
C18	conflict prediction function	3 or 4	=1	Not credible for one aircraft	N/A	N/A
C19		1	>1	Same as partial Loss (C05)	N/A	5
C20		2	>1	Same as partial Loss (C07)	N/A	5
C21		3 or 4	>1	Same as partial Loss (C09)	N/A	5

Table 15: Failure of Conflict Prediction stage 1 alert – undetected Failure

E.4.12 The following table lists the results of the workshop discussion relating to stage 2 (alert) alerts.

Ref.	Failure	Visibility Condition	Number of Mobile impacts	Discussion and Consequence	Severity Class	
					Taxi	RWY
C22	Undetected complete Loss of the conflict prediction function	1	all aircraft	No impact because not used at a control tool	N/A	5
C23		2	all aircraft	No impact because not used at a control tool	N/A	5
C24		3	all aircraft	No impact because not used at a control tool	N/A	5
C25	Undetected partial Loss of the conflict prediction function	1	=1	Not credible for one aircraft	N/A	N/A
C26		2	=1	Not credible for one aircraft	N/A	N/A
C27		3 or 4	=1	Not credible for one aircraft	N/A	N/A
C28		1	>1	No impact because not used at a control tool	N/A	5
C29		2	>1	No impact because not used at a control tool	N/A	5
C30		3 or 4	>1	No impact because not used at a control tool	N/A	5
C31	Undetected corruption of the conflict prediction function	1	=1	Not credible for one aircraft	N/A	N/A
C32		2	=1	Not credible for one aircraft	N/A	N/A
C33		3 or 4	=1	Not credible for one aircraft	N/A	N/A
C34		1	>1	Controller would be able to visually check is the alarm is correct, therefore not a credible failure.	N/A	2

Ref.	Failure	Visibility Condition	Number of Mobile impacts	Discussion and Consequence	Severity Class	
					Taxi	RWY
C35		2	>1	Possibility of a serious incident with no mitigation from controller or aircrew. Extreme action may be required by the aircrew in the event of aborted landing or take-off.	N/A	2
C36		3 or 4	>1	Possibility of a serious incident with no mitigation from controller or aircrew. Extreme action may be required by the aircrew in the event of aborted landing or take-off.	N/A	2
C37	Undetected delay of the conflict prediction function	1	=1	Not credible for one aircraft	N/A	N/A
C38		2	=1	Not credible for one aircraft	N/A	N/A
C39		1	>1	Same as undetected corruption (C32)	N/A	N/A
C40		3 or 4	=1	Not credible for one aircraft	N/A	N/A
C41		2	>1	Same as undetected corruption (C34)	N/A	2
C42		3 or 4	>1	Same as undetected corruption (C36)	N/A	2

Table 16: Failure of Conflict Prediction stage 2 alert – undetected Failure

E.5 Hazards and safety objectives

E.5.1 The total credible failures with safety consequences and their severity classification are illustrated in **Table 1**. These are grouped into a set of common Hazards (labelled H01 through H10). These are shown as taxi way and (runway)

HZ	Hazard	Failure Reference	Severity Class 2	Severity Class 3	Severity Class 4	Total
H01	Total loss of A-SMGCS	P01-P03, P16-P18		1 (1)	2 (2)	3 (3)
H02	Loss of the position function for one aircraft	P04-P06, P19-P21		1 (1)	1 (1)	2 (2)
H03	Loss of the position function impacting multiple aircraft	P07-P09, P22-P24	1 (1)	1 (2)	3 (2)	5 (5)
H04	Corruption of the position function for one aircraft	P10-P12, P25-P27	0 (2)	0 (1)		0 (3)

HZ	Hazard	Failure Reference	Severity Class 2	Severity Class 3	Severity Class 4	Total
H05	Corruption of the position function impacting multiple aircraft	P13-P15, P28-P30		1 (1)	2 (2)	3 (3)
H06	Total loss the identification function	I01-P03, I16-P18			0 (3)	0 (3)
	Loss of the identification function for one aircraft	I04-P06, I19-P21	No credible consequences of severity class 1,2,3 or 4			
H07	Loss of the identification function impacting multiple aircraft	I07-P09, I22-P24			0 (3)	0 (3)
H08	Corruption of the identification function for one aircraft	I10-P12, I25-P27	3 (3)			3 (3)
H09	Corruption of the identification function impacting multiple aircraft	I13-P15, I28-P30	3 (3)		0 (3)	3 (6)
	Total loss the conflict prediction function	C01-P03, C22-C24	No credible consequences of severity class 1,2,3 or 4			
	Loss of the conflict prediction function for one aircraft	C04-P06,C25-C27	No credible consequences of severity class 1,2,3 or 4			
	Loss of the conflict prediction function impacting multiple aircraft	C07-P09, C28-C30	No credible consequences of severity class 1,2,3 or 4			
	Corruption of the conflict prediction function for one aircraft	C10-P12, C31-C33	No credible consequences of 1,2,3 or 4			
H10	Corruption of the conflict prediction function	C13-P15, C34-C36	0 (2)			0 (2)

Table 17: Summary of credible failures for each hazard

F Developing Safety Objectives

F.1 Introduction

F.1.1 An event tree is used to calculate the acceptable probability of a hazard occurring, i.e. the safety objective.

F.1.2 As an example, an event tree for the total loss of the A-SMGCS (H01 in **Table 1**) is shown in **Figure 11**. This illustrates the event tree based on the probabilities of the event occurring whether the failure is detected (100% of the time in this case), if the failure occurs in a particular visibility and whether the aircraft is on the runway. Also illustrated is the resulting severity of the incident and the accident risk should that branch of the tree be followed.

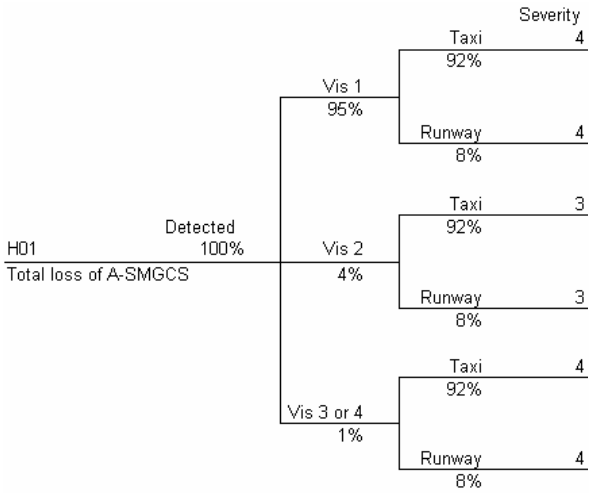


Figure 11: Example event tree

F.1.3 **Figure 12** calculates the probability of an accident should each branch of the event tree be followed.

F.1.4 Using the accident risk defined for each severity class (see **Table 10**), the total aggregated probability of an accident should this hazard occur is 5.0E-6.

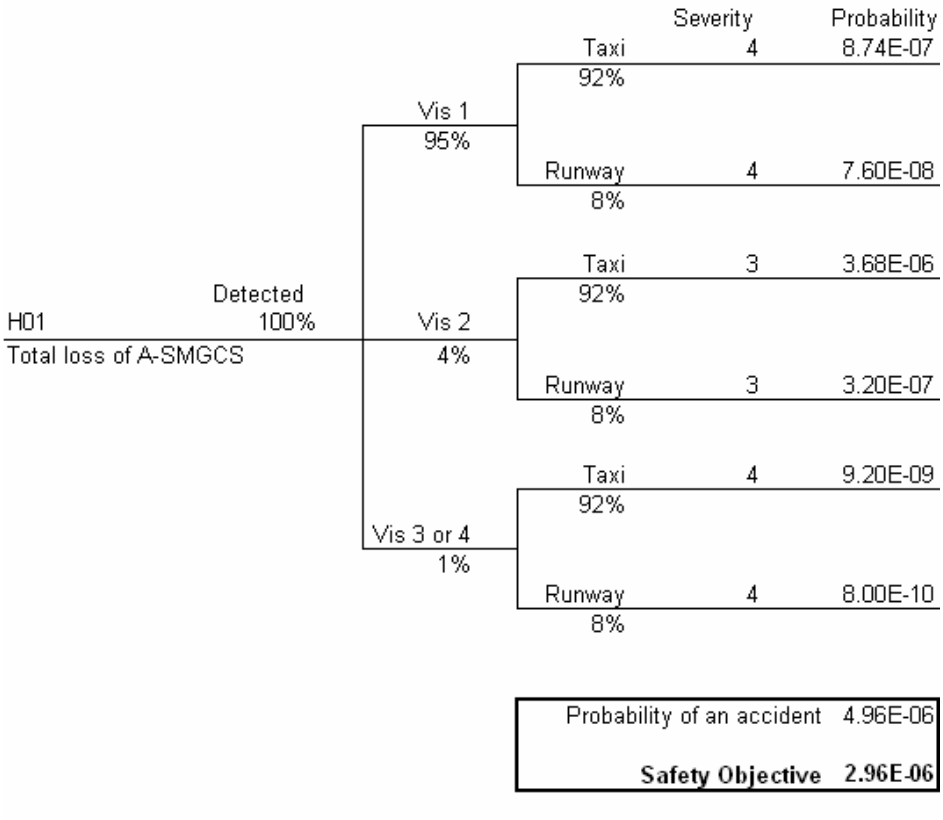


Figure 12: Event tree and probability of an accident for hazard 1

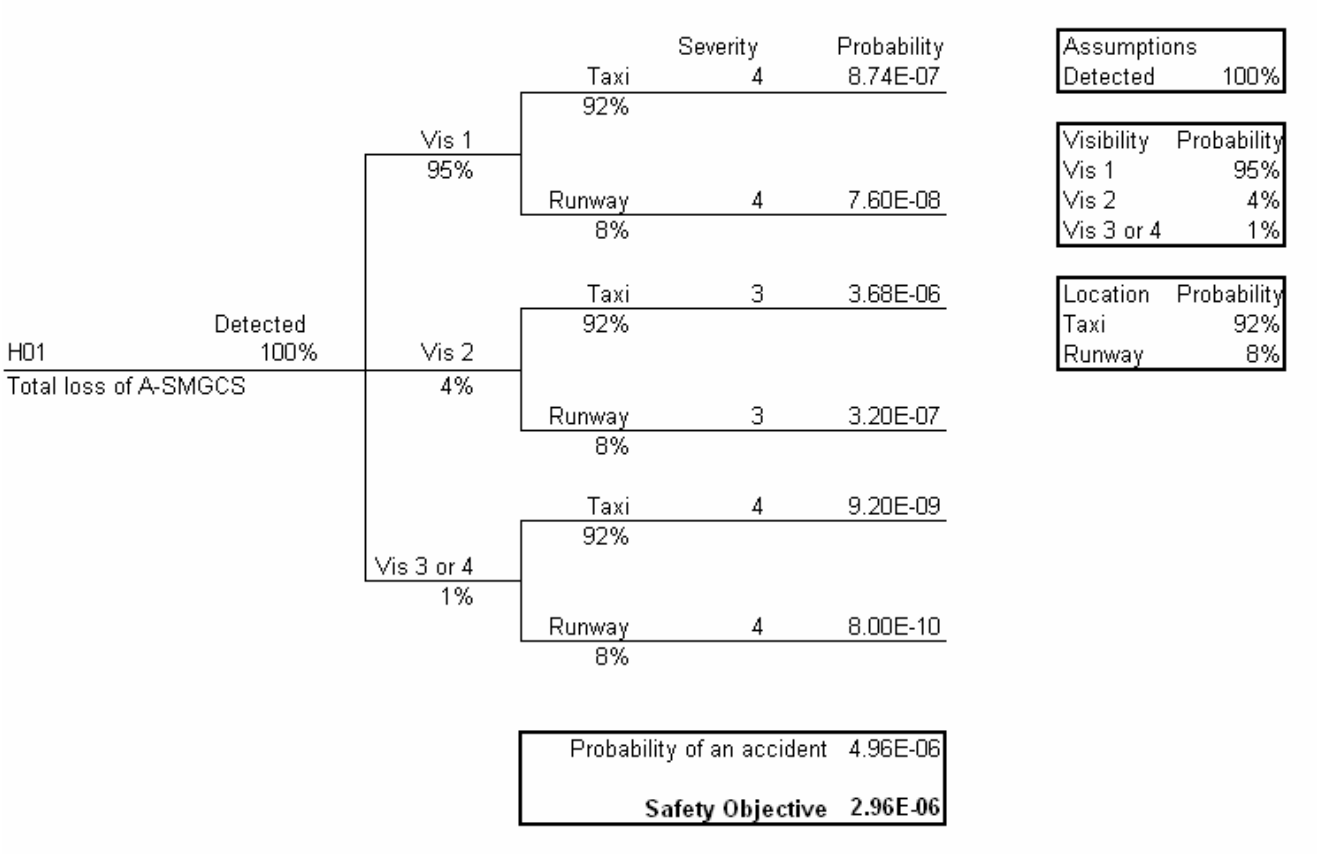
F.1.5 A total of ten hazards were identified for A-SMGCS (see **Table 1**). Initially, the PSSA assumed that the acceptable risk of an accident was distributed evenly over each hazard resulting in an acceptable risk of an accident per A-SMGCS hazard of 1.5E-10 per movement. The PSSA results were then used in a 'case study' based on LHR evidence to show that the safety requirements could be implemented. Based upon the results of this, the TLS distribution was changed from an even distribution to ensure that all safety requirements were achievable. The resulting TLS distribution with the TLS applied to each hazard and which the PSSA is based upon is shown in the following table.

HZ	Hazard	TLS (per movement)
H01	Total loss of A-SMGCS	1.47E-11
H02	Loss of the position function for one aircraft	1.47E-11
H03	Loss of the position function impacting multiple aircraft	1.47E-10
H04	Corruption of the position function for one aircraft	1.47E-11
H05	Corruption of the position function impacting multiple aircraft	1.47E-11
H06	Total loss the identification function	1.47E-11
H07	Loss of the identification function impacting multiple aircraft	1.47E-11
H08	Corruption of the identification function for one aircraft	1.47E-10
H09	Corruption of the identification function impacting multiple aircraft	1.47E-11
H10	Corruption of the conflict prediction function	1.07E-09
Overall TLS		1.47E-09

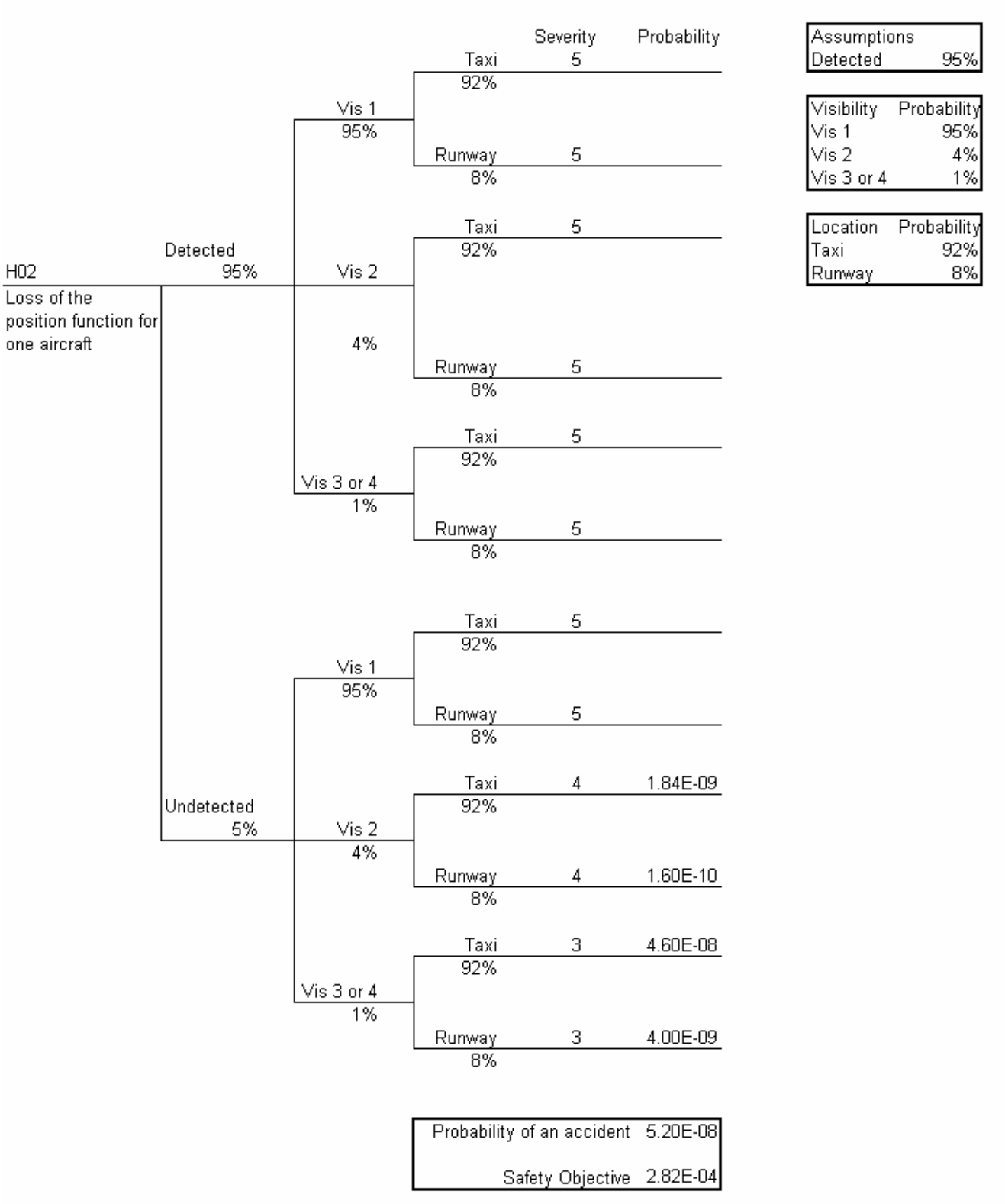
Table 18: Distribution of TLS

F.1.6 The safety objective is derived based on the risk per hazard as specified in the table above divided by the aggregated probability of an accident per hazard (in this case 4.96E-6). Therefore the safety objective for the total loss of A-SMGCS is 2.96E-6 per movement.

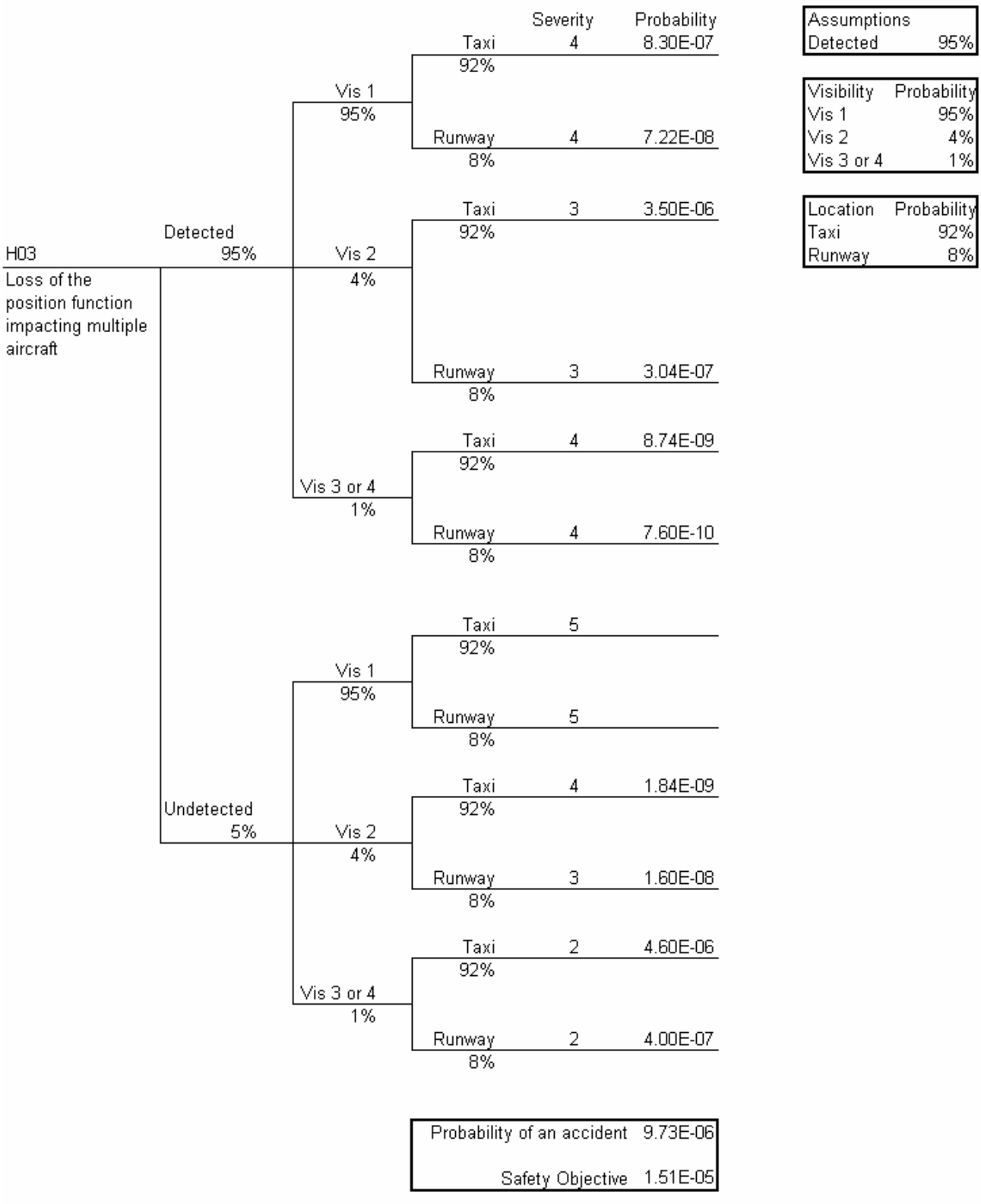
F.2 H01 Total loss of A-SMGCS



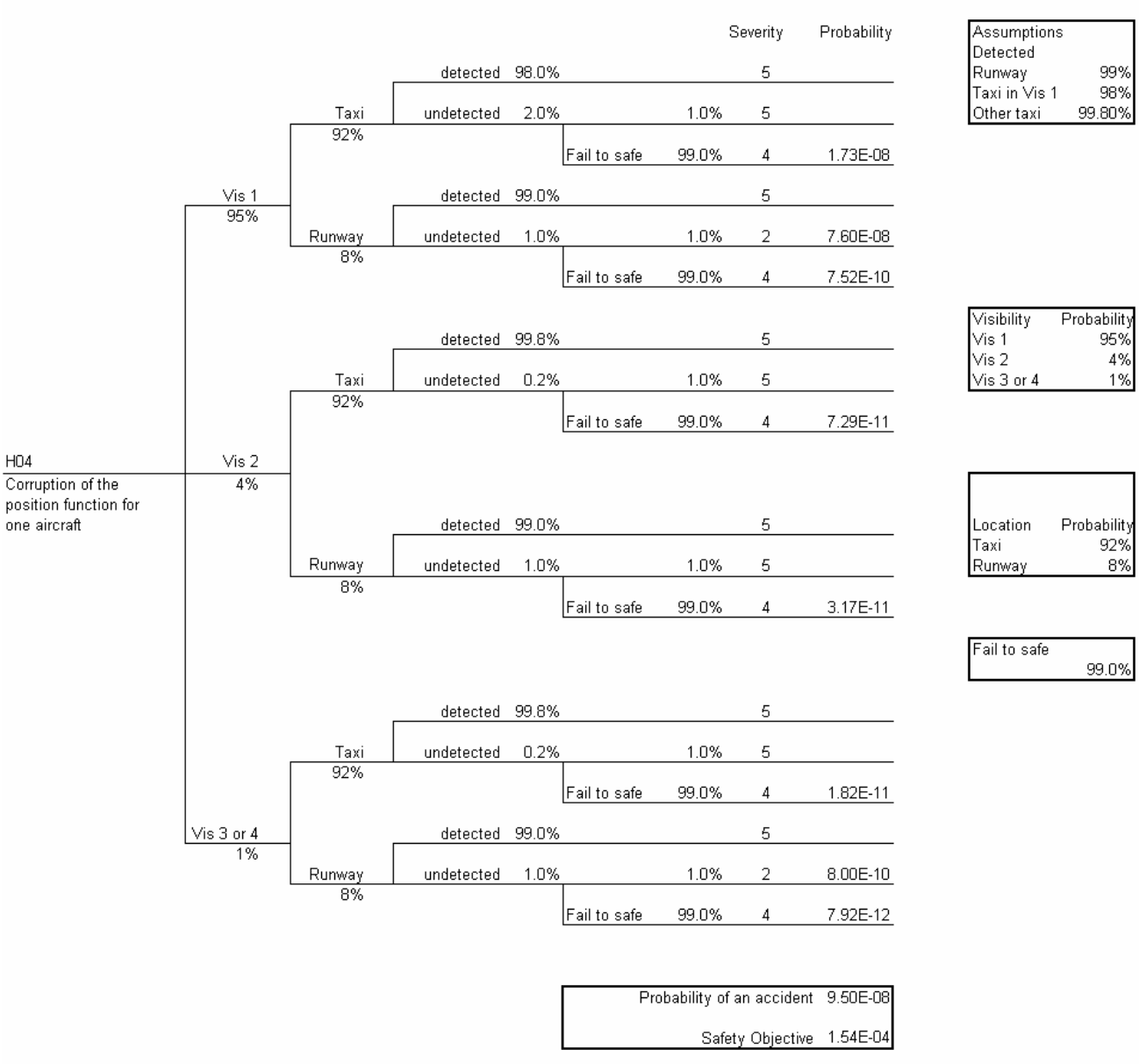
F.3 H02 Loss of the position function for one aircraft



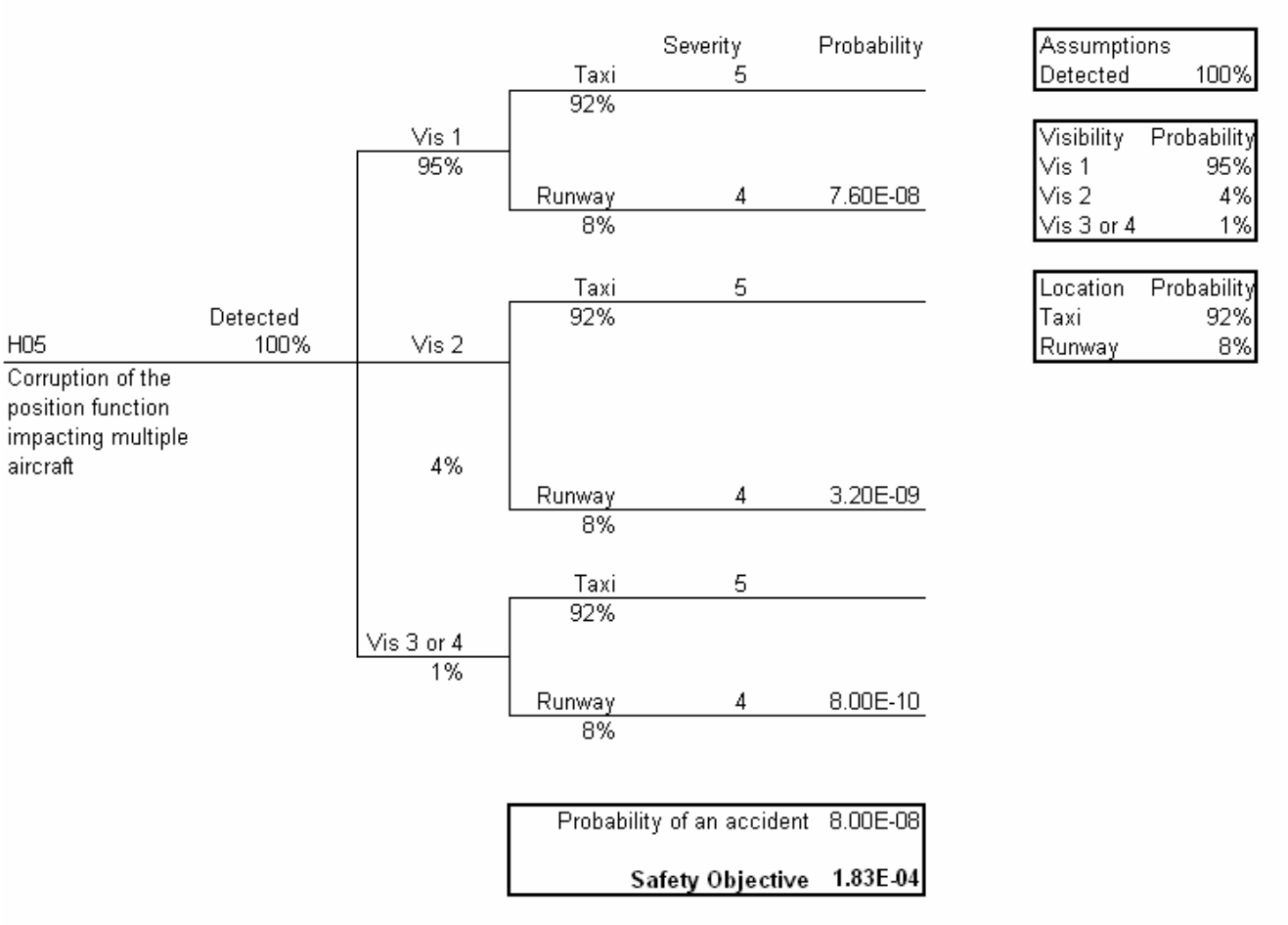
F.4 H03 Loss of the position function impacting multiple aircraft


Severity
Probability
H03
Loss of the position function impacting multiple aircraft
Detected 95%
Undetected 5%
Vis 1 95%
Vis 2 4%
Vis 3 or 4 1%
Taxi 92%
Runway 8%
Taxi 4 8.30E-07
Runway 4 7.22E-08
Taxi 3 3.50E-06
Runway 3 3.04E-07
Taxi 4 8.74E-09
Runway 4 7.60E-10
Taxi 5
Runway 5
Taxi 4 1.84E-09
Runway 3 1.60E-08
Taxi 2 4.60E-06
Runway 2 4.00E-07
Probability of an accident 9.73E-06
Safety Objective 1.51E-05
Assumptions
Detected 95%
Visibility Probability
Vis 1 95%
Vis 2 4%
Vis 3 or 4 1%
Location Probability
Taxi 92%
Runway 8%

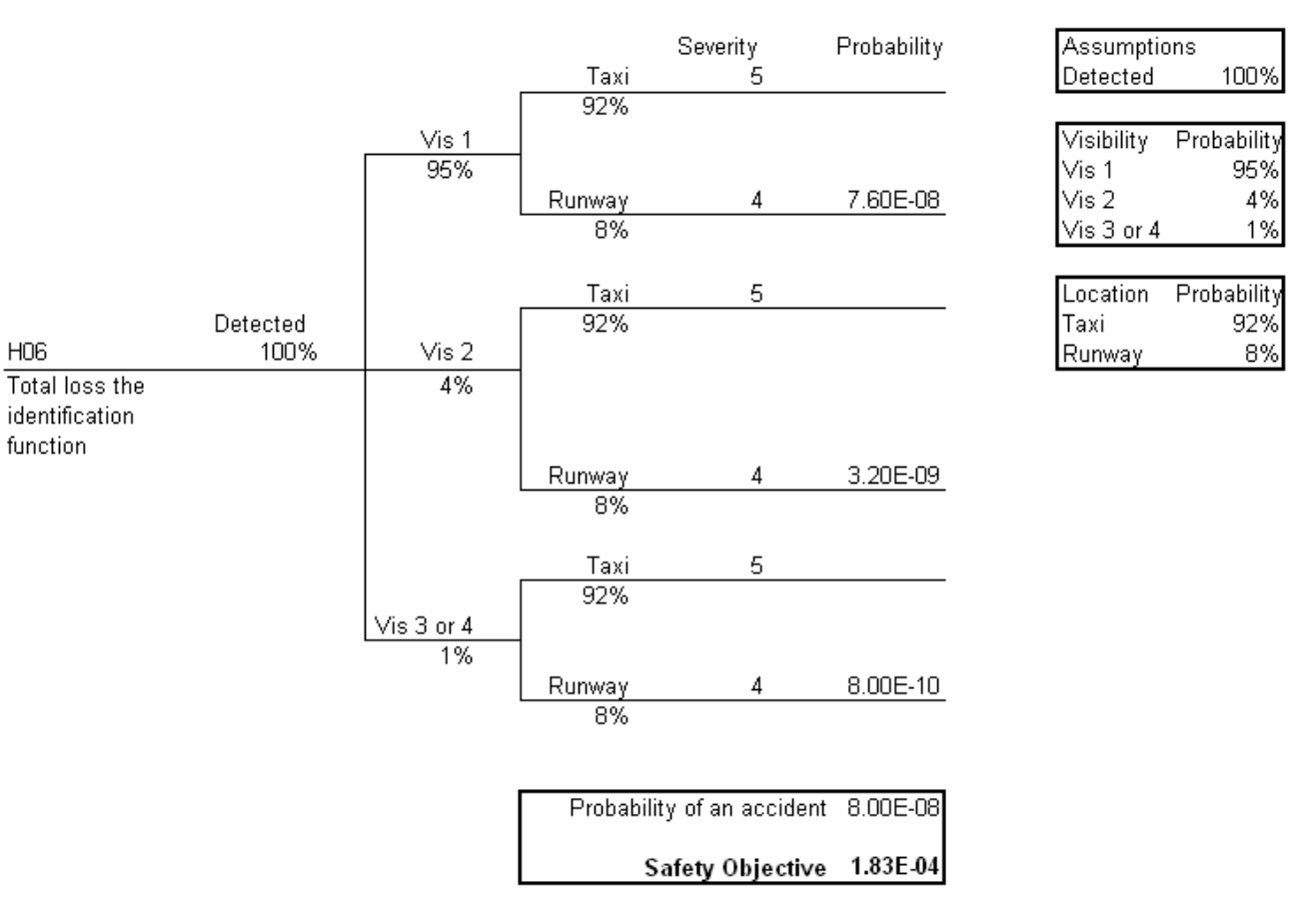
F.5 H04 Corruption of the position function for one aircraft



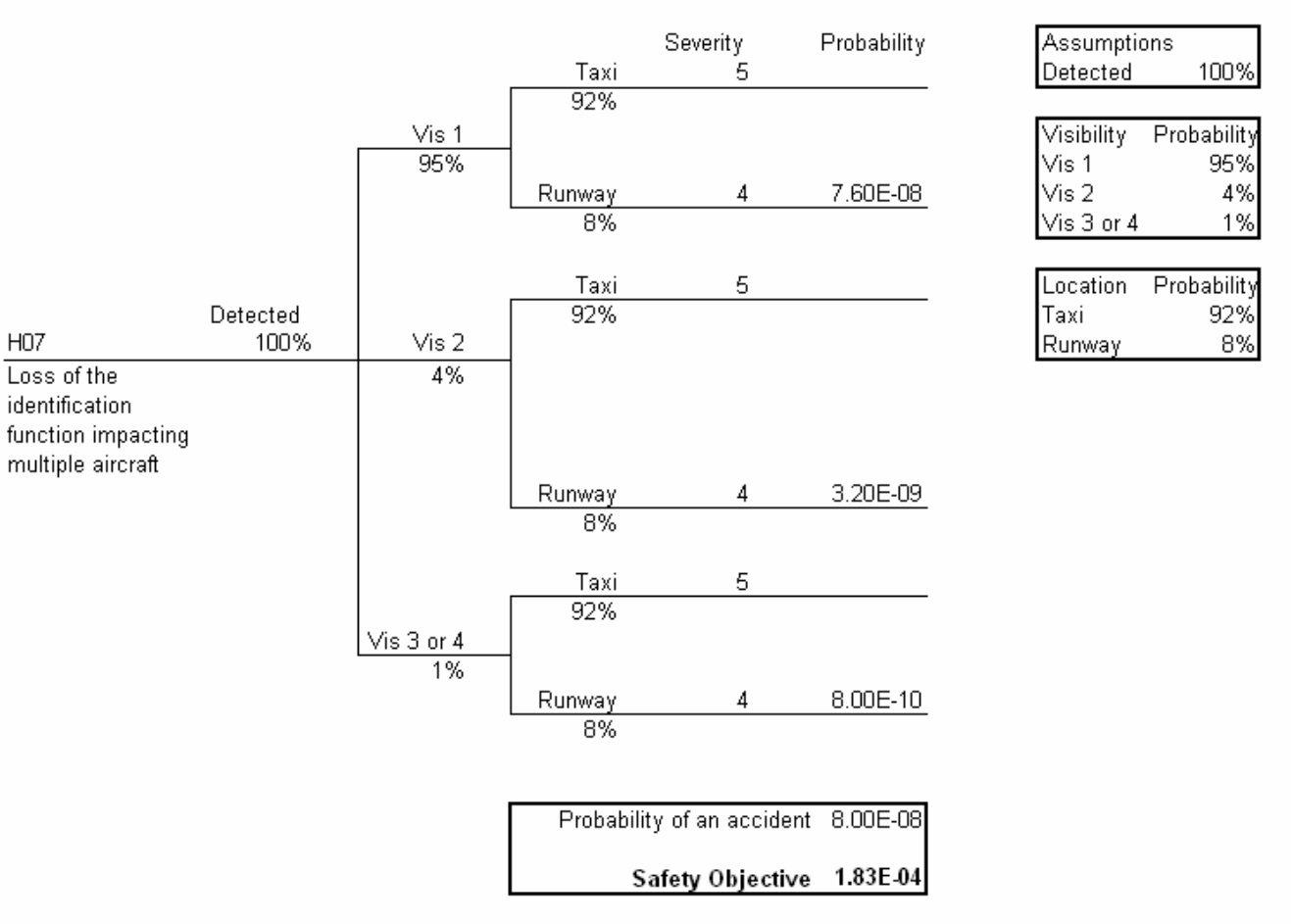
F.6 H05 Corruption of the position function impacting multiple aircraft



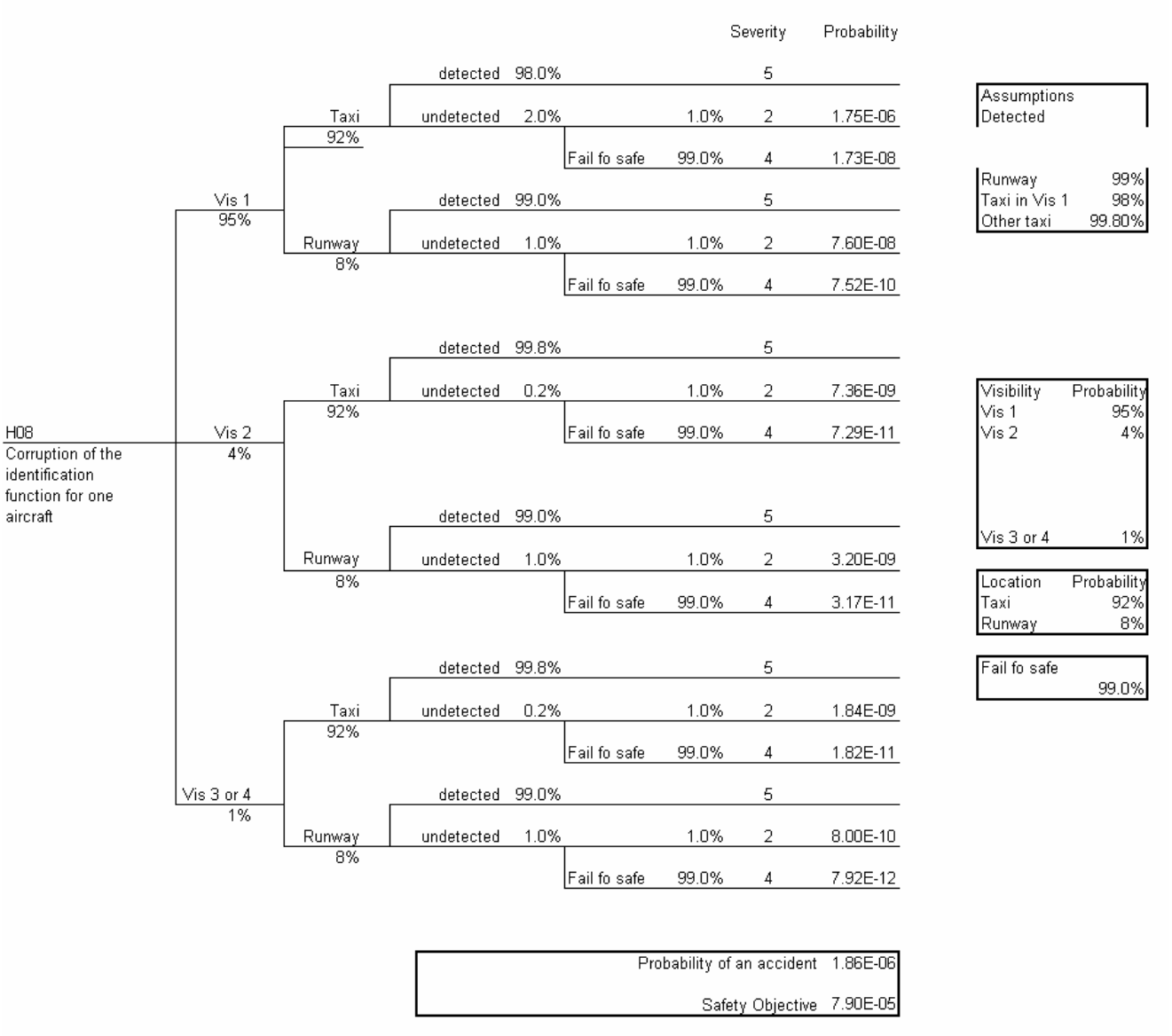
F.7 H06 Total loss the identification function



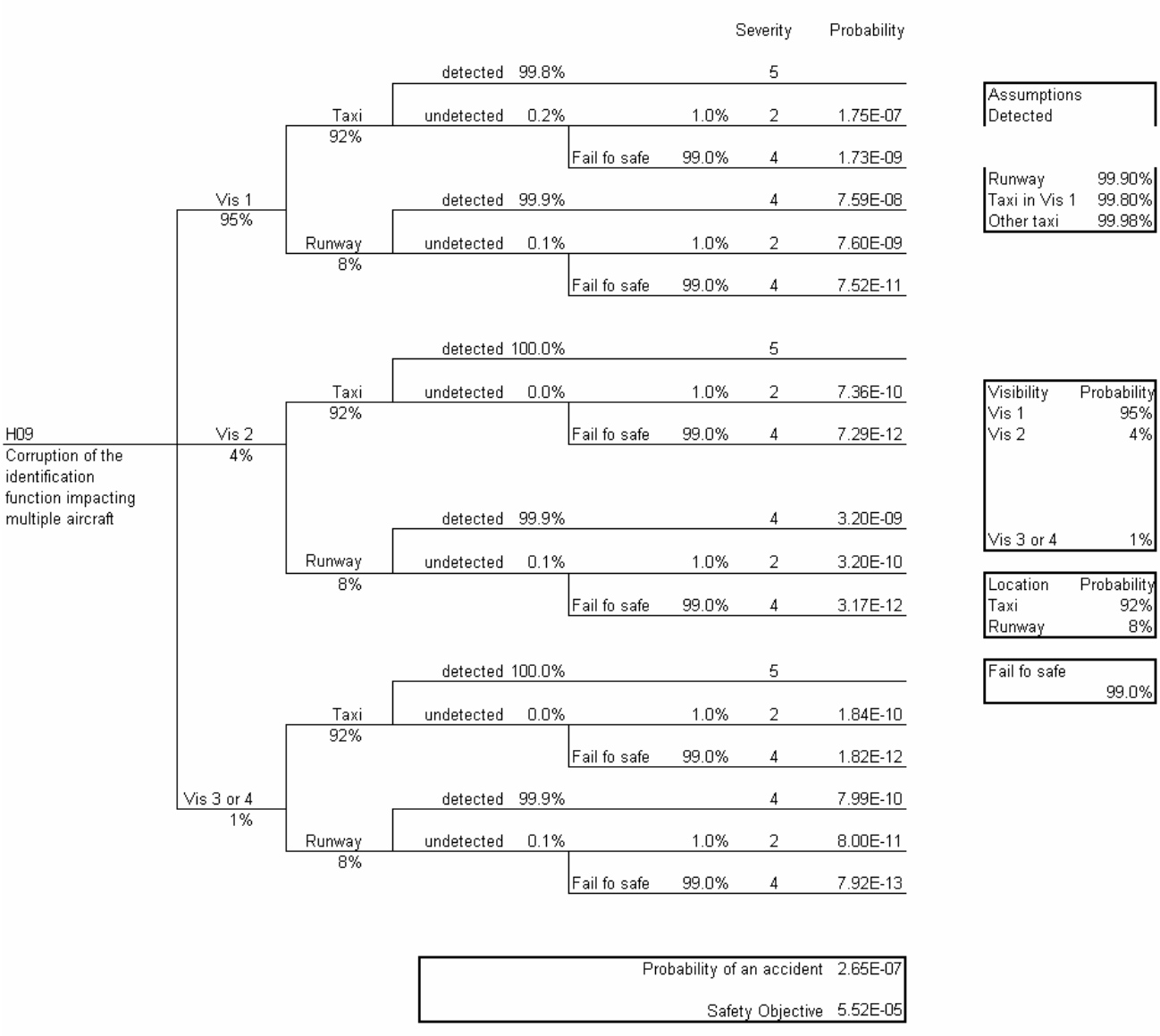
F.8 H07 Loss of the identification function impacting multiple aircraft



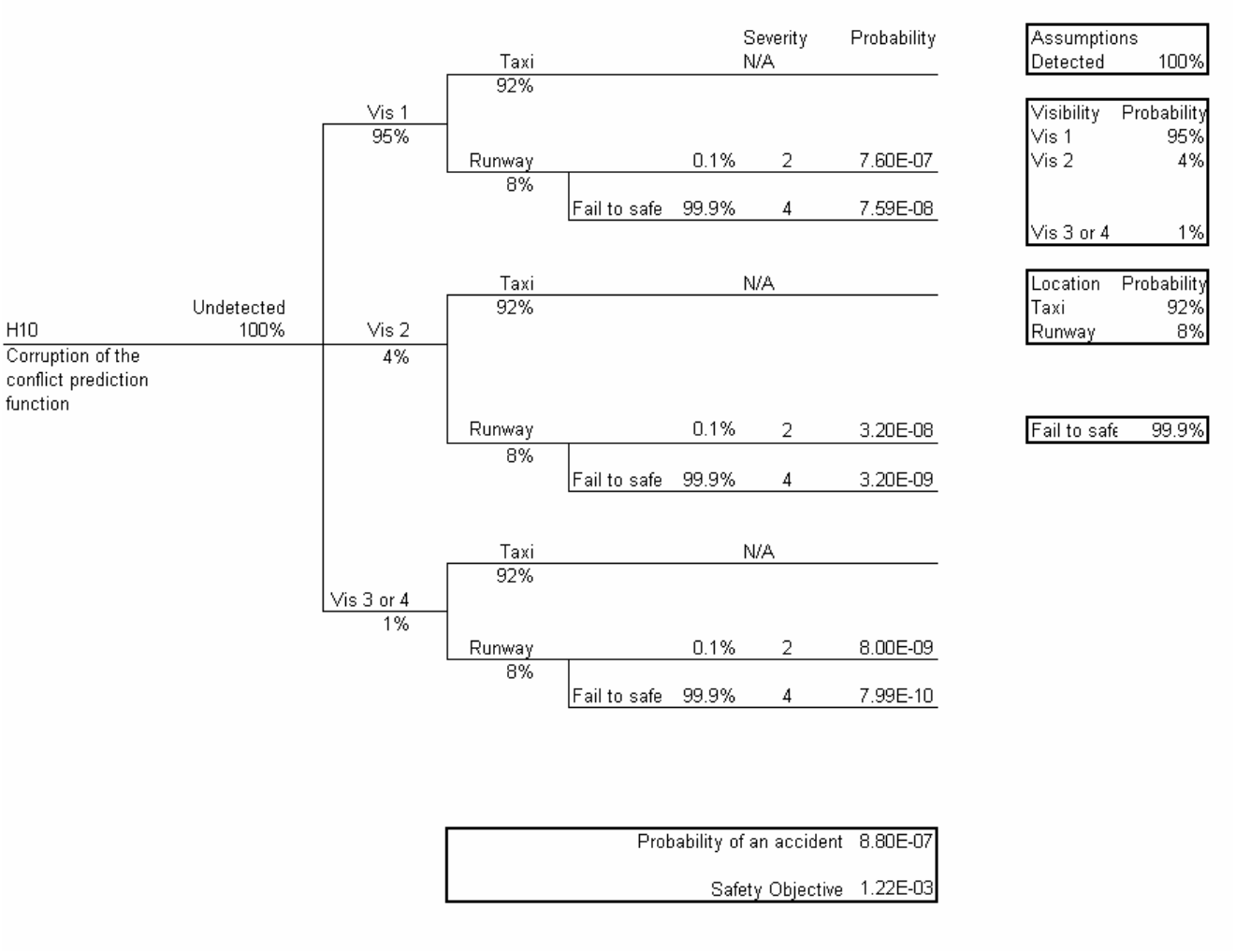
F.9 H08 Corruption of the identification function for one aircraft



F.10 H09 Corruption of the identification function impacting multiple aircraft



F.11 H10 Corruption of the conflict prediction function



F.12 Summary of safety objectives

F.12.1 The safety objectives for each hazard is presented below

HZ	Hazard	Safety Objective (per movement)
H01	Total loss of A-SMGCS	2.96E-06
H02	Loss of the position function for one aircraft	2.82E-04
H03	Loss of the position function impacting multiple aircraft	1.51E-05
H04	Corruption of the position function for one aircraft	1.54E-04
H05	Corruption of the position function impacting multiple aircraft	1.83E-04
H06	Total loss the identification function	1.83E-04
H07	Loss of the identification function impacting multiple aircraft	1.83E-04
H08	Corruption of the identification function for one aircraft	7.90E-05
H09	Corruption of the identification function impacting multiple aircraft	5.52E-05
H10	Corruption of the conflict prediction function	1.22E-03

G Developing Safety Requirements

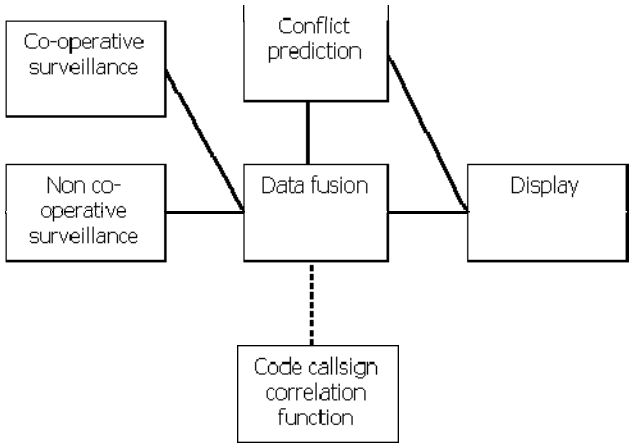
G.1 Introduction

G.1.1 The objective of the fault trees is to develop safety requirements for the A-SMGCS components and determine if they can be implemented to meet the requirement. Safety requirements are developed using fault tree analysis to partition the safety requirements between the components which contribute to each safety objective

G.1.2 Fault tree analysis is used to determine the performance requirements of system functions in order to meet the acceptable rates of each hazard (for example the total loss of A-SMGCS at 3.0E E-5 per movement). The process of dividing the acceptable failure rate between the components of the A-SMGCS permits performance targets for each element to be identified.

G.1.3 The workshop participants agreed to apportion safety requirements equally between the A-SMGCS components as follows:

- Data fusion;
- Display;
- Conflict prediction;
- Code callsign correlation;
- Surveillance (co-operative and non co-operative).



G.1.4 Note that:

- the code callsign function is not part of A-SMGCS. However, use of this function by A-SMGCS imposes safety requirements on the source of the data (e.g. flight data processing systems).
- where failures of both co-operative and non co-operative surveillance functions were required to produce the hazard, the requirements were apportioned equally.

Fault tree analysis

G.1.5 A fault tree is developed for each safety objective to determine the safety requirements for each system component.

G.1.6 As an example consider the loss of the A-SMGCS position function for multiple aircraft (hazard 03). A fault tree for this failure is presented in **Figure 13**.

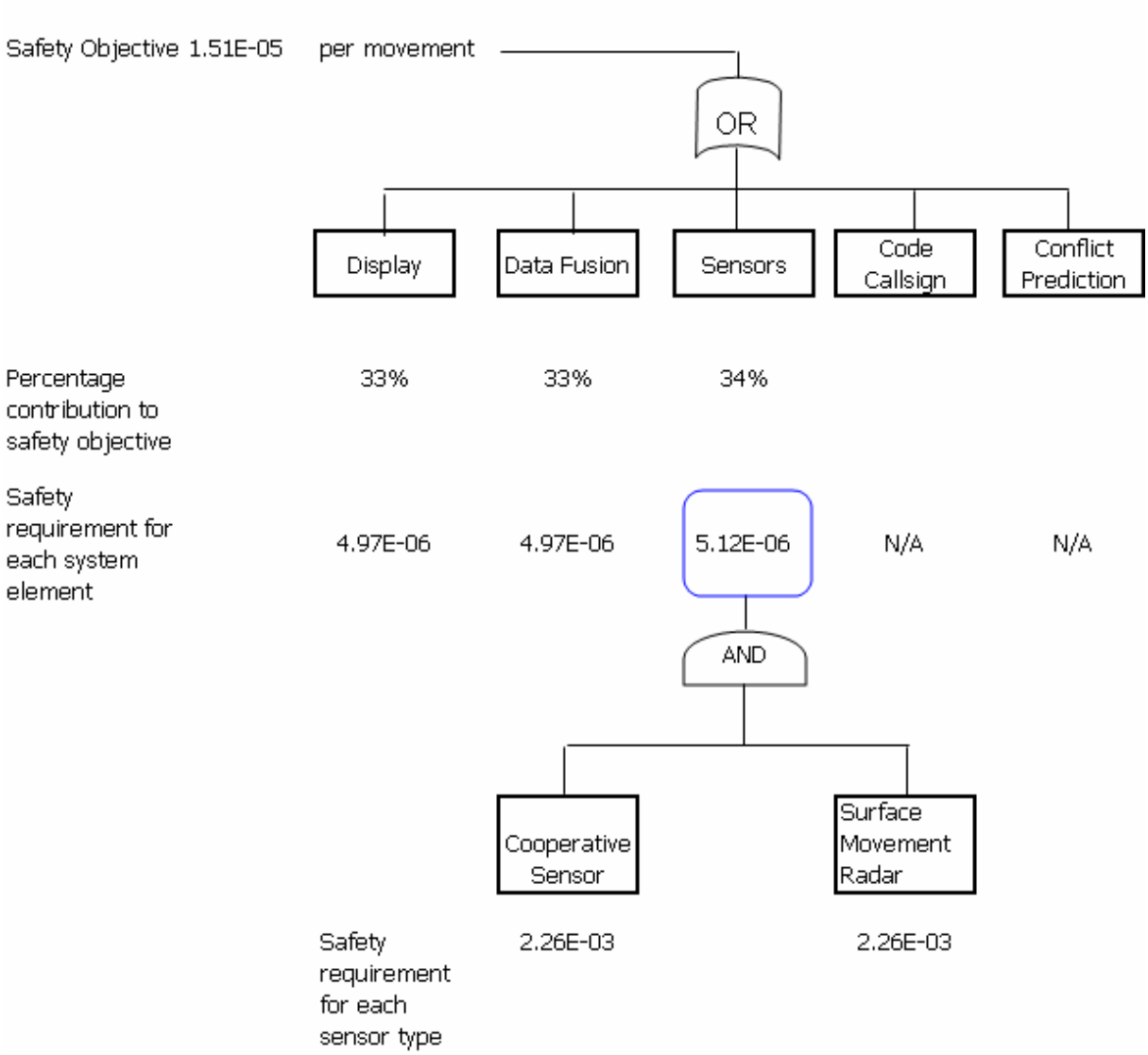


Figure 13: Fault Tree for loss of A-SMGCS for multiple aircraft (Hazard 3)

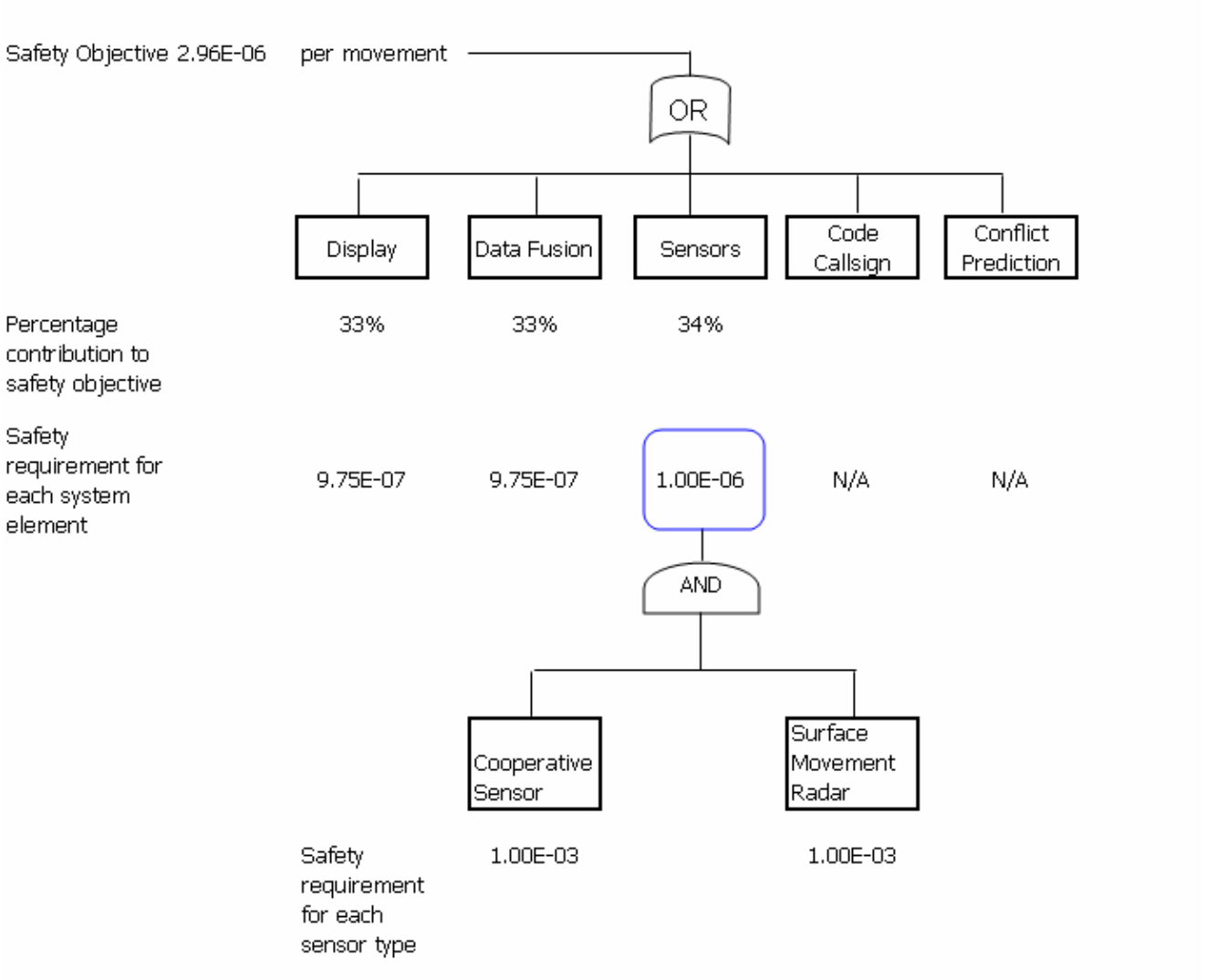
G.1.7 The fault tree shows the basic functions that may cause each failure. **Figure 13** shows that the possible causes of the failure are the loss of surveillance sensors (both cooperative and non-cooperative sensors) or the loss of the data fusion or the loss of the display. The conflict prediction or code/callsign function cannot contribute to this failure.

G.1.8 Based on a strategy that each function may contribute evenly to the failure then the failure rate, per component is:

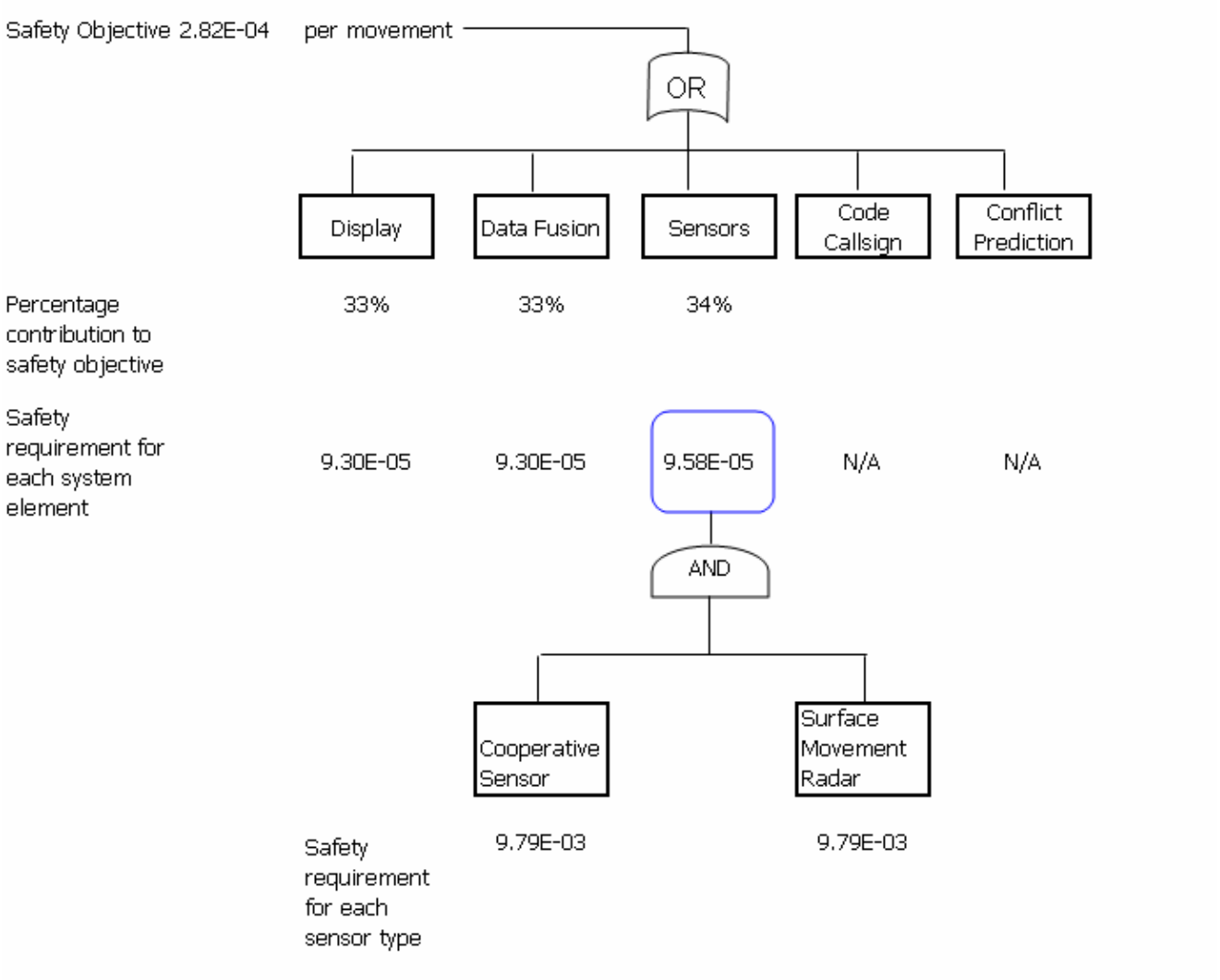
- 4.97E-6 per movement for the loss of the display;
- 4.97E-6 per movement for the loss of the data fusion;
- 5.12E-6 per movement for the loss of the sensors.

G.1.9 In the case of A-SMGCS function for multiple aircraft, both the cooperative and non-cooperative sensors need to fail to contribute to this hazard. Therefore, assuming an even distribution of the sensor safety requirement over each sensor, then they each have a safety requirement of 2.26E-3 per movement.

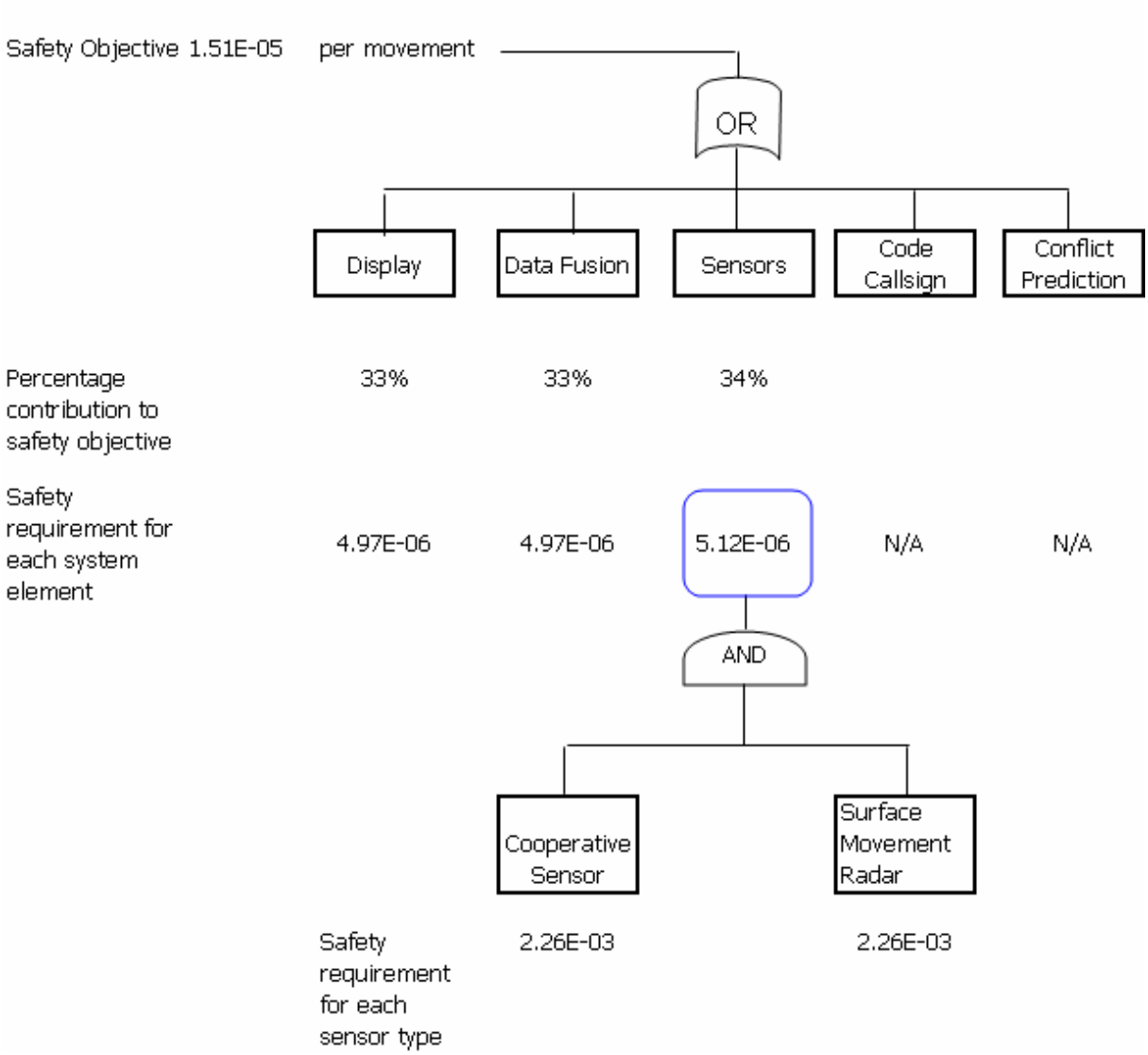
G.2 H01 Total loss of A-SMGCS



G.3 H02 Loss of the position function for one aircraft

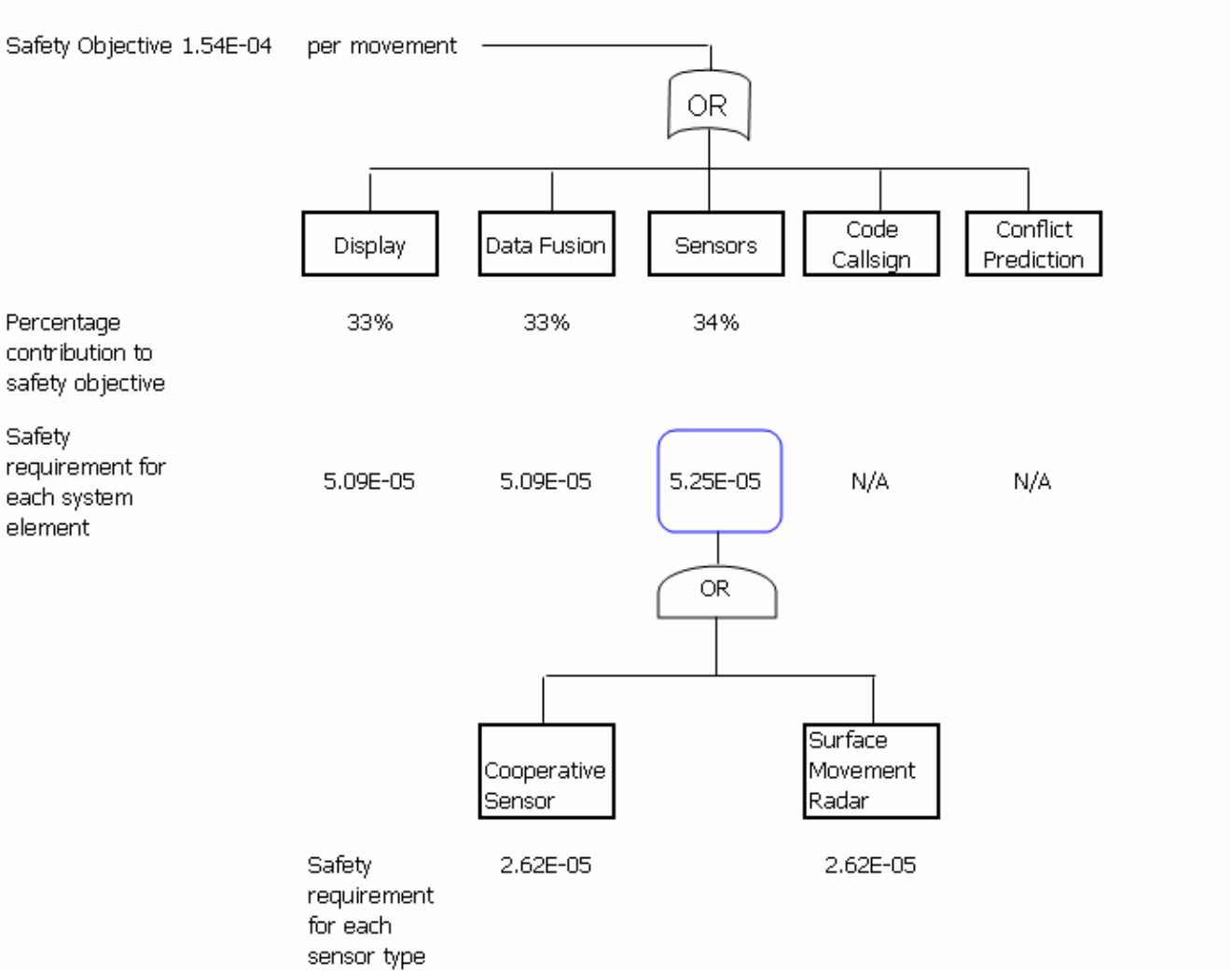


G.4 H03 Loss of the position function impacting multiple aircraft



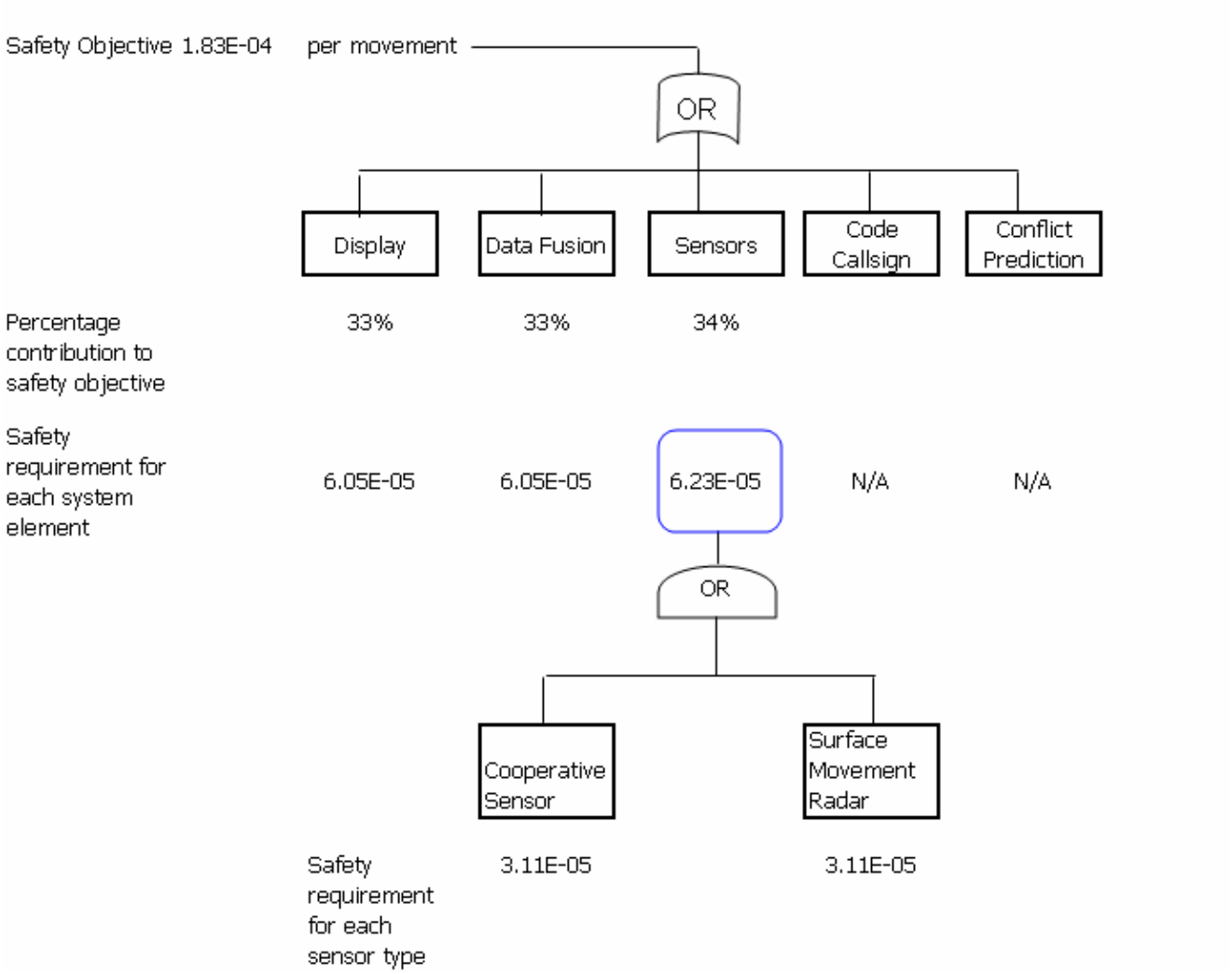
G.5 H04 Corruption of the position function for one aircraft

G.5.1 The corruption of position can be caused by either of the sensors; therefore there is an OR for sensors.

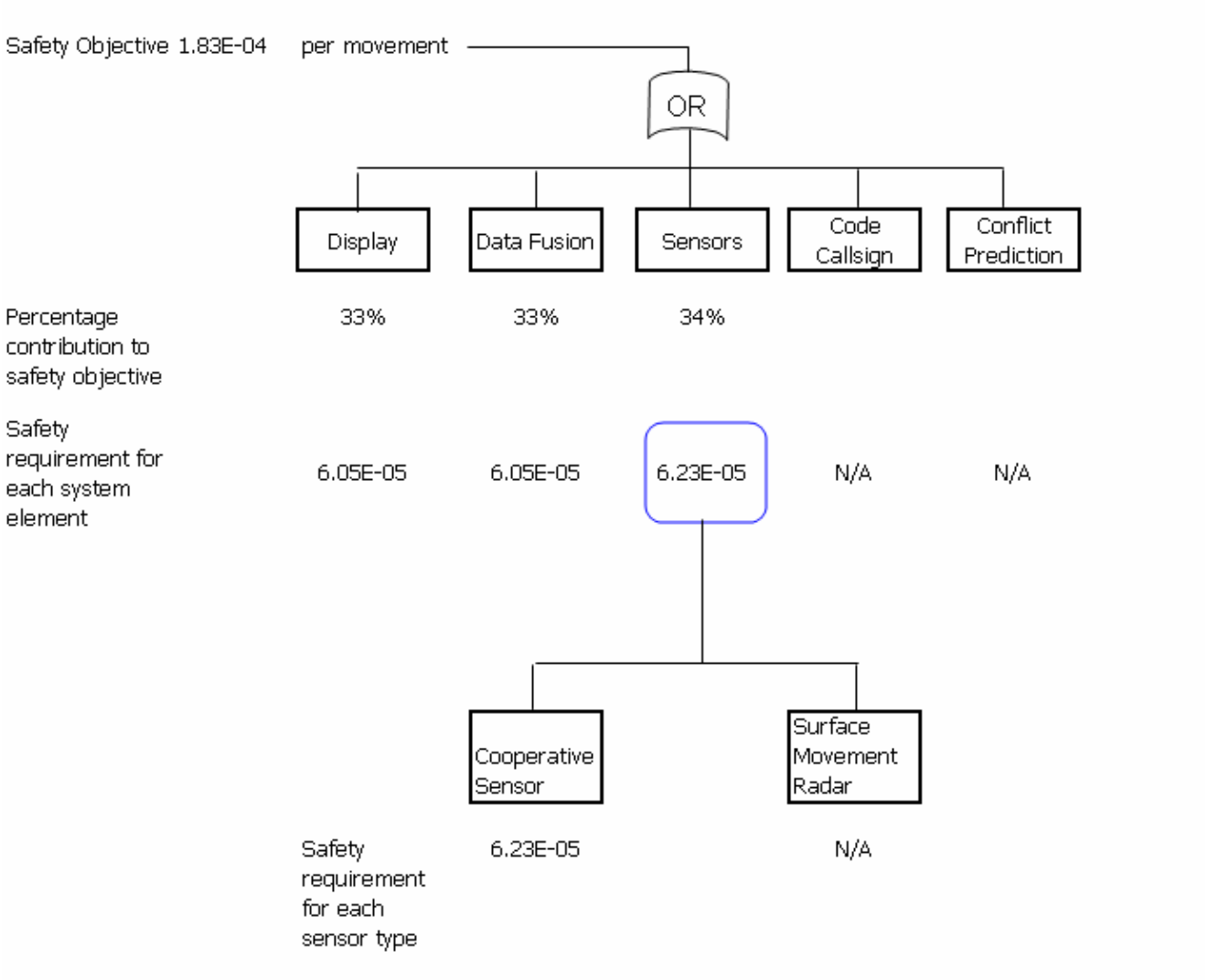


G.6 H05 Corruption of the position function impacting multiple aircraft

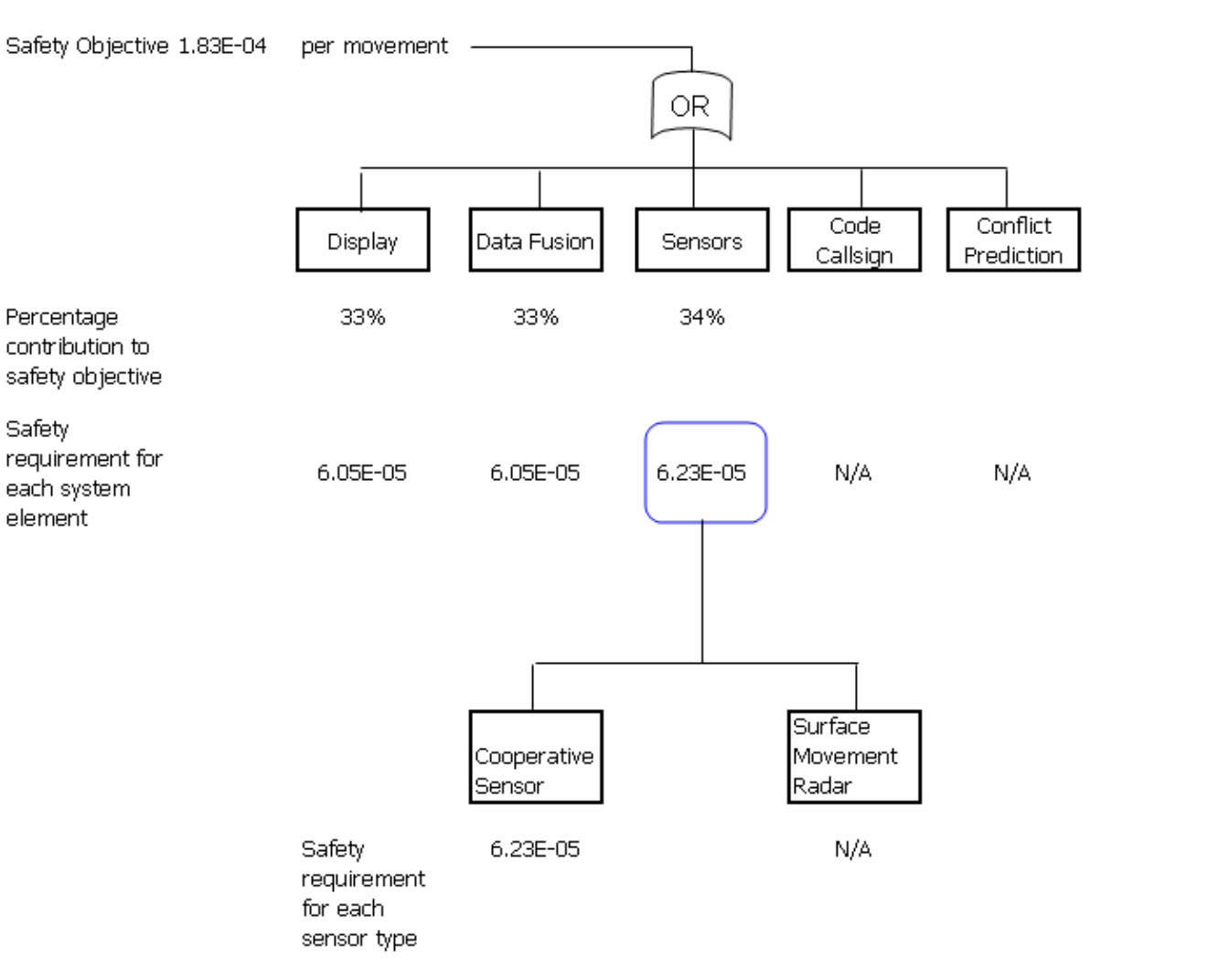
G.6.1 The corruption of position can be caused by either of the sensors; therefore there is an OR for sensors.



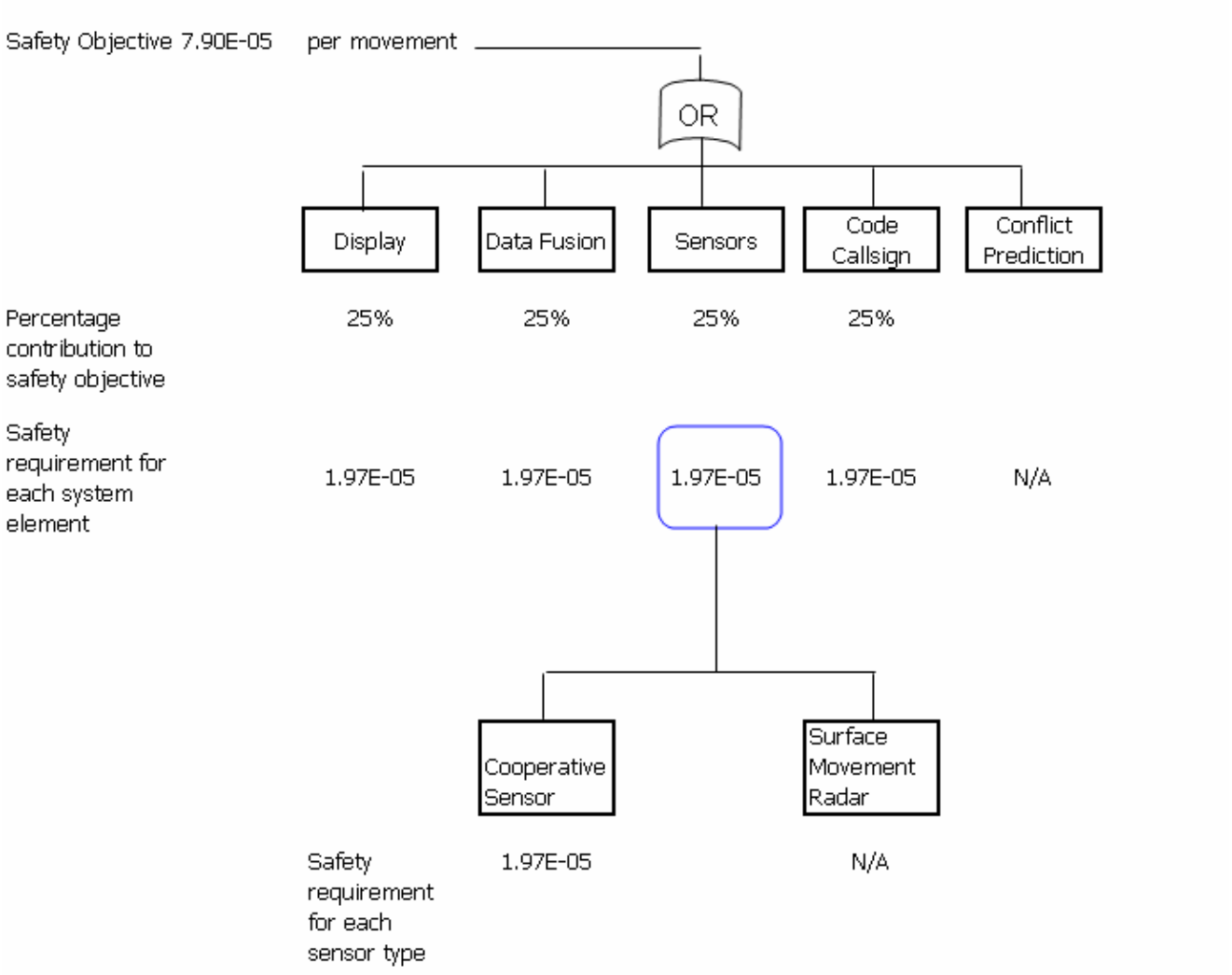
G.7 H06 Total loss the identification function



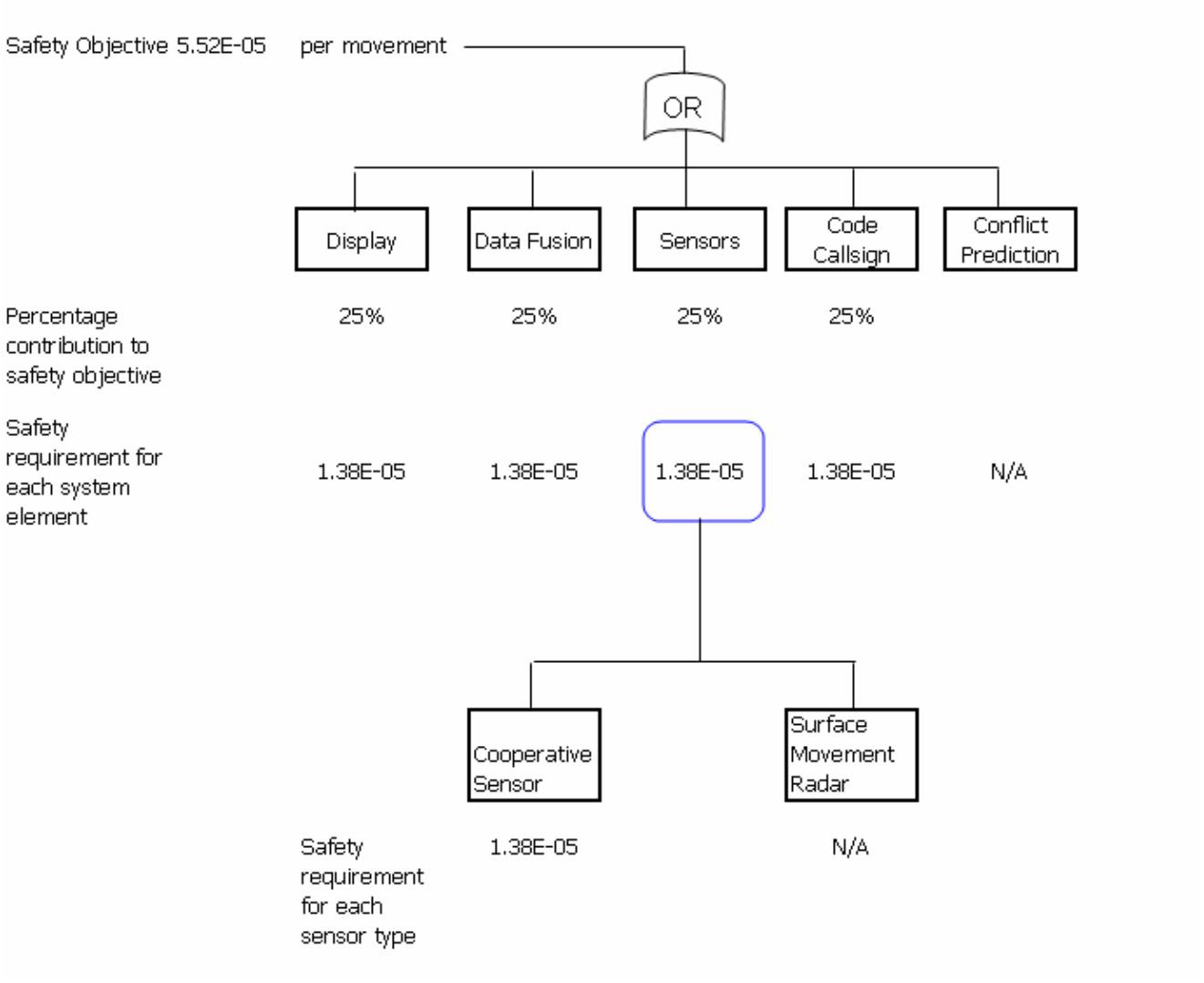
G.8 H07 Loss of the identification function impacting multiple aircraft



G.9 H08 Corruption of the identification function for one aircraft

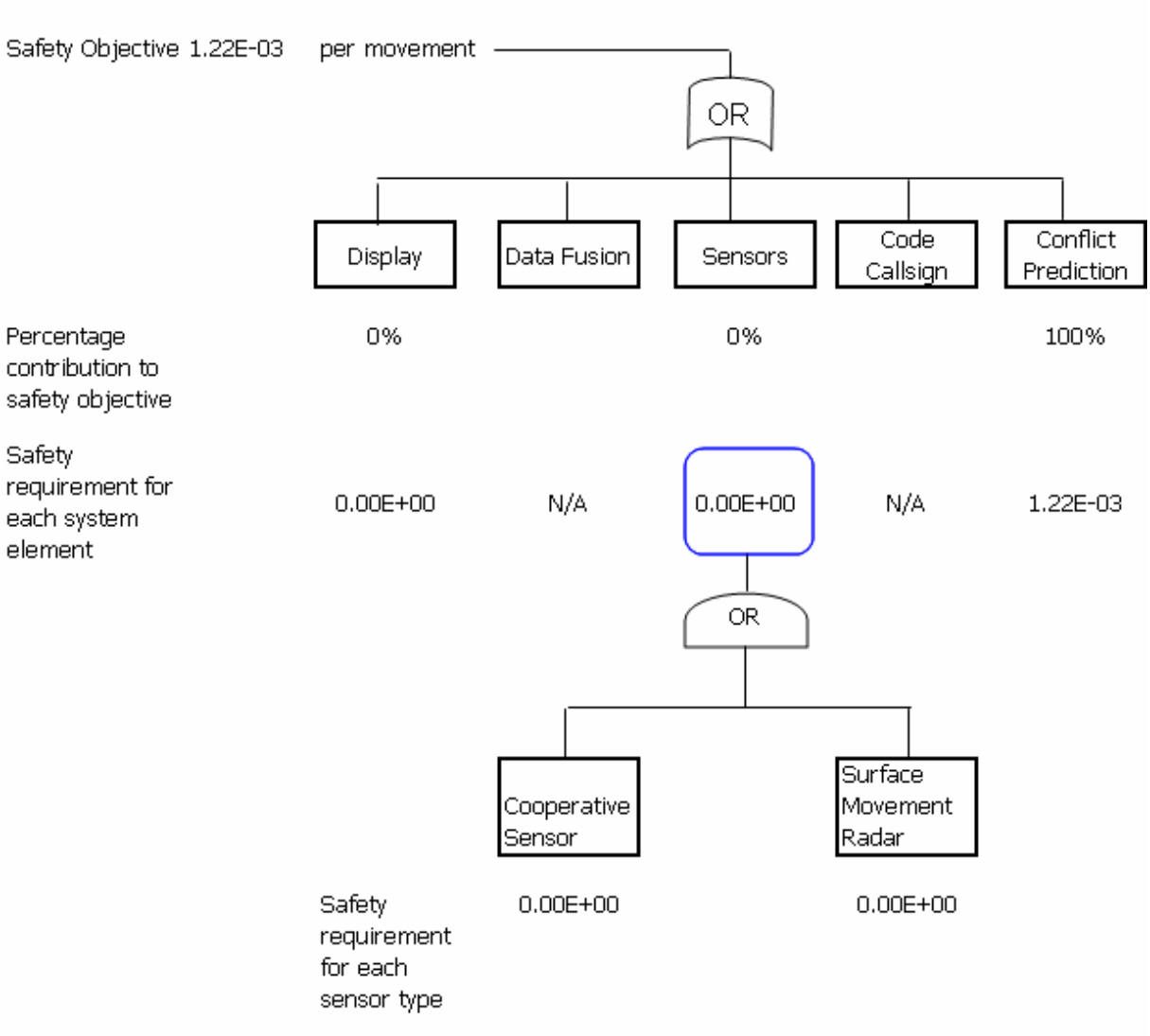


G.10 H09 Corruption of the identification function impacting multiple aircraft



G.11 H10 Corruption of the conflict prediction function

G.11.1 In the case of corruption of the conflict prediction function, the safety requirements are not distributed between the system elements. The conflict prediction function is considered to be an integrated system and it is not realistic to attribute its failures to any particular component of A-SMGCS. Therefore, the Safety Requirement is allocated to the conflict prediction function.



G.12 Summary of safety requirements

G.12.1 The safety requirements for each hazard are presented below

HZ	Hazard	Safety Objective (per movement)	System safety requirements (per movement)				
			Display	Data Fusion	Sensors	Code Callsign	Conflict Prediction
H01	Total loss of A-SMGCS	2.96E-06	9.75E-07	9.75E-07	1.00E-06	N/A	N/A
H02	Loss of the position function for one aircraft	2.82E-04	9.30E-05	9.30E-05	9.58E-05	N/A	N/A
H03	Loss of the position function impacting multiple aircraft	1.51E-05	4.97E-06	4.97E-06	5.12E-06	N/A	N/A
H04	Corruption of the position function for one aircraft	1.54E-04	5.09E-05	5.09E-05	5.25E-05	N/A	N/A
H05	Corruption of the position function impacting multiple aircraft	1.83E-04	6.05E-05	6.05E-05	6.23E-05	N/A	N/A
H06	Total loss the identification function	1.83E-04	6.05E-05	6.05E-05	6.23E-05	N/A	N/A
H07	Loss of the identification function impacting multiple aircraft	1.83E-04	6.05E-05	6.05E-05	6.23E-05	N/A	N/A
H08	Corruption of the identification function for one aircraft	7.90E-05	1.97E-05	1.97E-05	1.97E-05	1.97E-05	N/A
H09	Corruption of the identification function impacting multiple aircraft	5.52E-05	1.38E-05	1.38E-05	1.38E-05	1.38E-05	N/A
H10	Corruption of the conflict prediction function	1.22E-03	N/A	N/A	N/A	N/A	1.22E-03

G.12.2 Safety requirements for the sensors are presented below

HZ	Hazard	Cooperative Sensor	Non Cooperative sensor
H01	Total loss of A-SMGCS	1.00E-03	1.00E-03
H02	Loss of the position function for one aircraft	9.79E-03	9.79E-03
H03	Loss of the position function impacting multiple aircraft	2.26E-03	2.26E-03
H04	Corruption of the position function for one aircraft	2.62E-05	2.62E-05
H05	Corruption of the position function impacting multiple aircraft	3.11E-05	3.11E-05
H06	Total loss the identification function	6.23E-05	N/A
H07	Loss of the identification function impacting multiple aircraft	6.23E-05	N/A
H08	Corruption of the identification function for one aircraft	1.97E-05	N/A
H09	Corruption of the identification function impacting multiple aircraft	1.38E-05	N/A
H10	Corruption of the conflict prediction function	N/A	N/A

H Evidence based on LHR implementation

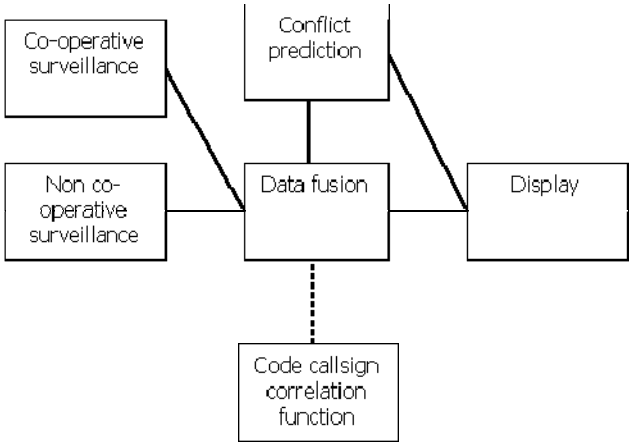
H.1 Introduction

H.1.1 This section presents evidence of the predicted failure rate of the A-SMGCS system at Heathrow in order to demonstrate the safety requirements are achievable.

H.1.2 Evidence is presented for each A-SMGCS component at an appropriate level. For example, data is available for the failure rate of the Multi-lateration system for a single aircraft. This is for both the hardware and software elements of the system. There is no requirement to break the evidence down further into the sub-components.

H.1.3 Evidence is presented for each of the main components of the fault tree. These are:

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



H.1.4 The implementation of A-SMGCS at Heathrow has a combined Display and Data Fusion System. Therefore evidence is presented for the combined element.

H.1.5 The safety requirements for Heathrow are presented in **Table 18**. These have been calculated as follows:

- A-SMGCS Level 1 safety requirements are translated into per hour by calculating the movement hours at the airport by multiplying the average movements per hour by their duration(for LHR this is 16.6 movement hours)
- A-SMGCS level 2 remains per movement because the conflict alert function concerns only two aircraft and is an instantaneous requirement at the time of the alert.

HZ	Hazard	Safety requirements (per hour)						
		Display and data fusion	Sensors	Code Callsign	Conflict Prediction		MLAT	SMR
H01	Total loss of A-SMGCS	3.25E-05	1.67E-05	N/A	N/A		1.67E-02	1.67E-02
H02	Loss of the position function for one aircraft	3.10E-03	1.60E-03	N/A	N/A		1.63E-01	1.63E-01
H03	Loss of the position function impacting multiple aircraft	1.66E-04	8.54E-05	N/A	N/A		3.77E-02	3.77E-02
H04	Corruption of the position function for one aircraft	1.70E-03	8.74E-04	N/A	N/A		4.37E-04	4.37E-04
H05	Corruption of the position function impacting multiple aircraft	2.02E-03	1.04E-03	N/A	N/A		5.19E-04	5.19E-04
H06	Total loss the identification function	2.02E-03	1.04E-03	N/A	N/A		1.04E-03	N/A
H07	Loss of the identification function impacting multiple aircraft	2.02E-03	1.04E-03	N/A	N/A		1.04E-03	N/A
H08	Corruption of the identification function for one aircraft	6.58E-04	3.29E-04	3.29E-04	N/A		3.29E-04	N/A
H09	Corruption of the identification function impacting multiple aircraft	4.60E-04	2.30E-04	2.30E-04	N/A		2.30E-04	N/A
H10	Corruption of the conflict prediction function	N/A	N/A	N/A	2.03E-02		N/A	N/A

Table 18: Safety Requirements (per hour) for Heathrow airport

H.2 Estimation of performance of the LHR A-SMGCS

Introduction

H.2.1 This section presents evidence for each of the system components relating to the predicted probabilities for the loss or corruption A-SMGCS information.

Avionics impact

H.2.2 No firm evidence is available to predict the failure rate of the Mode S transponder. Therefore, to predict the failure rate of avionics, two sources are used[10]:

- The JAA position paper regarding Mode S enhanced surveillance[11] proposes that the classification for aircraft identification is ‘minor’;
- AC/AMJ.25.1309[12] section 8 indicates a probability of loss or corruption (both detected or undetected) for a minor classification of between 1 and 10-5 per flight hour. This analysis assumes that the probability of loss or corruption of information from the avionics is 10-4 per flight hour.

H.2.3 A failure rate of 10-4 per flight hour relates to all possible failures of the transponder including both detected and undetected, failures of registers, squitter and Mode S all-call functionality.

10 The avionics assumptions and method is based on the EUROCONTROL Mode S programme Enhanced Surveillance FHA and PSSA presented to the SRC [awaiting approval].

11 JAA CNS/ATM Steering Group on enhanced surveillance will SSR Mode S No. and Revision pp025_76 17th April 2003

12 FAA/JAA AC/AMJ No: 25.1309 dated Date: 6/10/2002

H.2.4 There are 100 movements per hour at Heathrow each lasting 10 minutes. Therefore the failure rate of the transponder (per operation hour) is 1.66E-3 per hour for all aircraft.

$$\frac{flight\_hour}{duration\_of\_Movement} \times number\_of\_movements$$

$$\frac{10E-4}{6} \times 100 = 1.66E-3 \text{ per hour}$$

H.2.5 The preliminary safety assessment assumes the following decomposition of the consequences relating to avionics failures:

- 90% of failures result in loss of data (e.g. typically hardware failure where no data is processed or transmitted by the transponder; the consequence is that the aircraft is not detected by the ground system);
- 9% result in corruption of data content (e.g. corruption of Mode A, or aircraft identification). It is assumed that the corruption applies to all data rather than a single element (pessimistic viewpoint);
- 1% result in corruption of position information (e.g. delays in the transponder process resulting in the SSR miscalculating the position of the aircraft).

H.2.6 The impact of the assumptions on A-SMGCS safety case are:

- The complete loss of the transponder (i.e. no squitter or identification information) is 90% x 1.66E-3 per hour;
- The corruption of the identification delivered from the transponder is 9% x 1.66E-3 per hour.

H.2.7 Therefore for Heathrow airport:

- the complete loss of a transponder function is 1.5E-3 per hour;
- the corruption of the identification delivered from the transponder is 1.5E-4 per hour.

H.2.8 The following table summarises the estimated performance of the transponder.

Number of aircraft	Loss of position	Corruption of identification
Single aircraft	1.5E-3 per hour	1.5E-4 per hour
Multiple aircraft (assume 2)	2.25E-6 per hour	2.25E-8 per hour

Sensor Performance

H.2.9 The probability of detection for a target specified for the Heathrow system is that the SMR system will detect and display a target with a radar cross section of 1m2[13], with a probability of 95% [per scan].

H.2.10 An aircraft is within the coverage of one SMR and therefore the probability of a target drop, per scan, is 5%.or 5 E-2 per scan.

(1-0.95) = 5E - 2

[13] Note that aircraft are typically larger than the radar cross section

H.2.11 The probability that the SMR will not meet its specification for three consecutive seconds (i.e. three scans) and assuming independent causes is 1.25E-4.

$(5E\text{-}2)^3$ per aircraft

H.2.12 The SMR at LHR was recently upgraded with a predicted reliability of 2.5E-05 per hour, against a tendered reliability of 1.3E-06.

H.2.13 The reliability analysis, carried out by NATS in support of their local safety case, predicted the probability of anomalous behaviour (e.g. inaccurate position) of better than 2.3E-04 per hour

H.2.14 The Multi-lateration system was measured (i.e. during site acceptance tests) as detecting 99.96% of aircraft plot pairs for each update [per second][14]. This means that there is a 4 x 10-4 probability that an aircraft is not detected per update period

(1 – 0.9996) = 4E - 4

H.2.15 This analysis assumes three consecutive track drops constitutes a safety event. The probability of three consecutive track drops for the same aircraft (assuming independent causes) for the Multi-lateration is 6.4e-11 per aircraft.

H.2.16 The Multi-lateration system was assessed (i.e. during site acceptance tests) as detecting targets within 7.5m of their position with 97.80% accuracy, within 12m of their position with a 99.02% accuracy and within 30m of their true position with a 99.93% accuracy. This analysis assumes two consecutive false position reports is a safety event. The probability of three consecutive false positions (at 1 per second) is 4.9E-7 i.e. $(1\text{-}.9993)^3$

H.2.17 The following table summarises the estimated performance of the sensors

Sensor	Loss of position	Corruption of position
MLAT	6.4E-11 per aircraft	4.9E-7 per aircraft
SMR	1.25E-4 per aircraft	2.3E-4 per hour

H.2.18 There are 100 movements per hour at LHR, each movement an estimated 10 minutes. There are therefore 10 movement/hours at LHR. This impacts on the estimated sensor performance as below.

Sensor	Loss of position	Corruption of position
MLAT	6.4E-9 per hour	4.9E-5 per hour
SMR	1.25E-2 per hour	2.3E-4 per hour

Use of Historical evidence

H.2.19 Display and Data Fusion Systems with identical hardware and similar software have been in service at Birmingham since March 1999, at Gatwick since October 1999. The phase 1 D&DFS has been in service at Heathrow since October 2000. Birmingham has 2 display channels, Gatwick 3 and Heathrow has 6. Therefore the total amount of display channel operational time is +/-250000 hours.

[14] The Multi-lateration system design requirement was for detection of greater than or equal to 99.9% of aircraft plot pairs.

H.2.20 Historical evidence is provided based on the incidents reported during this period. Parts of the Heathrow A-SMGCS system has been in operation from the end of 1999. This equates to approximately five and a half years of operation or 50000 hours of operation.

H.2.21 The following table shows the historical MTBF at a 90% confidence for various numbers of system failures and display channel failures. For example, if it is known that there have been losses of a single display channel, then the MTBF is 28200 hours.

Number of failures	MTBF (System)	MTBF(Display channel)
0	21300	65600
1	12600	38600
2	9200	28200
3	7300	22500

Table 19: Display and Data Fusion Display and Data Fusion MTBF

H.2.22 The reliability of historical data can be questioned because the data refers to a 'detected' failure. Therefore the system may have failed more than the incident rate provided by historical data. However it is assumed that even if the system has failed more frequently than reported, the consequence of the unreported incident has had no safety impact.

H.2.23 Assumptions relating to the operational Environment

Introduction

H.2.24 A number of assumptions were made about mitigations that affected the system safety objectives. The assumptions related to:

- Visibility conditions;
- The likelihood that the controller would detect the failure before any significant event occurred; and
- The chance that if a failure occurred, and was not detected, that this would not result in a significant event.

H.2.25 These assumptions impact on the probability of an accident.

Visibility assumptions

H.2.26 The definitions for these visibility conditions in use at Heathrow is:

- Visibility condition 1: visibility greater than or equal to 2000m;
- Visibility condition 2: visibility less than 2000m but greater than 400m (based on the distance from the VCR to the furthest taxiway);
- Visibility condition 3:visibility less than 400m;
- Visibility condition 4: currently not defined.

Detection by the controller of an A-SMGCS failure

H.2.27 Assumptions regarding the detection probability with which a controller will detect a failure.

		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 20: Assumptions regarding detection rates of A-SMGCS failures

H.2.28 Assumptions made regarding the probability of an incident occurring if a hazard occurs

		'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 21: Assumptions regarding the probability of an incident should a failure occur

H.3 H01 – Total loss of A-SMGCS

H.3.1 Introduction

H.3.1.1 The contributing elements for total loss of A-SMGCS are

- Display and Data Fusion or;

- Surveillance (Multi-lateration and SMR).
-
-
-
-
-

H.3.2 A-SMGCS display and data fusion system

Evidence ID	Type of evidence	Argument	System to which argument applies
E-ID I.	System specifications	NATS specification for the Display and Data Fusion System for total failure was 1E-04 per hour. Tender response for the reliability of the system was 1.0E-06 per hour for the Display and Data Fusion System	Display and Data Fusion System
E-ID II.	System Specifications	NATS specified the loss of one position at 1E-03	System
E-ID III.	Historical	One instance of the loss of a single display due to a display power supply is recorded with a historical MTBF of 38600 hours (2.6E-5 per hour). This did not result in a loss of service due to the dual power architecture.	Display System
E-ID IV.	Historical	In one installation a number of failures were recorded for the display shortly after installation. However, these were determined to be due to a software fault. During this period, total loss of A-SMGCS display did not occur since the controller had access to the slave display.	Display System
E-ID V.	Procedure	The Data Fusion system is designed to be maintenance free. Very little on-site maintenance activities are required reducing the chance of accidental damage during maintenance activities.	Data Fusion System
E-ID VI.	System specifications	Much of the system has been developed using standard COTS products that are already mature in design.	Data Fusion System
E-ID VII.	System specifications	The system includes software to protect against the failure of system critical components.	Data Fusion System
E-ID VIII.	System specifications	The system has inbuilt redundancy.	Data Fusion System

H.3.3 A-SMGCS sensors

Evidence ID	Type of evidence	Argument	System to which argument applies
E-ID IX.	System specifications	SMR system was manufactured to a tendered reliability of 1.3E-06.	SMR
E-ID X.	System specifications	The failure rate of the multi-lateration system was specified as 1E-04 per hour	Multi-lateration System
E-ID XI.	Reliability analysis	The SMR was calculated to have an estimated failure rate of 2.5E-04 per hour.	SMR
E-ID XII.	System specifications	The SMR has been upgraded at Heathrow with a predicted reliability of 2.5E-05 per hour.	SMR
E-ID XIII.	System specifications	The software content of the SMR is negligible and as such any software failure causing total loss of the sensor would be remote.	SMR
E-ID XIV.	Reliability analysis	The multi-lateration system was calculated to have an estimated failure rate of 7.45E-05 per hour	Multi-lateration System

H.3.4 Other evidence

H.3.4.1 The Heathrow A-SMGCS system has been in operation from the end of 1999 and a complete system failure has never occurred. This equates to approximately five and a half years of operation or 50000 hours of operation.

H.3.4.2 A reliability analysis for the total loss of A-SMGCS was performed (see annex I). The predicted probability of a complete failure is 9.9E-5 per hour. This was dominated by the power within the control tower

H.4 H02 – Loss of the position function for one aircraft

H.4.1 Introduction

H.4.1.1 The contributing elements for to Loss of the Position Function for one aircraft are

- Display and Data Fusion or;
- Surveillance (Multi-lateration and SMR) or;
- Avionics failure.

H.4.2 Display and data fusion system

Evidence ID	Type of evidence	Argument	System to which argument applies
E-ID XV.	System specifications	The failure rate of the Display and Data Fusion System was specified at 1E-06 per hour	Display and Data Fusion System
E-ID XVI.	Historical	There is no evidence of the Display and Data Fusion System contributing to this failure condition. This results in an estimated MTBF for this component of 2.0E-05 per hour.	Display and Data Fusion System
E-ID XVII.	System	Much of the system has been developed using standard COTS products that are already	Display and Data

	specifications	mature in design.	Fusion System
E-ID XVIII.	Historical	There is no evidence of the Heathrow Display system exhibiting this failure. The Heathrow A-SMGCS system has been in operation from the end of 1999. This equates to approximately five and a half years of operation or 50000 hours of operation.	Display and Data Fusion System
E-ID XIX.	System specifications	Much of the system has been developed using standard COTS products that are already mature in design.	Display and Data Fusion System
E-ID XX.	System specifications	The system includes software to protect against the failure of system critical components.	Display and Data Fusion System
E-ID XXI.	System specifications	The system has inbuilt redundancy.	Display and Data Fusion System
E-ID XXII.	System specifications	The Data Fusion system is designed to be maintenance free. Very little on-site maintenance activities are required reducing the chance of accidental damage during maintenance activities.	Servers

H.4.3 Sensors and avionics

Evidence ID	Type of evidence	Argument	System to which argument applies
E-ID XXIII.	System Specifications	The estimated loss of position for one aircraft is 6.4E-9 per hour	Multi-lateration system
E-ID XXIV.	System Specifications	The estimated loss of position for one aircraft is 1.25E-2 per hour	SMR
E-ID XXV.	System specifications	SMR has been upgraded at Heathrow with a predicted reliability of 2.5E-05 per hour	SMR
E-ID XXVI.	Calculated	The complete loss of a transponder function is 1.49E-3 per hour	Aircraft Mode S transponder
E-ID XXVII.	System specifications	The failure rate of the multi-lateration system was specified as 1E-04 per hour	Multi-lateration system
E-ID XXVIII.	System specifications	SMR system was manufactured to a tendered reliability of 1.3E-06.	SMR
E-ID XXIX.	System specifications	The SMR performance was specified at 2.44E-14 per hour	SMR
E-ID XXX.	Reliability analysis	The multi-lateration system was calculated to have an estimated failure rate of 7.45E-05 per hour	Multi-lateration system

E-ID XXXI.	System specifications	The software content of the SMR is negligible and as such any software failure causing total loss of the sensor would be remote.	SMR

H.5 H03 – Loss of position function impacting multiple aircraft

H.5.1 Introduction

H.5.1.1 The worst case (in safety terms) is to assess the loss of position for two aircraft. The contributing elements for to Loss of the Position Function for multiple aircraft are

- Display and Data Fusion or;
- Surveillance (Multi-lateration and SMR) or;
- Avionics failure.

H.5.2 Display and data fusion system

Evidence ID	Type of evidence	Argument	System to which argument applies
E-ID XXXII.	Historical	There is no evidence of the Display and Data Fusion System contributing to this failure condition. This results in an estimated MTBF for this component of 2.0E-05 per hour.	Display and Data Fusion System
E-ID XXXIII.	System specifications	The displays are designed without a frame buffer. Therefore, the possibility of the display freezing in a certain area of the screen is not possible.	Display system

H.5.3 Sensors

H.5.3.1 Both multi-lateration and SMR are required to fail at the same time for two aircraft to be dropped. This is highly unlikely based on the probability of failure of a single target. Dual sensor failure is not considered.

H.5.3.2 For this failure to occur, either

- the target is in SMR and Multi-lateration coverage and both the transponder and SMR fail at the same time;
- the target is in SMR and Multi-lateration coverage and both the Multi-lateration sensors and SMR fail at the same time.

Evidence ID	Type of evidence	Argument	System to which argument applies
E-ID XXXIV.	Calculated	The complete loss of a transponder function is 1.49E-2 per hour. The probability that this occurs for two aircraft, independently, at the same time is 2.2E-4	Aircraft Mode S transponder
E-ID XXXV.	System Specifications	The estimated loss of position for one aircraft is 6.4E-9 per hour. For two aircraft this is 4.1E-7	Multi-lateration system
E-ID XXXVI.	System	The estimated loss of position for one aircraft is	SMR

	Specifications	1.25E-3 per hour. For two aircraft this is 1.56E-6	
E-ID XXXVII.	System specifications	SMR has been upgraded at Heathrow with a predicted reliability of 2.5E-05 per hour	SMR
E-ID XXXVIII.	System specifications	The failure rate of the multi-lateration system was specified as 1E-04 per hour	Multi-lateration system

H.5.3.3 It is noted that avionics failure and SMR failure are required at the same time when the aircraft is in full sensor coverage.

H.6 H04 – Corruption of position function for one aircraft

H.6.1 Introduction

H.6.1.1 The contributing elements for to Corruption of Position Function for a single aircraft are

- Display and Data Fusion or;
- Surveillance (Multi-lateration or SMR).

H.6.1.2 Avionics failure does not contribute to this failure

H.6.1.3 NATS have specified the multi-lateration system be able to prevent the output of positions that are more than 30m from the target's true position. This is defined as the corruption of position.

H.6.2 Display and data fusion system

H.6.2.1 This failure may be described as the presentation of an incorrect position report due to the display. This corruption is due entirely to the display element of the system. There is no evidence that this failure has occurred for operations at Heathrow.

H.6.3 Sensors

Evidence ID	Type of evidence	Argument	System to which argument applies
E-ID XXXIX.	System Specifications	The estimated corruption of position for one aircraft is 4.9E-5 per hour.	Multi-lateration system
E-ID XL.	System Specifications	The estimated corruption of position for one aircraft is 2.3E-4 per hour.	SMR
E-ID XLI.	Reliability analysis	The reliability analysis, carried out by NATS in support of their local safety case, predicted the probability of anomalous behaviour (e.g inaccurate position) of better than 2.3E-04 per	SMR

		hour.	
E-ID XLII.	System specifications	NATS specification for the MLAT system was 7.5m 95% and 12m 99%.	Multi-lateration system
E-ID XLIII.	Historical	The amount of spurious plots form the SMR system at Heathrow is well documented and produced at tolerable levels. However, these plots occur in known areas and can be dealt with by the Data Fusion System.	SMR
E-ID XLIV.	System specifications	The system should be able to prevent the output of positions that are more than 30m from the target's true position.	Multi-lateration system

H.7 H05 – Corruption of the position function impacting multiple aircraft

H.7.1 Introduction

H.7.1.1 The contributing elements for to Corruption of Position Function affecting multiple aircraft are

- Display and Data Fusion or;
- Surveillance (Multi-lateration or SMR).

H.7.1.2 Avionics failure does not contribute to this failure

H.7.2 Display and data fusion system

H.7.2.1 The Display and Data Fusion System is unlikely to corrupt the position for more than one aircraft

Evidence ID	Type of evidence	Argument	System to which argument applies
E-ID XLV.	Historical	There has not been any evidence of the Display and Data Fusion System causing corruption of position.	Display and Data Fusion System
E-ID XLVI.	System specification	The software in the display system has been developed using accredited formal software development procedures	Display and Data Fusion System
E-ID XLVII.	System specification	Displays are designed such that it is not possible for the system to display delayed data.	Display and Data Fusion System
E-ID XLVIII.	System specification	The software in the Display and Data Fusion System has been developed using accredited formal software development procedures	Display and Data Fusion System

H.7.3 Sensors

H.7.3.1 It is unlikely that both multi-lateration and SMR will fail for a sub-set of aircraft on the aerodrome surface at the same time. Evidence suggests that the probability is so low that the sensors are more probable to fail completely than loose a number of tracks simultaneously.

Evidence ID	Type of	Argument	System to which

	evidence		argument applies
E-ID XLIX.	System Specifications	The estimated corruption of position for one aircraft is 4.9E-5 per hour. For two aircraft this is 2.4E-9	Multi-lateration system
E-ID L.	System Specifications	The estimated corruption of position for one aircraft is 2.3E-4 per hour. For two aircraft this is 5.29E-8	SMR
E-ID LI.	Reliability analysis	The reliability analysis, carried out by NATS in support of their local safety case, predicted the probability of anomalous behaviour (inaccurate position) of better than 2.3E-04 per hour.	SMR
E-ID LII.	Calculated	The specification for the multi-lateration system was for a probability of false detection of 1.0E-3 with an update rate of 2 seconds.	Multi-lateration system
E-ID LIII.	System specification	The specification for the multi-lateration system was for a probability of false detection of 1.0E-3 with an update rate of 2 seconds.	Multi-lateration system
E-ID LIV.	System specification	NATS specification for the MLAT system to output the target positions within 7.5m for at least 95% of detections and within 12m for 99% of detections. All targets had to be reported within 30m of their actual position.	Multi-lateration system
E-ID LV.	Historical	The amount of spurious plots form the SMR system at Heathrow is well documented and produced at tolerable levels. However, these plots occur in known areas and can be dealt with by the Data Fusion System.	SMR
E-ID LVI.	System specification	There is very little software content within the sensors. Failures will predominantly be due to hardware or external factors	Multi-lateration system SMR

H.8 H06 – Total loss of the identification function

H.8.1 Introduction

H.8.1.1 The Total Loss of Identification Function will impact all targets on the display.

H.8.1.2 Issues relating to reliability of complete systems (e.g. MTBF of Multi-lateration) are not considered in this analysis because, should they occur then hazard 01 (total loss of system functions) would occur. Therefore components, which only impact the identification, are discussed. Failures, which would result in complete system failure, are covered in hazard 01.

Evidence

H.8.1.3 There has been no incident of total loss of identification during the operations at Heathrow providing an estimated failure rate of 2.0E-05 per hour (see **Error! Reference source not found.**)

H.8.2 Display and data fusion system

Evidence ID	Type of evidence	Argument	System to which argument applies
E-ID LVII.	System specification	The system specification for the inability of the Display and Data Fusion System to process the identification from the multi-lateration system was 1.0E-04 per hour.	Display and Data Fusion System
E-ID LVIII.	System specification	The software in the Display and Data Fusion System has been developed using accredited formal software development procedures	Display and Data Fusion System

H.9 H07 – Loss of the identification function impacting multiple aircraft

H.9.1 Introduction

H.9.1.1 The contributing elements for to Loss of the identification function impacting multiple aircraft are:

- Display and Data Fusion or;
- Surveillance (Multi-lateration).
- Avionics

H.9.2 Display and data fusion system

H.9.2.1 The following table presents evidence that the Heathrow Display and Data Fusion System meets the requirement for the Loss of Identification Function for multiple aircraft.

Evidence ID	Type of evidence	Argument	System to which argument applies
E-ID LIX.	System specification	The system specification for the inability of the Display and Data Fusion System to process the identification from the multi-lateration system was 1.0E-04 per hour. Assuming common cause failure, this figure may apply to multiple targets.	Display and Data Fusion System
E-ID LX.	Historical	There has been on incident of total loss of identification due to a software fault that has been corrected.	Display and Data Fusion System
E-ID LXI.	System specification	The software in the Display and Data Fusion System has been developed using accredited formal software development procedures	Display and Data Fusion System

H.9.3 Sensors

Evidence ID	Type of evidence	Argument	System to which argument applies
E-ID LXII.	System specifications	The NATS requirement for the probability of false identification of aircraft ID has been specified as 1.0E-06 per hour. Assuming a	Multi-lateration system

		common cause failure, this figure remains valid	
E-ID LXIII.	Calculated	The instantaneous loss of identification from the avionics will occur in when the transponder fails. This will result in the loss of position and is therefore not considered as part of this failure	Avionics
E-ID LXIV.	System specification	The software in the multi-lateration system has been developed using accredited formal software development procedures	Multi-lateration system
E-ID LXV.	System specification	A system specification was placed for the availability of the multi-lateration system of H24 365 days	Multi-lateration system

H.10 H08 – Corruption of the identification function for one aircraft

H.10.1 Introduction

H.10.1.1 The contributing elements for to Corruption of identification function for one aircraft

- Display and Data Fusion or;
- Surveillance (Multi-lateration).
- Avionics
- Code Callsign Function

H.10.2 Display and data fusion system

Evidence ID	Type of evidence	Argument	System to which argument applies
E-ID LXVI.	Historical evidence	There is no recorded evidence that the Display and Data Fusion System has contributed to this hazard. Therefore the MTBF is estimated at 2.0 E-5.	Display and Data Fusion System
E-ID LXVII.	Design specifications	The reliability of the design of the displays	Display and Data Fusion System
E-ID LXVIII.	System specifications	The software used within the Display and Data Fusion System has been developed using accredited formal software development procedures	Display and Data Fusion System
E-ID LXIX.	Design specifications	The Display and Data Fusion System is dependent upon the multi-lateration system for identification of the aircraft. In the event that the multi-lateration system should have a total or partial loss, the system will revert to using the track information supplied by the SMR to maintain aircraft ID. When no multi-lateration cover is available outside of the areas of good SMR coverage, the identification is removed after a short period of time.	Display and Data Fusion System

E-ID LXX.	Design specifications	The Display and Data Fusion System tracks the target to maintain identification. As no updates are received on the identification once the Display and Data Fusion System start tracking, presentation of identification is limited to the runways.	Display and Data Fusion System

H.10.3 Sensors

Evidence ID	Type of evidence	Argument	System to which argument applies
E-ID LXXI.	System specifications	The NATS requirement for the probability of false identification of aircraft has been specified as 1.0E-06 per hour	Multi-lateration system
E-ID LXXII.	Calculated	The corruption of the identification delivered from the transponder is 1.5E-4 per hour.	Avionics
E-ID LXXIII.	System design	The multi-lateration system will update the identification of the aircraft once every second. The identification transmission is received from the aircraft by at least three ground multi-lateration system sensors; it is unlikely that all three sensors will be susceptible to the same fault at the same time.	Multi-lateration system

H.10.4 Code callsign

H.10.4.1 The following table presents evidence that the Heathrow Code Callsign system meets the requirement for the Corruption of Identification Function for one aircraft.

Key Evidence item

Evidence ID	Type of evidence	Argument	System to which argument applies
E-ID LXXIV.	Reliability analysis	The NATS safety case for CCDS claims a probability of credible or incredible corruption in the order of 1.0E-06 per hour	Code Callsign
E-ID LXXV.	System design	It is assumed that, as the radars providing the SSR code and the code callsign distribution system (CCDS) are high integrity systems, it is improbable that they would provide incorrect callsigns.	Code Callsign

H.11 H09 – Corruption of the identification function impacting multiple aircraft

H.11.1 Introduction

H.11.1.1 The contributing elements for the Corruption of the identification function impacting multiple aircraft are

- Display and Data Fusion or;
- Surveillance (Multi-lateration).
- Avionics

- Code Callsign Function

H.11.2 Display and data fusion system

Evidence ID	Type of evidence	Argument	System to which argument applies
E-ID LXXVI.	Historical evidence	There is no recorded evidence that the Display and Data Fusion System has contributed to this hazard. Therefore the MTBF is estimated at 2.0 E-5.	Display and Data Fusion System
E-ID LXXVII.	Design specifications	The reliability of the design of the displays	Display and Data Fusion System
E-ID LXXVIII.	System specifications	The software used within the Display and Data Fusion System has been developed using accredited formal software development procedures	Display and Data Fusion System
E-ID LXXIX.	Design specifications	The Display and Data Fusion System is dependent upon the multi-lateration system for identification of the aircraft. In the event that the multi-lateration system should have a total or partial loss, the system will revert to using the track information supplied by the SMR to maintain aircraft ID. When no multi-lateration cover is available outside of the areas of good SMR coverage, the identification is removed after a short period of time.	Display and Data Fusion System
E-ID LXXX.	Design specifications	The Display and Data Fusion System tracks the target to maintain identification. As no updates are received on the identification once the Display and Data Fusion System start tracking, presentation of identification is limited to the runways.	Display and Data Fusion System

H.11.3 Sensors

H.11.3.1 The following table presents evidence that the Heathrow Sensor system meets the requirement for the Corruption of Identification Function for one aircraft.

Evidence ID	Type of evidence	Argument	System to which argument applies
E-ID LXXXI.	Calculated	The corruption of the identification delivered from the transponder is 1.5E-3 per hour. For two transponder to simultaneously fail, the probability is 2.2 E-8	Avionics
E-ID LXXXII.	System specifications	The NATS requirement for the probability of false identification of aircraft ID has been specified as 1.0E-06. Assuming common cause fail then this figure remains valid	Multi-lateration system
E-ID LXXXIII.	System design	The multi-lateration system will update the identification of the aircraft once every second.	Multi-lateration system

		The identification transmission is received from the aircraft by at least three ground multi-lateration system sensors; it is unlikely that all three sensors will be susceptible to the same fault at the same time.	

H.11.4 Code Callsign

H.11.4.1 The following table presents evidence that the Heathrow Code Callsign system meets the requirement for the Corruption of Identification Function for one aircraft.

Evidence ID	Type of evidence	Argument	System to which argument applies
E-ID LXXXIV.	Reliability analysis	The NATS safety case for CCDS claims a probability of credible or incredible corruption in the order of 1.0E-06 per hour. Assuming common cause fail then this figure remains valid	Code Callsign
E-ID LXXXV.	System design	It is assumed that, as the radars providing the SSR code and the code callsign distribution system (CCDS) are high integrity systems, it is improbable that they would provide incorrect callsigns.	Code Callsign

Other Evidence

H.11.4.2 There has been no incident of corruption of identification for multiple aircraft during the operations at Heathrow providing an estimated failure rate of 2.0E-05 per hour.

H.12 H10 – Corruption of the conflict prediction function

H.12.1.1 Following initiatives to analyse and improve performance, the Heathrow RIMCAS performance has been measured as 26 false alerts over a period of 10 weeks. Of these, 20 alerts persisted for more than 3 seconds and were included in the false alert total.

H.12.1.2 This equates to a false alert rate of 1.2E-02 per operational hour.

H.12.1.3 This false alert rate has not been apportioned to different sub-systems. There is no evidence or technical possibility for the display system to contribute to this failure. Furthermore, the system is designed to reject false targets and therefore failures of the multi-lateration system or SMR will not necessarily result in false alerts. Therefore, it is not considered appropriate to discuss RIMCAS performance in terms of individual components.

H.13 Summary of LHR performance

H.13.1 The evidence presented above is summarised below.

HZ	Hazard	Order of magnitude for the evidence at LHR						
		Display and data fusion	Sensors	Code Callsign	Conflict Prediction		MLAT and avionics	SMR
H01	Total loss of A-SMGCS	1.00E-06	1.30E-10	N/A	N/A		1.00E-04	1.30E-06
H02	Loss of the position function for one aircraft	2.00E-05	1.88E-05	N/A	N/A		1.50E-03	1.25E-02
H03	Loss of the position function impacting multiple aircraft	2.00E-05	3.52E-10	N/A	N/A		2.25E-06	1.56E-04
H04	Corruption of the position function for one aircraft	Not Credibl	2.79E-04	N/A	N/A		4.90E-05	2.30E-04
H05	Corruption of the position function impacting multiple aircraft	Not Credibl	5.43E-07	N/A	N/A		4.90E-07	5.29E-08
H06	Total loss the identification function	1.00E-04	N/A	N/A	N/A		N/A	N/A
H07	Loss of the identification function impacting multiple aircraft	1.00E-04	1.00E-06	N/A	N/A		1.00E-06	N/A
H08	Corruption of the identification function for one aircraft	2.00E-05	1.50E-04	1.00E-06	N/A		1.50E-04	N/A
H09	Corruption of the identification function impacting multiple aircraft	2.00E-05	1.00E-06	1.00E-06	N/A		1.00E-06	N/A
H10	Corruption of the conflict prediction function	Not Credibl	N/A	N/A	1.79E-02		N/A	N/A

Note that the avionics failure is included in the MLAT failure

I Reliability Analysis

I.1 Introduction

I.1.1 This section presents the reliability analysis which was carried out as part of the safety case for A-SMGCS for Heathrow.

I.1.2 Failure modes analysis has been carried out on the A-SMGCS system to determine the probability of various failures and the time to repair the failures.

I.1.3 A-SMGCS is made up of subsystems. A failure mode can happen as a result of one or more subsystem failures. Sections 1.3 – 1.5 provide preliminary modelling of each subsystem.

I.1.4 The MTBF (Mean Time Between Failure) and MTTR (Mean Time To Repair), have been calculated by modelling the system using RAM4. The reliability figures are taken from table 1. All reliability figures are in hours.

I.2 RAM4

I.2.1 RAM4 version 3.3 has been used to model the A-SMGCS system with its subsystems and to calculate the reliability figures. A table of reliability figures has been given with each subsystem.

I.2.2 For the failure and repair distributions a lognormal distribution has been used. The lognormal distribution is usually used to describe repair times. The distribution value is always 0.6 which is being associated with a modular repair policy (e.g. replacement of Line Replaceable Units on failure), the median value is associated with equipment repair at component level.

I.2.3 The MTTR median and distribution have been estimated as follows:

- Median = MTTR * 0.84
- Distribution = 0.6

I.3 SMR System

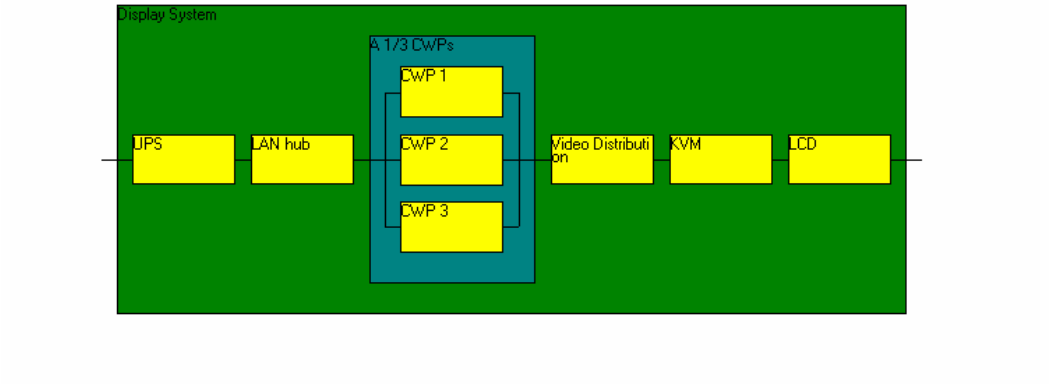
- The reliability of the SMR has been calculated for SMR and are:MTBF = 4402 MTTR = 17

I.3.1 This includes the dualised radar extractors. From this point the probability of a failure occurring that causes a total loss of SMR, but that does not cause total loss of the whole A-SMGCS are very small. The hardware and software used to display the SMR data is common to other elements of the system. There have been no reported instances of loss of SMR alone, caused by the display system. In order to account for the small probability of the display system generating this kind if failure, a figure of 1 failure per 5 years is assessed as being valid.

I.3.2 The overall probability of total loss of SMR is calculated as 2.5 x 10-4 per hour.

I.4 Display System (Single channel of full display system).

I.4.1 The data for the Display System (Single Channel) has been calculated. The Reliability block diagram for Display System 1 is shown below.



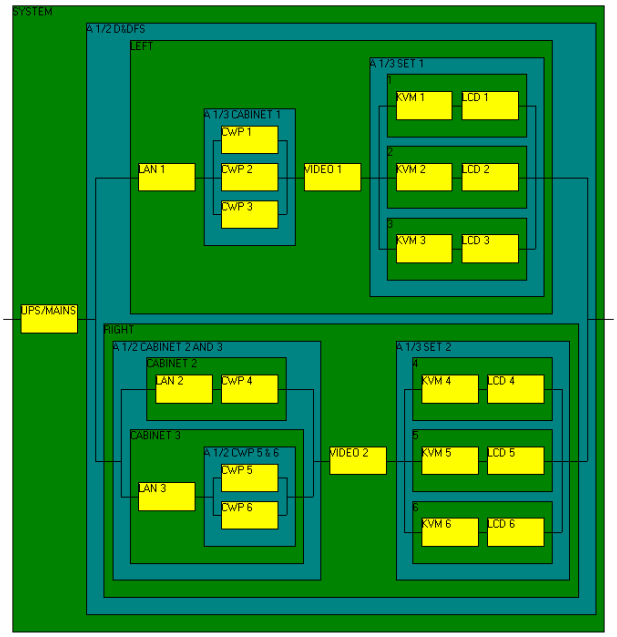
I.4.2 The figures for Display System 1 have been calculated out by modelling the system and the results are as follows:

- Mission Length = 100 000
  No. of Replications = 10 000

	Estimate	Lower 95% CI	Upper 95% CI
MTBF	4069.74	4027.37	4112.11
MTTR (Arith)	3.73662	3.63166	3.84158
MTTR (Geom)	1.03868	1.02127	1.05638
MTFF	4083.76	3861.09	4306.43
Availability	99.9083	99.9056	99.9110
SFR (1/MTBF)	2.457160E-04	2.431842E-04	2.483011E-04

I.5 Full Display System.

I.5.1 The Reliability Block Diagram for the Full Display System is shown below. The system has been modelled and the MTBF and MTTR have been calculated.



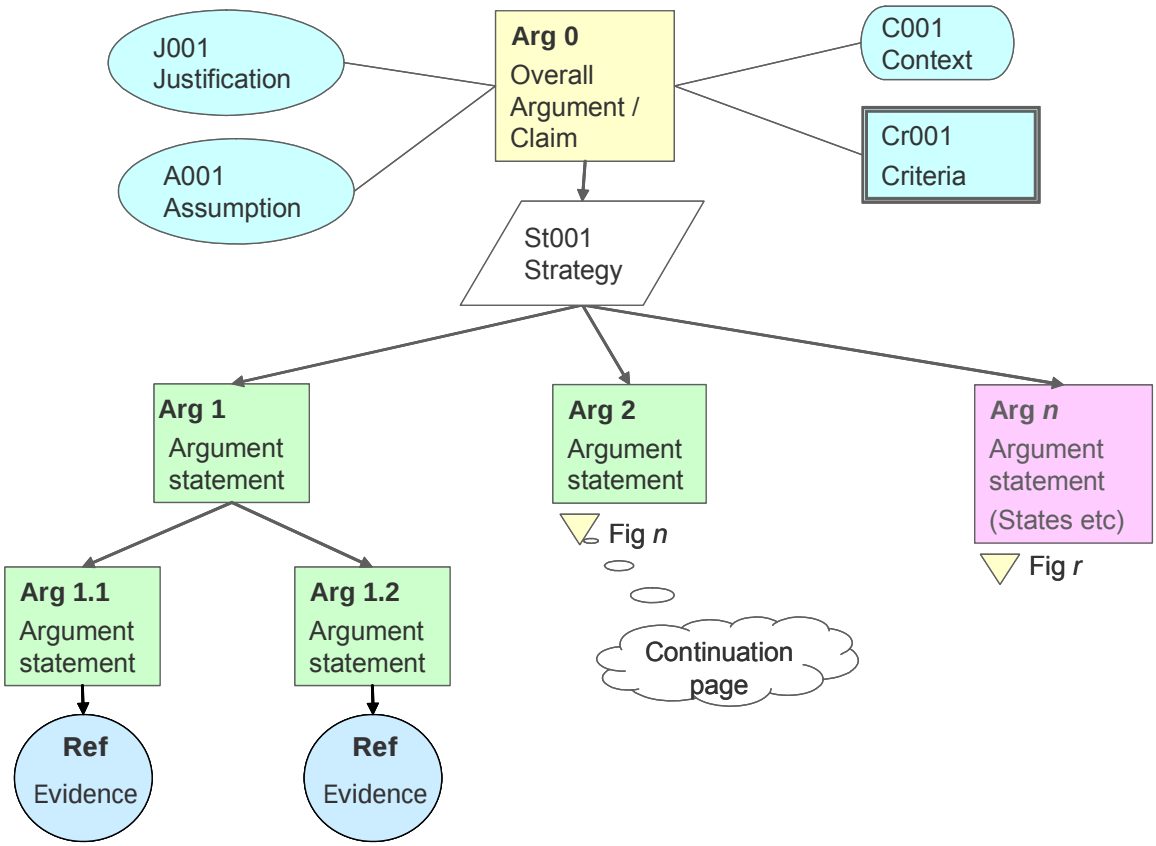
I.5.2 Mission Length = 100 000
No. of Replications = 10 000

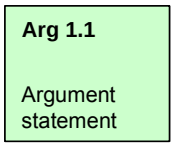
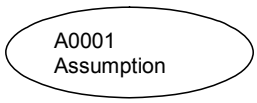
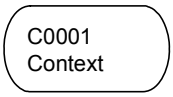
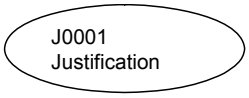
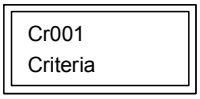
	Estimate	Lower 95% CI	Upper 95% CI
MTBF	10010.9	9914.10	10107.7
MTTR (Arith)	1.01542	1.00402	1.02681
MTTR (Geom)	0.565479	0.557656	0.573411
MTFF	10007.3	9665.98	10348.6
Availability	99.9899	99.9897	99.9900
SFR (1/MTBF)	9.989126E-05	9.893476E-05	1.008665E-04

J Goal structured notation

J.1.1 This section presents an overview of GSN which is used to define the A-SMGCS argument

Requirement	Since the Safety Argument forms the framework of a Safety Case, it is important that the Argument is set out in a rigorous, hierarchical and well-structured and easily-understood way.
GSN Solution	Goal structured Notation (GSN), developed by the University of York, provides a graphical means of setting out hierarchical safety arguments, with textural annotations and references to supporting Evidence. The logical approach of GSN, if correctly applied, brings some rigour into the process of deriving safety arguments and provides the means for capturing essential explanatory material, including assumptions, context and justifications, within the argument framework. The diagram below shows, in an adapted form of GSN, a specimen *Argument* and *Evidence* structure to illustrate the GSN symbology most commonly used in EUROCONTROL ATM safety applications.



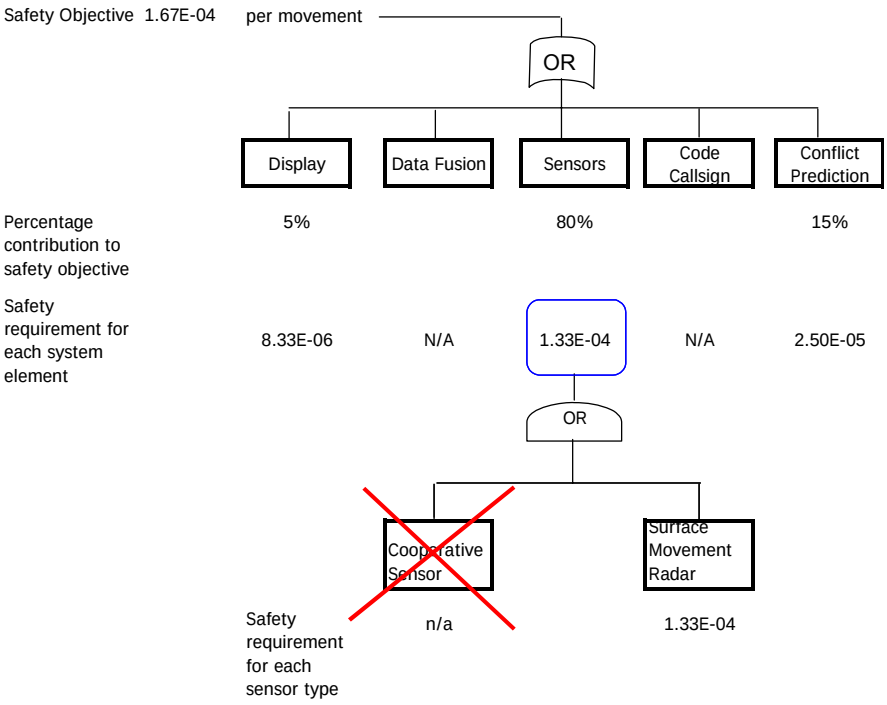
Arguments 	An Argument should take the form of a simple predicate - i.e. a statement which can be shown to be only either true or false. GSN provides for the structured decomposition of Arguments into lower-level Arguments; logically. For an Argument structure to be valid, it is essential to ensure that, at each level of decomposition: - the family of Arguments is sufficient to show that the parent Argument is true. - there is no valid (negative) Argument that could undermine the parent Argument. In the above diagram, for example, if it can be shown that Arg 1 is satisfied by the combination of Arg 1.1 and Arg 1.2, then we need to show that Arg 1.1 and Arg 1.2 are true in order to show that Arg 1 is true. If this principle is applied rigorously all the way down through and across a GSN structure, then it is necessary to show only that each element at the very bottom of the structure is satisfied (i.e. shown to be true) in order to assert that the top-level Argument (or Claim – see below) has been satisfied. Satisfaction of the lowest-level Arguments is the purpose of Evidence.
Evidence 	The reference in this document to the supporting evidence for the argument.
Strategies 	Strategies are a useful means of adding “comment” to the structure to explain, for example, how the decomposition will develop. They are not predicates and do not form part of the logical decomposition; rather, they are there purely for explanation of the decomposition.
Assumptions 	An Assumption is a statement that has to be relied upon in order for the satisfaction of an Argument. Assumptions may also be attached to other GSN elements including Strategies and Evidence. The validity of each Assumption must be demonstrated before a Safety Argument can be considered to be complete.
Context 	Context provides information necessary to for an Argument (or other GSN element) to be understood, amplified or satisfied. Context may include a statement which limits the scope of an Argument in some way.
Justification 	A Justification is used to give a rationale for the use or satisfaction of a particular Argument or Strategy. More generally it can be used to justify the change that is the subject of the overall Safety Argument.
Criteria 	Criteria are the means by which the satisfaction of an Argument can be checked.

K Relative argument

K.1.1 This section presents a brief analysis of the safety impact of introducing A-SMGCS Level 1 against a baseline of SMR only at an airport for the POSITION function only because SMR only influences position.

K.1.2 The analysis presented in the annex is for illustration purposes only and is not intended to be a comprehensive, systematic comparative safety assessment.

K.1.3 If we assume that the safety requirements for A-SMGCS Level 1 apply at LHR for an SMR only implementation then all the sensors safety requirements are allocated to SMR as illustrated below (for hazard 10).



K.1.4 If the cooperative sensors are elimated from all hazards where SMR influences the safety requirements, then the resulting safety requirements will be re-allocated as illustrated below.

HZ	Hazard	Safety requirements (per hour)						
		Display and data fusion	Sensors	Code Callsign	Conflict Prediction		MLAT	SMR
H01	Total loss of A-SMGCS	3.25E-05	1.67E-05	N/A	N/A		N/A	1.67E-05
H02	Loss of the position function for one aircraft	3.10E-03	1.60E-03	N/A	N/A		N/A	1.60E-03
H03	Loss of the position function impacting multiple aircraft	1.66E-04	8.54E-05	N/A	N/A		N/A	8.54E-05
H04	Corruption of the position function for one aircraft	1.70E-03	8.74E-04	N/A	N/A		N/A	8.74E-04
H05	Corruption of the position function impacting multiple aircraft	2.02E-03	1.04E-03	N/A	N/A		N/A	1.04E-03
H10	Corruption of the conflict prediction function	N/A	N/A	N/A	2.03E-02		N/A	N/A

K.1.5 Evidence from Heathrow relating to the performance of SMR is illustrated

HZ	Hazard	Order of magnitude for the evidence at LHR						
		Display and data fusion	Sensors	Code Callsign	Conflict Prediction		MLAT and avionics	SMR
H01	Total loss of A-SMGCS	1.00E-06	1.30E-06	N/A	N/A		N/A	1.30E-06
H02	Loss of the position function for one aircraft	2.00E-05	1.25E-02	N/A	N/A		N/A	1.25E-02
H03	Loss of the position function impacting multiple aircraft	2.00E-05	1.56E-04	N/A	N/A		N/A	1.56E-04
H04	Corruption of the position function for one aircraft	Not Credibl	2.30E-04	N/A	N/A		N/A	2.30E-04
H05	Corruption of the position function impacting multiple aircraft	Not Credibl	5.29E-08	N/A	N/A		N/A	5.29E-08
H10	Corruption of the conflict prediction function	Not Credibl	N/A	N/A	1.07E-03		N/A	N/A

K.1.6 This shows that the order of magnitude between the performance of an SMR only solution against the safety requirements for A-SMGCS Level 1 results in a reduced safety margin against A-SMGCS performance. In some cases the safety margin is reduced such that the safety requirements are not achieved in an SMR only implementation.

HZ	Hazard	Results of LHR assessment (order of magnitude difference between requirement and perfromance						
		Display and data fusion	Sensors	Code Callsign	Conflict Prediction		MLAT	SMR
H01	Total loss of A-SMGCS	1	1	N/A	N/A		N/A	1
H02	Loss of the position function for one aircraft	2	-1	N/A	N/A		N/A	-1
H03	Loss of the position function impacting multiple aircraft	0	-1	N/A	N/A		N/A	-1
H04	Corruption of the position function for one aircraft	Not Credible	0	N/A	N/A		N/A	0
H05	Corruption of the position function impacting multiple aircraft	Not Credible	4	N/A	N/A		N/A	4
H10	Corruption of the conflict prediction function	Not Credible	N/A	N/A	1		N/A	N/A

Note that the avionics failure is included in the MLAT failure

safety requirement not achieved
order of magnitude same or less that 10 times greater
order of magnitude between 10 and 100 times greater
order of magnitude greater than 100 times

L Stakeholder involved in the development and validation of the preliminary safety case

L.1.1 The following stakeholders participated in the development and validation of the Preliminary Safety Case

Name	Organisation and role	Qualification
Bechere Maria Grazia	Airport Department at the Head Office in Rome	Bechere Maria Grazia has been an Air Traffic Controller since 1996 at ENAV the Italian Agency for Air Navigation Services. She is qualified in Tower and Radar Approach. She has over seven years as active controller at Genoa airport and is an internal expert for operations and procedures during low visibility conditions She is currently participating in a number of international activities including as member of the "A-SMGCS Procedure Group" within EUROCONTROL and a member for ENAV of the EC project "EMMA"
Bengt Collin	EUROCONTROL A-SMGCS Project	Bengt Collin was trained as a tower and approach controller with LFV Sweden and was posted at Stockholm-Arlanda Airport 1976. He often worked with parallel tasks; including one year at LFV headquarters. After working as Operational Manager at Arlanda Tower for four years he joined EUROCONTROL and the A-SMGCS project September 2002. Bengt held a valid air traffic controller licence until spring 2004.
Chris Diggins	NATS	Chris is Head of Airport System engineering at NATS, responsible for all aspects of airports project and design engineering. Since 1993 Chris has been involved in Eurocae activities relating to A-SMGCS and has contributed several papers in this area, recently taking on the role of chairman of the working group. In 1995 he was asked by the EC to evaluate tenders in their Fourth Framework Research Programme, as an expert in Surface Movement systems. He has also been closely involved with the working end of Safety Management since it was first conceived in NATS and has been responsible for its implementation within the groups he has managed.
Chris Wilson	NATS	Chris was responsible to the General Manager ATS for all aspects of the ATC service at

Name	Organisation and role	Qualification
		Heathrow including Safety Management, service delivery, ATC training and staff development. He is also responsible for the oversight of a number of projects affecting the ATC operation. Chris sits on the EUROCONTROL project procedures group and implementation strategy group and attends the A-SMGCS procedures and project co-ordination meetings accordingly.
Filip Prahl	Air Navigation Services (ANS) of the Czech Republic (Safety Expert)	Since 2001 Philip has been a member of ANS CR Safety & Quality Department as Safety Expert He has participated in safety management system design and implementation, developing ANS CR safety assessment methodology and conducting safety cases for systems (equipment and procedures). He is currently a member of the EUROCONTROL Safety Assessment Methodology Task Force (SAMTF)
Graeme Henderson	NATS	§Graeme is Manager of Surveillance and Display Systems in Airport Services division of NATS. He is the System Design Authority for NATS airport surveillance systems (including A-SMGCS) and project manager for the Heathrow A-SMGCS. As project manager, he was responsible for the production of the System Safety Case for A-SMGCS, which was necessary to gain approval from UK CAA for operational use of the system. He is also responsible for the production of System Safety Cases for Aeronautical Ground Lighting systems at Heathrow and several other UK airports and has participated in various European working groups settings standards for A-SMGCS (eg Multilateration Task Force, STFRDE – A-SMGCS, WG41).
Janet Wills	NATS	Janet was Manager Engineering at Heathrow Airport. Her roles include contributing to the safe and efficient operation of ATC systems. She has responsibility for ensuring the safe and efficient operation of Air Traffic Engineering at Heathrow Airport, and Civil Aviation Communication Centre in accordance with the ANO and SRG requirements. Janet is tasked with fully considering the safety implications of both the installation of and changes to ATS and CACC equipment and

Name	Organisation and role	Qualification
		ensuring that Safety and Quality requirements map to the NATS policies and principles.
Jean-Pierre Lesueur	EUROCONTROL	Jean-Pierre has over 30 years experience of ATM. Until 1999 he was an ATCO, Supervisor and Instructor, in charge of the training organisation of the tower side of the ATS in CDG. He was a member of many Working groups, notably SALADIN (SMGCS) and AVISO (A-SMGCS) projects for ADP. He then became Deputy Head of the Air Traffic Control Division (DNA 2C). In 2003 he became a contractor member of the EUROCONTROL APR programme.
Marc Vettovaglia,	Skyguide DMS, Systems Safety Management	Marc Vettovaglia has been working for skyguide for 4 years, He has an ATC licenses in TWR and APP, and an Airline Transport Pilot license.
Neil “Spike” Bainbridge	NATS	Neil has worked at Heathrow for over 14 years holding a number of posts and gaining a very thorough understanding of all the aspects of the operation. As a member of the technical committee, he was involved in the redesign of many procedures, most notably the Heathrow standard missed approach. From 2000 onwards, he was heavily involved in the taxiway designation project at Heathrow, including design of the designation system, development and delivery of the training system. Since joining ATC Operations in 2001 he has continued to work with HAL and the Airline Operators to align the operation with customer needs without compromising safety. He has been involved in numerous ATC investigations and developed procedures to prevent recurrence whenever necessary and he has also been involved in the establishment of a successful OJT scheme for TATC students. All the experience gained with Heathrow Approach and Thames Radar allows him to take into account the needs of other units when developing procedures. He has worked with EUROCONTROL on a number of projects, most notably A-SMGCS and Airport CDM.
Paul Adamson	EUROCONTROL A-SMGCS Project Manager	Paul trained as a tower/approach controller with UK NATS and has worked as an Air Traffic Controller in the UK, Luxembourg &

Name	Organisation and role	Qualification
		United Arab Emirates. Since 2002 he has been the Project Manager of the EUROCONTROL A-SMGCS Project. To complement his ATC experience, he has completed a Master of Science degree in Airport Planning & Management and is also an active private pilot.
Phil Faulkner	Skyguide – Swiss Air Navigation Services Ltd	Phil has over 30 years experience in ATM, He is currently the manager, OPS Safety Management and an Expert in ATM Procedures with Skygide. He was previously (until 2003) a Head air traffic controller and Operations manager with Airservices Australia.
Robert Granville	NATS	Robert is currently Manager SMS, the Safety and Quality division of NATS. He endorses NATS System Safety Cases, ensuring the requirements of the NATS Safety Management System are met. He acts as an independent advisor on Safety Management to NATS Chief Executive and is NATS representative at the EUROCONTROL Safety Assessment Methodology Task Force. In his previous roles in the Directorate of Safety, Robert represented NATS on the EUROCONTROL Safety Domain Task Force specifically with regard to Safety Assessment Methodology derivation and application. He has been responsible for the development of NATS SMS procedures and guidance for safety cases taking account of existing standards and safety practices in other organisations, both nationally and internationally.
Karin Anghus	EUROCONTROL	Started as operational Air Traffic Controller at Arlanda tower and approach in 1973. OJT Instructor from 1976. Has been working as Tower supervisor, Group super visor and managing the incident reporting system, all at Arlanda. Involved in IFATCA (1997) and chairman of the Flight Safety Committee for Sweden from 1998. Managing Flight safety seminars for 5 years. 2006: ATC operational expert at EUROCONTROL Airport unit, A-SMGCS project
Pascal Henry Ducos	DSNA-SDER	Expert ATCo at DSNA/SDER from 2001, specialised in Tower & Approach environments - HMI elaboration & testing 1991/2001: 10 years as Roissy-CDG ATCo and instructor, 1983/1991: 8 years in Toussus le Noble airport as

Name	Organisation and role	Qualification
		ATCo then Air Traffic Manager Involved with A-SMGCS design by: Set up of specifications for our experimental RIMS in DSNA/SDER for Roissy & Orly. DSNA representative to the EUROCONTROL A-SMGCS procedures workgroup. Participation to the EUROCONTROL A-SMGCS validation simulations / (Elaboration of runs and validation master plan) and participation to EMMA project Workshops and EUROCONTROL A-SMGCS Safety case
David Rayer	DSNA/ SNA RP	Paris CDG Airport, ATC Training Unit, in charge of Tower and Approach Simulators Air Traffic Controller at Paris CDG since January 2000 (Valid Tower and approach Radar ATCO Licence) Representing CDG ATC at different meetings related to A-SMGCS from 2006 (EUROCONTROL workshops on training and licencing, CBA) Presentation of CDG A-SMGCS level II at Luxembourg Eurocontrol Workshop)
Miroslav Tykal	ANS CR	Diploma(Dipl.-Ing) in Operation and economy of Aviation transport in 1976 at University of Transport and Communication in Zilina. Air traffic Controller,Senior Controller,Instructor of approach and tower Praha Ruzyne Airport from 1967 to 1981. Head of tower APP/TWR from 1981 to 1989 then Flight Navigator and Procedures designer for CAA until 1993. 1993-1996: Chief inspector ANS CR training centre. From 1996 : ATC specialist for Tower and approach procedures, Chief of the BETA and EMMA EC Project ANS CR Teams.

M Severity classification matrix

Severity Class	1 [Most Severe]	2	3	4	5 [Least Severe]
Effects on Airport Operations	Accidents	Serious Incidents	Major Incidents	Significant Incidents	No Immediate Effect on Safety
SEVERITY INDICATORS SET1: EFFECTS ON AIR NAVIGATION SERVICE					
Effect on Air Navigation Service at Airport	Total inability to provide or maintain safe service	Serious inability to provide or maintain safe service	Partial inability to provide or maintain safe service	Ability to provide or maintain safe but degraded service	No safety effect on service
ATCO and/or Flight Crew Working Conditions	Workload, stress or working conditions are such that they cannot perform their tasks at all	Workload, stress or working conditions are such that they are unable to perform their tasks effectively	Workload, stress or working conditions such that their ability is significantly impaired	Workload, stress or working conditions are such that their abilities are slightly impaired	No effect
Effect on ground ATM System and/or Aircraft Functional Capabilities	Total loss of functional capabilities	Large reduction of functional capabilities	Significant reduction of functional capabilities	Slight reduction of functional capabilities	No effect
ATCO and/or Flight Crew Ability to Cope with Adverse Operational and Environmental Conditions	Unable to cope with adverse operational and environmental conditions	Large reduction of the ability to cope with adverse operational and environmental conditions	Significant reduction of the ability to cope with adverse operational and environmental conditions	Slight reduction of the ability to cope with adverse operational and environmental conditions	No effect
SEVERITY INDICATORS SET 2: EXPOSURE					
Duration of the hazard	The presence of the hazard is almost permanent. Reduction of safety margins persists even after recovering from the immediate problem.	Hazard may persist for a substantial period of time	Hazard may persist for a moderate period of time.	Hazard may persist for a short period of time such that no significant consequences are expected.	Too brief to have any safety-related effect
Number of aircraft or vehicles exposed / area of responsibility	All aircraft in the area of responsibility	All aircraft/vehicles at the airport	Aircraft/vehicles within a small area or an area of low traffic density	Single aircraft or vehicle	No aircraft or vehicle affected

Severity Class	1 [Most Severe]	2	3	4	5 [Least Severe]
SEVERITY INDICATORS SET 3: RECOVERY					
Annunciation, Detection and Diagnosis	Undetected misleading indication.	Ambiguous indication. Not easily detected. Incorrect diagnosis likely	May require some interpretation. Detectable. Incorrect diagnosis possible	Clear annunciation. Easily detected, reliable diagnosis	Clear annunciation. Easily detected and very reliable diagnosis
Contingency measures (other systems or procedures) available	No existing contingency measures available. Operators unprepared. Limited ability to intervene.	Limited contingency measures, providing only partial replacement functionality. Operators not familiar with procedures or may need to devise a new procedure at the time.	Contingency measures available, providing most of required functionality. Fall back equipment usually reliable. Operator intervention required, but a practised procedure within the scope of normal training	Reliable, automatic, comprehensive contingency measures	Highly reliable, automatic, comprehensive contingency measures
Rate of development of the hazardous condition, compared to the time necessary for annunciation, detection, diagnosis and application of contingency measures	Sudden. It does not allow recovery	Fast	Similar	Slow	Plenty of time available.