EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

Generic Safety Assessment for ATC Surveillance using Wide Area Multilateration

Edition Number	:	5.0
Edition Date	:	23 October 2008
Status	:	Proposed Issue
Intended for	:	EATMP Stakeholders

EUROPEAN AIR TRAFFIC MANAGEMENT PROGRAMME

DOCUMENT CHARACTERISTICS

TITLE		
Generic Safety Assessment for ATC Surveillance using Wide Area Multilateration		
	EATMP Infocentre Reference:	
Document Identifier	**Edition Number:**	4.1
	Edition Date:	29.07.2008

Abstract

This document presents a generic safety assessment of the use of Wide Area Multilateration (WAM) for ATC surveillance. The assessment considers WAM in support of an ATC service (vectoring, monitoring and separation) in en-route and terminal airspace.

This safety assessment is a starting point for ANSPs developing a safety case for WAM systems. It also contains guidance for those undertaking such safety cases.

Keywords

Contact Person(s)	**Tel**	**Unit**

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:	\\HHBRUNA04\darbyb$\WAM\WAM CONTRACT Generic Safety (T06-11093EB)\2008 Final-final review	
Host System	Software	Size
Windows_NT	Microsoft Word 10.0	4329 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.		

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

CONTENTS

VOLUME 1

VOLUME 2

List of Figures

List of Tables

EXECUTIVE SUMMARY

This document presents a generic safety assessment for the provision of Wide Area Multilateration (WAM) surveillance in the en-route and terminal airspace in core area Europe. It is intended to support European Air Navigation Service Providers (ANSPs) that are implementing WAM equipment either as a sole means of surveillance or in conjunction with other surveillance sensors.

This report has been prepared for the EUROCONTROL Surveillance Domain. It is NOT a formal safety case for the use of WAM derived data.

The **aims** of the document are to:

- show that WAM can in principle be a safe source of data for the provision of an ATC (vectoring, monitoring and separation) service in terminal and en-route airspace,
- provide guidance to ANSPs to help them complete their own safety case;
- help ensure a consistent approach to the content of WAM safety cases across Europe.

The document contains a safety argument that ANSPs can use as a basis for the structure of their own safety cases.

The following **approach** is taken to demonstrating that WAM is 'safe in principle':

- The assumption is made that WAM will be used to enable the same services as radar - specifically aircraft vectoring, monitoring and separation. The presentation of WAM information to the controller will be very similar (or identical) to radar presentation. Controller procedures will be unchanged from radar procedures.
- Airborne equipment and procedures are assumed to be the same for WAM as for a radar environment.
- A generic Operational Service and Environment Description (OSED) is defined for the assessment. This describes a high-density environment based on future expected core-European traffic levels.
- A safety argument is defined, laying out the logic and evidence to show the ATC surveillance system including a WAM component is 'safe'. A core part of this argument is demonstrating compliance with ESARR4.
- An example minimal WAM surveillance sub-system is defined[1]. This illustrates the WAM functions that are expected to be present in a surveillance system of which WAM is a component.
- A generic Functional Hazard Assessment (FHA) and example Preliminary System Safety Assessment (PSSA) are undertaken. The FHA examines possible hazards associated with the presentation of information to the

[1] For clarity and brevity in the rest of the document, the word 'system' will be reserved for the ATC surveillance system, whereas WAM will be referred to as a 'sub-system'.

controller and their possible consequences and is based on the OSED. The PSSA examines possible failure modes of the example WAM sub-system.

- From the FHA and PSSA, example safety requirements are identified that would need to be implemented for the example WAM sub-system to be considered 'safe' in the defined environment.

This document is structured according to the safety argument found in Section 2 (i.e. each main sub-argument is addressed in a new section of this document). Most of the document is intended to be re-used in ANSPs' own safety cases (modified and updated as necessary to reflect the local situation). In particular the applicable sections are the:

- safety argument, (Section 2)
- generic OSED, (Section 3 and Annex E)
- behaviour in normal operations – the "success case", (Section 4)
- example WAM sub-system, (Section 5.2 and Annex K)
- generic FHA, (Section 5.3 and Annex H)
- example PSSA (Section 5.4 and Annex L) and,
- example safety requirements (Annex M).

The document consists of two volumes, the first of which is the main document, including Annexes: A, Acronyms; B, Glossary and Definitions, C, References and D, Explanation of the Goal Structured Notation (GSN) used for the Safety Argument. The second volume contains the remainder of the Annexes.

The preparation of the assessment and its review has identified a number of **considerations** that are worth highlighting here:

- The assessment assumes that the controller procedures are identical when using WAM as a surveillance sensor compared to radar. If the procedures deviate significantly in the local environment, then the OSED will need to be modified.
- Although operationally WAM 'looks' similar to SSR, it is technically very different. For example there is a need to plan WAM coverage and it will be highly dependent on the relative positions of the WAM receivers. Surveillance performance quality for WAM varies in a very different manner to that of radar. Careful validation of the WAM coverage is therefore required to ensure that it is as good as radar in the volume of airspace where an operational service is provided.
- Moderate to high-density en-route and TMA airspace is assumed in the generic analysis. If WAM is implemented in lower traffic density airspace, a lower safety objective may be derived to reflect the reduced risk in that airspace.

The **conclusions** of the study are as follows:

- The analyses described within this document demonstrate that the use of Wide Area Multilateration for ATC surveillance is safe in principle.

- The Safety Assessment Methodology and Safety Case Development Methodology have led to the derivation of realistic and achievable Safety Requirements for WAM sensor implementation.

- A WAM sole means surveillance sensor can meet the Safety Objectives to support ATC services, incorporating vectoring, monitoring and separation provision, in a high-density traffic environment. Even a minimal WAM sensor can meet most of the safety objectives. By adding redundancy, all safety objectives can be met.

- Implementers should note that this study has been performed for the high-density traffic environment. Local environments with lower traffic densities may require less stringent Safety Requirements placed upon the surveillance system (in order to meet the same Target Level of Safety).

- The fact that WAM sub-systems are used operationally by at least two ANSPs in ECAC demonstrates that WAM sub-systems for ATC surveillance can be safe in practice.

- In addition to these conclusions on the WAM surveillance subsystem, it should be noted that, as for all cooperative surveillance techniques, there is dependence on the transponder. Although airborne equipment and pilot procedures are assumed to be unchanged, the airborne transponder is identified as a relatively weak link in the safety assessment of the overall surveillance system because it can be very hard to mitigate against problems in the transponder by capabilities in the ground system.

1. INTRODUCTION

1.1 General

This document is a generic Wide Area Multilateration (WAM) surveillance safety assessment. It has been developed to assist ANSPs that wish to introduce WAM. These ANSPs will have to prepare a Safety Case for the introduction of WAM and this document may contribute by helping to structure the safety argument and providing material that ANSPs can re-use (after tailoring to their local environment) to develop their own safety cases. It will also help to ensure a consistent approach to the development of WAM safety cases in Europe.

The distinction between a safety assessment (this document) and a safety case (to be developed by an ANSP and approved by a Regulator before the service and/or equipment are used operationally) must be clearly understood.

A safety assessment looks at hazards, their effects and mitigations to the effects and makes reasonable **assumptions** about the behaviour of system elements (such as their likely reliability, accuracy or failure rates) so as to be able to **assess** quantitatively the likelihood of hazards resulting in incidents or accidents.

A safety case, in addition to the work of an assessment, gathers **evidence to demonstrate that the assumptions are valid in a real life situation**.

The difference is primarily the degree to which valid appropriate evidence is available. Note that the value of post-implementation safety monitoring, although beyond the scope of the current document, is to further validate the evidence that used for the safety case.

1.2 Background

Multilateration based surveillance sub-systems are increasingly being installed for the provision of an ATC (vectoring, monitoring and separation) service over wide areas (including both en-route and terminal airspace) as a replacement for and/or complement to existing surveillance techniques such as SSR, PSR and ADS-B.

The driver for the adoption of this cooperative independent surveillance technology is based upon the combined potential economic, efficiency and safety benefits it can offer inside a defined volume of airspace. Safety benefits are brought if WAM is installed to provide ATC surveillance in current non-radar airspace; economic benefits may be brought by eventual replacement of current radar surveillance by WAM; and efficiency benefits by improvement of surveillance coverage at a lower cost than extension of radar surveillance. The airspace volume in which coverage is required can be flexibly shaped according to the location of WAM ground sensors and can be easily extended to meet operational needs by installing additional ground sensors.

WAM offers high quality surveillance without requiring additional aircraft equipage, as it can make use of signals from existing Mode A/C and Mode S transponders. Further, a WAM ground sub-system is relatively inexpensive to maintain (compared to a conventional SSR sub-system) because it involves few, if any, moving parts.

For these reasons initial WAM implementation is already under way. As adoption of this technology becomes increasingly widespread, EUROCONTROL has undertaken this safety assessment in its capacity to provide safety support (in accordance with ESARR 4 [1]) and to avoid duplication of service provider effort in developing individual *ab initio* safety cases,

Therefore, this document is designed to act as a starting point and provide an initial way forward for ANSPs conducting a safety case for the implementation of WAM in their local area. This assessment is also intended to show that this application of WAM is safe in principle.

1.3 Relationship to the local safety case

The purpose of a safety case is to enable system implementers to assure themselves and their regulators that a system being assessed will deliver an acceptable level of safety throughout its lifetime. This is done through documented logical arguments and the provision of supporting evidence.

This safety assessment considers a generic ATC service and an example WAM sub-system. The specific issues for a particular application in a specific area must be considered through a local Safety Case. **This document DOES NOT take the place of a local Safety Case**.

1.4 Contents

The document provides:

- A high-level safety argument that ANSPs can re-use in their own safety cases; the remainder of the document is structured according to this safety argument, with each new section addressing a new sub-argument;
- A generic Operational Services and Environment Description (OSED) which ANSPs can tailor to their local conditions;
- A functional model of an example minimal WAM sub-system;
- A justification that the WAM concept is safe in principle, which is itself based on two arguments:
    1. A justification that when operating according to specification (the ‘success case’) WAM performance can meet or exceed the performance of conventional Monopulse Secondary Surveillance Radar (MSSR), known as the ‘reference sub-system’.
    2. An analysis to ensure that the safety risks in the example WAM sub-system operating in the generic OSED are understood and acceptable (the ‘failure case’). This includes a generic Functional Hazard Analysis (FHA) and an example Preliminary System Safety Assessment (PSSA) of the example WAM sub-system. Both FHA and PSSA can be re-used as the basis for the specific FHA or PSSA that may be developed by ANSPs implementing their own WAM sub-systems.
- Guidance on how to satisfy the rest of the safety argument.

- A summary of assumptions and example Safety Requirements.

1.5 Scope

Key points in the selection of the scope of this assessment are:

- The application considered is an ATC (vectoring, monitoring and separation) service because this reflects the most likely use of WAM as an alternative to SSR.
- High-density en-route and TMA airspace is assumed, on the basis that it should lead to the most stringent safety and performance requirements. It is recognised that a different environment (with for example lower traffic density figures) may lead to alternative Safety Objectives and resultant Safety Requirements. The local Implementer should address this in the local Safety Case as necessary.
- This assessment looks at the provision of ATC surveillance using solely Wide Area Multilateration (i.e. WAM sole means) as this should lead to the most stringent system requirements. If other surveillance techniques are implemented alongside WAM (for a particular coverage volume), they must be taken account of in the local Safety Case.
- The assessment has also looked at some possible combined architectures (e.g. WAM + SSR), in order to ensure feasibility of combining these surveillance techniques. The sections in the document describing alternative architectures are given at the ends of Annexes E, K and L.
- The end-to-end system is being assessed, from the aircraft transponder to the controller working position (CWP), which is where the operational hazards are evaluated. The comparative element of the assessment, which is key to the success case, is however confined to the differences between the radar surveillance sensor or sub-system and the WAM surveillance sub-system. This is shown in Figure 1 below. (Note however that a more detailed system description is needed for the PSSA part of this analysis.)

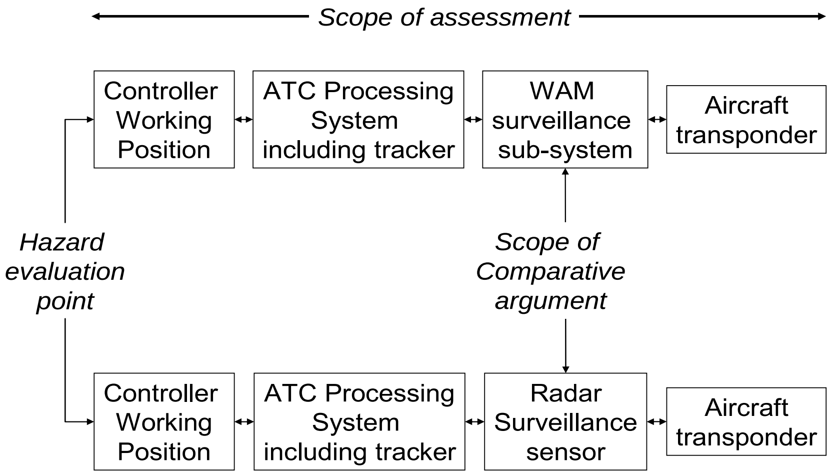

Scope of assessment
Controller Working Position
ATC Processing System including tracker
WAM surveillance sub-system
Aircraft transponder
Hazard evaluation point
Scope of Comparative argument
Controller Working Position
ATC Processing System including tracker
Radar Surveillance sensor
Aircraft transponder

Figure 1: Assessment scope

Issues associated with a specific ANSP operation or implementation are outside the scope of this safety assessment (but are included in the safety argument), such as:

- The local environment and operations where the WAM sub-system is implemented.
- Specific risks associated with the transition and implementation phases of the introduction of a WAM sub-system.
- Validation of all assumptions and safety requirements in specific locations.

These issues must be considered in the local safety case.

Note that the assumptions contained in this assessment (and gathered together in Annex F), when reused by the local safety case, will become Safety Requirements since the availabilities determined in the local safety case are dependent upon the assumptions used.

1.6 Relationship to EUROCONTROL SAM and SCDM

The methodology used within this safety assessment is based on the EUROCONTROL Safety Assessment Methodology (SAM) [2] and Safety Case Development Manual (SCDM) [3]. It is assumed that the reader is familiar with this material which describes the development of:

- A Safety Argument. This is a framework to which other elements of the safety assessment relate. It provides a logical argument that the system considered will be safe if certain assumptions are met and evidence is documented.
- An Operational Service and Environment Description (OSED). An example OSED is provided here for a generic environment.
- A Functional Hazard Assessment (FHA). An example FHA is provided here for the ATC (vectoring, monitoring and separation) service in the generic environment.
- A Preliminary System Safety Analysis (PSSA). An example PSSA is provided here for the assessed minimal WAM sub-system. The PSSA, however, does not provide quantitative Safety Requirements for each element of the WAM sub-system. This is because the allocation of requirements to individual components may be different by different manufacturers and this document does not wish to constrain them.
- A System Safety Analysis (SSA). A SSA is not provided here because it is implementation specific.

The document also follows the principles of Eurocae ED-125 “Guidance on Risk Assessments” [4]. (At the time of writing, this is still a draft document.)

1.7 Document Structure.

The document consists of two volumes.

Volume 1 contains the Safety Argument (Section 2) the structure of which guides the structure of the document as a whole; together with a summarised OSED (Section 3); a description of the “Success Case” (Section 4); and “Failure Case” (Section 5) as well as the specific elements of the overall Argument that are the responsibility of the local implementer. Some guidance to implementers, to assist the creation of their local safety case, is included (Section 6).

The summary, highlighting the main elements of the safety assessment approach; the conclusions, that WAM sub-systems can be designed installed and operated to provide a safe means of ATC surveillance; and the recommendations for the local safety case process close the main part of the document (Section 7).

Volume 1 is completed with those Annexes necessary to fully understand its content, namely: Annex A, Acronyms; Annex B, Glossary and Definitions, Annex C, References and Annex D, Explanation of the Goal Structured Notation (GSN) used for the Safety Argument.

Volume 2 contains the remainder of the Annexes, which consist of detailed material, amplifying and supporting the sections of the main document. These are Annex E, OSED; Annex F, Assumptions and Conditions; Annex G, Failure Case; Annex H, Functional Hazard Assessment; Annex I, Severity Classification Tables; Annex J, Severity Classification Scheme; Annex K, Example Functional Models; Annex L, Example PSSA; Annex M, Example Safety Requirements and Annex N, General Guidance to Implementers.

At the start of Volume 2, there is a detailed introduction explaining the role of each Annex in the overall development of this example safety assessment.

1.8 Comments on the overall Safety Assessment process.

Hazard severity and technical requirements.

It must be recognised that the whole process, although quantified as far as possible (because system developers need quantified requirements against which to work) still contains a significant element of subjectivity. A very visible outcome of the process is the severity assigned to particular hazards. It can be thought that a system with severity 1 hazards is inherently “bad”. To draw such a conclusion is to misunderstand the process; the severity is just the starting point for consideration of the hazard in its context. What matters more, certainly for WAM system developers, is the requirement in its technical and operational context that is placed on the WAM sub-system and whether that can be met by the system as developed and installed.

Use of Severity 1 in the analysis.

In this study, the initial assessment was that certain position related hazards should be assigned severity 1. The quantification of safety objectives related to these hazards in Volume 2 was initially worked out from the starting point of severity 1. Further internal review led to a decision to change this. Section 5.3.1 explains the rationale. However, in order to cater for the possibility that ANSPs’ own hazard assessments might be more cautious and assign severity 1 to some hazards, the safety objective values related to severity 1 were retained for comparison purposes. The Fault Tree Analysis shows, in fact, that these more stringent values can also be met by WAM surveillance.

2. SAFETY ARGUMENT

2.1 Introduction

The purpose of a safety argument is to provide the structured logic that a system, process or procedure is acceptably safe, subject to the provision of evidence detailed in the argument.

The system implementer (assumed to be the ANSP) must prove to its own satisfaction that the safety argument, if followed correctly and completely, will result in an acceptably safe system.

The regulator has the responsibility of declaring that the safety case, developed by following the logic of the safety argument, is adequate for the purposes of demonstrating the safety level of the overall ATM system.

This safety argument is developed from the point of view of this generic safety assessment – i.e. it includes the responsibilities of EUROCONTROL as well as ANSPs and other actors in the system.

An explanation of the Goal Structured Notation (GSN) used in the following figures can be found in Annex D. Argument boxes in green are satisfied by EUROCONTROL through this document. Argument boxes in pink must be satisfied by the ANSP.

2.2 High-level Safety Argument

Figure 2 shows the high-level safety argument. The central premise is that “providing an ATC separation service in en-route and TMA airspace using WAM derived data is acceptably safe” (Argument 0).

A key part of the safety argument is to define “acceptably safe”. Criteria **[Cr001]** defines this as the risk of an accident / incident being:

- No greater than for the reference sub-system. The reference sub-system is the Monopulse Secondary Surveillance Radar (MSSR).
- Within the relevant Target Level of Safety (TLS). The TLS is defined by ESARR 4 [1] as explained in Annex N.4.2.
- Further reduced as far as reasonably practicable (AFARP). This is achieved by conducting a local FHA, PSSA and SSA in addition to performing a concluding “sanity check” that all operating procedures guarantee safety. It is the responsibility of the local system implementer to ensure that this requirement is considered.

Justification for this work is also provided within the context of Argument 0 **[J001]** and this provides an indicator for the motivation for this work – that WAM is being introduced in en-route or TMA airspace to meet economic and/or capacity and/or safety needs. In addition two assumptions are made regarding this high level argument, firstly that the reference sub-system is acceptably safe **[A001]** and secondly that guidance is available to those implementing the WAM sub-system **[A002].** These assumptions are addressed in sections 4.3 and 6, and Annex N, of this document.

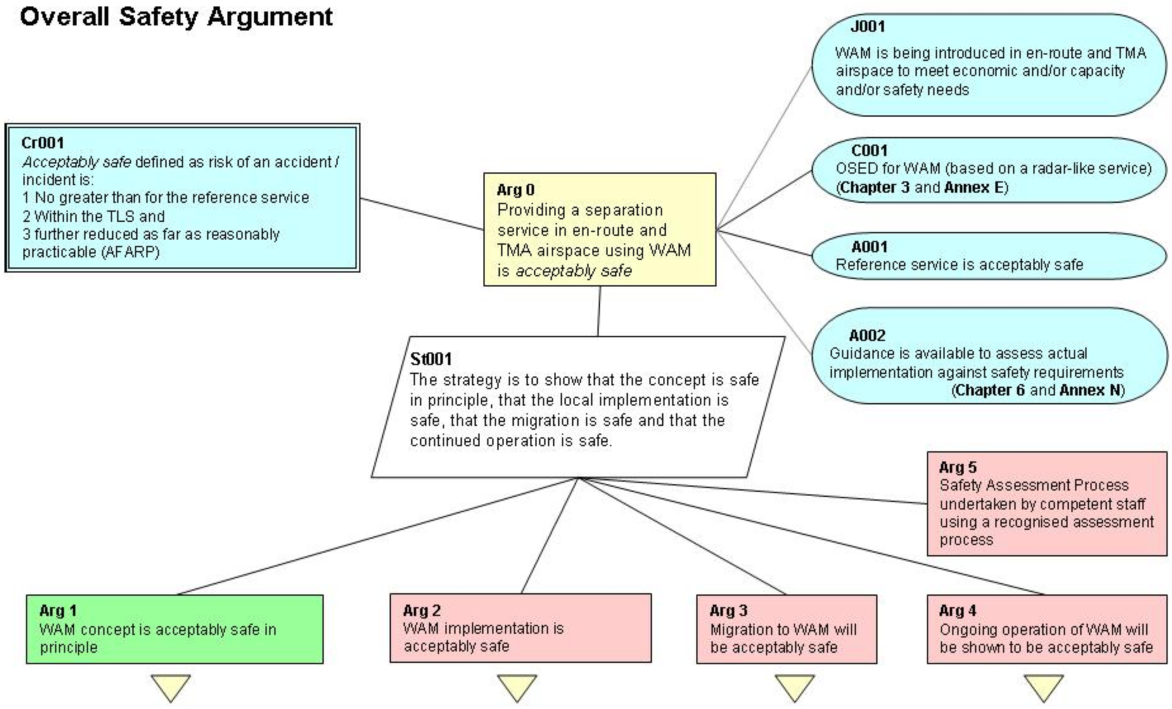

Overall Safety Argument
Cr001
Acceptably safe defined as risk of an accident / incident is:
1 No greater than for the reference service
2 Within the TLS and
3 further reduced as far as reasonably practicable (AFARP)
Arg 0
Providing a separation service in en-route and TMA airspace using WAM is acceptably safe
J001
WAM is being introduced in en-route and TMA airspace to meet economic and/or capacity and/or safety needs
C001
OSED for WAM (based on a radar-like service) (Chapter 3 and Annex E)
A001
Reference service is acceptably safe
A002
Guidance is available to assess actual implementation against safety requirements (Chapter 6 and Annex N)
St001
The strategy is to show that the concept is safe in principle, that the local implementation is safe, that the migration is safe and that the continued operation is safe.
Arg 5
Safety Assessment Process undertaken by competent staff using a recognised assessment process
Arg 1
WAM concept is acceptably safe in principle
Arg 2
WAM implementation is acceptably safe
Arg 3
Migration to WAM will be acceptably safe
Arg 4
Ongoing operation of WAM will be shown to be acceptably safe

Figure 2: Overall safety argument

The strategy for Argument 0 is:

- To show that the WAM concept is acceptably safe in principle [Arg 1]. This has been undertaken by EUROCONTROL in this document.
- To show that the implementation of WAM is acceptably safe [Arg 2]. This is undertaken by the ANSP based on specific information about their local environment and equipment.
- To show that the migration to WAM will be acceptably safe [Arg 3]. This is undertaken by the ANSP and requires planning for the migration to the new WAM service.
- To show the ongoing operation of WAM will be shown to be acceptably safe [Arg 4]. This is undertaken by the ANSP and requires in-service monitoring of incidents and corrective action to be undertaken.
- To show that the safety assessment process was undertaken by competent staff **[Arg 5]**.

Thus argument 1 provides a theoretical *in principle* starting point for arguments 2-5 which, taken together, demonstrate that WAM is acceptably safe *in practice*.

Each argument is further decomposed into sub-arguments indicating appropriate evidence. Subsequent Sections and Appendices of this document substantiate this evidence.

2.3 Argument 1

This argument (Figure 3) is that the WAM concept is acceptably safe *in principle*. "In principle" means that an example WAM system should be acceptably safe when used in the conditions described by the generic OSED. In other words:

- An "example WAM sub-system" is defined. From knowledge of manufacturer systems, it is known that this is similar to some commercial systems. The example WAM sub-system is defined at a functional level only.
- A "generic OSED" is defined. This is a description of the ATC service provided and the environment, such as traffic density. It is generic because local procedures and environment may differ slightly.
- The example WAM sub-system is analysed to show that it can be acceptably safe in this environment providing that it meets a set of defined safety requirements.

The final bullet is satisfied using two analyses:

- A justification that WAM performance can meet or exceed the performance of a 'reference sub-system' (i.e. MSSR) when WAM is working correctly (the 'success case').
- An analysis that the safety risks in the example WAM sub-system operating in the generic OSED do not exceed the TLS when a failure occurs (the 'failure case'). This includes a functional hazard analysis (FHA) and a Preliminary System Safety Assessment (PSSA) of the example WAM sub-system. (It should be noted that in compiling these aspects of a safety case, the entire surveillance system should be considered - i.e. WAM + unchanged elements from the rest of the surveillance system, such as CWP, SDPD).

Evidence that these analyses have been satisfied relies upon gathering

- Direct evidence: generic system design is shown to be acceptably safe (meeting the TLS stipulated by the regulator) e.g. a given accuracy or integrity is met within specified error limits.
- Indirect evidence: That the proper process is followed and is trustworthy, (using accepted standards and competent people). The evidence for this is collected in Argument 5.

Additionally it is the responsibility of the service providers that use this argument to review it to ensure that this generic case/implementation captures all the facets of their local case.

Figure 3 shows how Argument 1 is decomposed and satisfied by evidence given in this and other documents. Argument 1.2 shows the success case, whilst Argument 1.3 outlines the failure case. Section 4, "Normal Operations (Success Case)" explains Arguments 1.1 and 1.2 in more detail. Section 5 "Abnormal Operations (Failure Case)" explains Argument 1.3.

The evidence bubbles shown in the Figure refer to various Annexes within this document. A summary of the applicable evidence is also given in the relevant main section of the report; e.g. for Argument 1.1, evidence for the argument that "the WAM operational service and airborne equipment are the same as for the reference service" is summarised in section 3.1, 3.2 and 3.3 below.

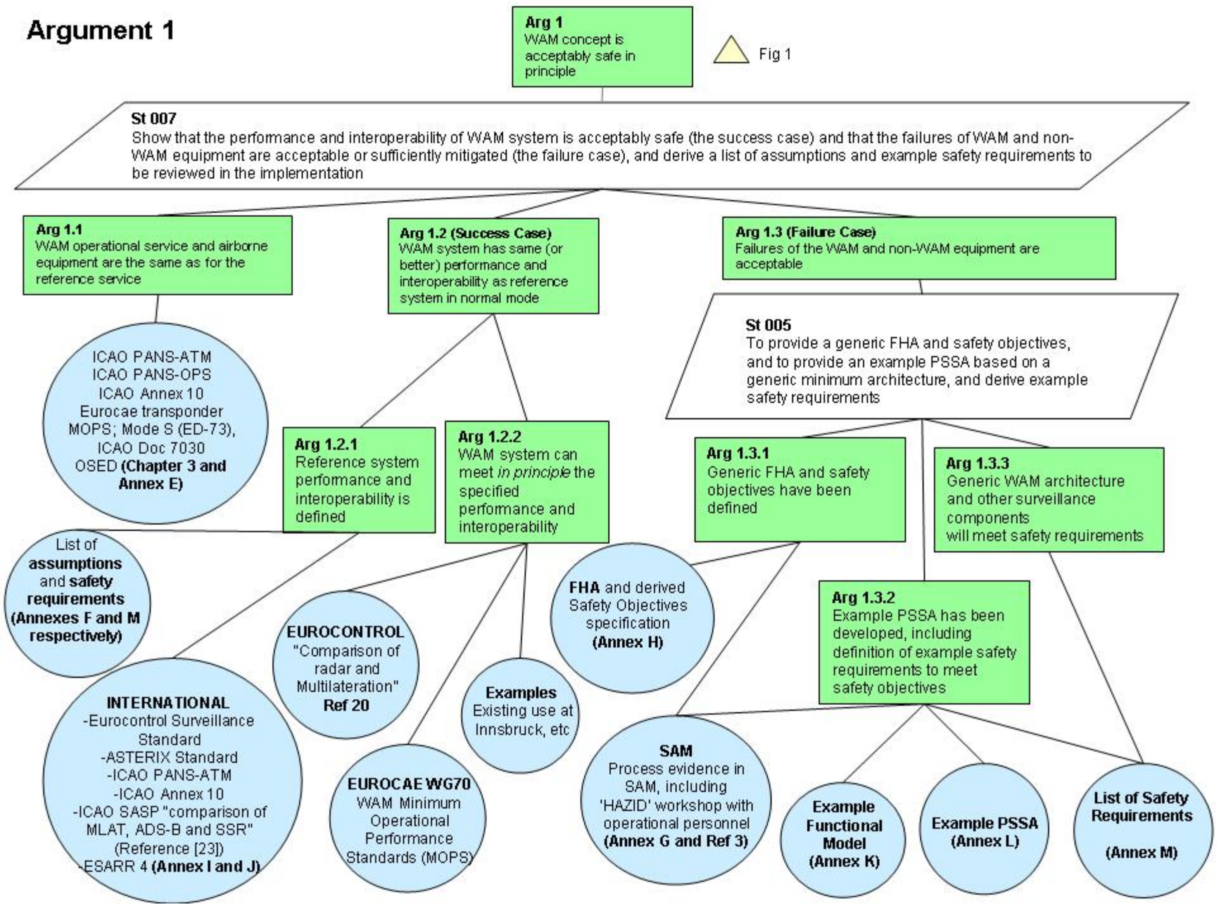

Argument 1
Arg 1
WAM concept is acceptably safe in principle
Fig 1
St 007
Show that the performance and interoperability of WAM system is acceptably safe (the success case) and that the failures of WAM and non-WAM equipment are acceptable or sufficiently mitigated (the failure case), and derive a list of assumptions and example safety requirements to be reviewed in the implementation
Arg 1.1
WAM operational service and airborne equipment are the same as for the reference service
Arg 1.2 (Success Case)
WAM system has same (or better) performance and interoperability as reference system in normal mode
Arg 1.3 (Failure Case)
Failures of the WAM and non-WAM equipment are acceptable
ICAO PANS-ATM
ICAO PANS-OPS
ICAO Annex 10
Eurocae transponder MOPS; Mode S (ED-73),
ICAO Doc 7030
OSED (Chapter 3 and Annex E)
St 005
To provide a generic FHA and safety objectives, and to provide an example PSSA based on a generic minimum architecture, and derive example safety requirements
Arg 1.2.1
Reference system performance and interoperability is defined
Arg 1.2.2
WAM system can meet in principle the specified performance and interoperability
Arg 1.3.1
Generic FHA and safety objectives have been defined
Arg 1.3.3
Generic WAM architecture and other surveillance components will meet safety requirements
List of assumptions and safety requirements (Annexes F and M respectively)
FHA and derived Safety Objectives specification (Annex H)
Arg 1.3.2
Example PSSA has been developed, including definition of example safety requirements to meet safety objectives
EUROCONTROL
"Comparison of radar and Multilateration"
Ref 20
Examples
Existing use at Innsbruck, etc
INTERNATIONAL
-Eurocontrol Surveillance Standard
-ASTERIX Standard
-ICAO PANS-ATM
-ICAO Annex 10
-ICAO SASP "comparison of MLAT, ADS-B and SSR" (Reference [23])
-ESARR 4 (Annex I and J)
EUROCAE WG70
WAM Minimum Operational Performance Standards (MOPS)
SAM
Process evidence in SAM, including 'HAZID' workshop with operational personnel (Annex G and Ref 3)
Example Functional Model (Annex K)
Example PSSA (Annex L)
List of Safety Requirements (Annex M)

Figure 3: Argument 1

2.4 Arguments 2, 3, 4 and 5

Arguments 2, 3, 4 and 5 must be satisfied by the ANSP and this document only gives guidance on how to achieve this (Section 6). Whereas Argument 1 is satisfied by EUROCONTROL (subject to validation by the ANSP) and establishes that the WAM concept is acceptably safe **in principle**, Arguments 2, 3 and 4 are concerned with the ANSP showing that the implementation of the WAM concept is acceptably safe **in practice**. Argument 5 depends on the ANSP activities being carried out competently and correctly using a recognised process.

Arguments 2, 3 and 4 relate to the implementation, introduction and ongoing operation of the WAM sub-system. Therefore knowledge is required of the specific WAM sub-system to be introduced and the local environment.

It is the responsibility of the service provider, in consultation with their regulator, to define the meaning of what can be considered ‘acceptably safe’ *in practice* and then for the service provider to demonstrate to its regulator that its service meets this definition. The implementer should also check that risks are reduced ‘As Far As Reasonably Practical’ which is a final check that all reasonable safety measures have been undertaken.

This might be accomplished by defining a particular set of safety requirements (which may have evolved from the requirements of a generic case to that of a specific implementation) and then showing that they have been met.

2.4.1 Argument 2

Argument 2 explains why an implementation of Argument 1 in a particular local case is acceptably safe in practice. This argument rests upon factors in the local environment into which a WAM sub-system is placed, in addition to its specific design, implementation and operation. The fulfilment of such an argument will be satisfied in part by the capability to safely revert to the previous surveillance sub-system (or operation, in the case of WAM surveillance introduced where there was previously no surveillance) until a time when sufficient confidence in the operation of the WAM sub-system has been adequately demonstrated and therefore such redundancy is no longer required.

2.4.2 Argument 3

Argument 3 outlines the reasons why the migration to WAM is acceptably safe, according to a strategy that identifies risks and formulates a plan that mitigates them. This plan should be structured in terms of a system architecture that allows both migration and reversion - one that bridges the gap between an operationally untried new sub-system and the previous platform that was known and trusted (i.e. has been shown to be safe from years of experience). Features of this argument could include outlining:

- A decommissioning process: e.g. that a previous surveillance sub-system will be decommissioned (taken off standby) only when it has been shown that the new sub-system provides the surveillance performance required by the service provider and their regulator.

- A review of procedures/training to prepare controllers for any changes deemed necessary in the Controller Working Position (e.g. a new update rate) and the procedures to go through if reversion to the original surveillance sub-system or procedural control is required (e.g. in the event of SDPD failure).

2.4.3 Argument 4

Argument 4 sets out the case for ongoing WAM operation to be acceptably safe. It can be satisfied by implementing standard in-service monitoring procedures of incidents and performance provided that they are followed up by appropriate corrective actions. Such a monitoring system may already be in place as part of the ANSP’s Safety Management System (SMS).

Within argument 4, emphasis is placed upon the value of sharing performance analysis and reporting activities within the WAM community. Although not a formal Safety Requirement, fostering such an atmosphere of collaboration will ultimately be to the benefit of all users because it will provide a large resource of WAM sub-system performance data (from which each user can assess the performance of their own sub-system by comparing error behaviour and using statistical analysis techniques).

2.4.4 Argument 5

The evidence that the Safety Assessment has been undertaken by competent staff using a recognised assessment process is the essence of Argument 5. The assessment process here is based on the EUROCONTROL Safety Assessment Methodology [2] and the Safety Case Development Manual [3]. The evidence that it is being followed correctly and completely is contained

- within this assessment, with each section covered in appropriate detail and highlighting reasonable and accurate findings
- within the local Safety Case, where the ANSP follows the same process, based upon this generic safety assessment, but tailored to the local environment and carried out by suitably skilled experts.

The sub-arguments for Arguments 2, 3, and 4 are shown below. Some guidance on how to satisfy these arguments is given in Section 6 'Guidance to Implementers'.

Argument 2 - Implementation

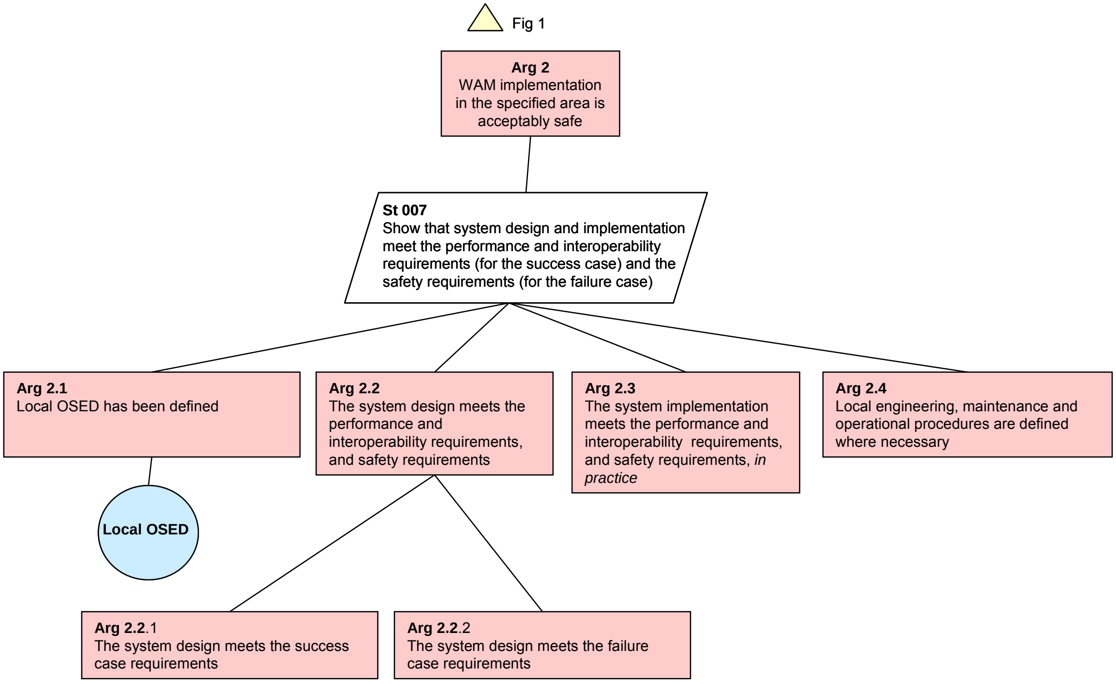


Fig 1
Arg 2 WAM implementation in the specified area is acceptably safe
St 007 Show that system design and implementation meet the performance and interoperability requirements (for the success case) and the safety requirements (for the failure case)
Arg 2.1 Local OSED has been defined
Arg 2.2 The system design meets the performance and interoperability requirements, and safety requirements
Arg 2.3 The system implementation meets the performance and interoperability requirements, and safety requirements, *in practice*
Arg 2.4 Local engineering, maintenance and operational procedures are defined where necessary
Local OSED
Arg 2.2.1 The system design meets the success case requirements
Arg 2.2.2 The system design meets the failure case requirements

Figure 4: Argument 2

Argument 3 - Migration

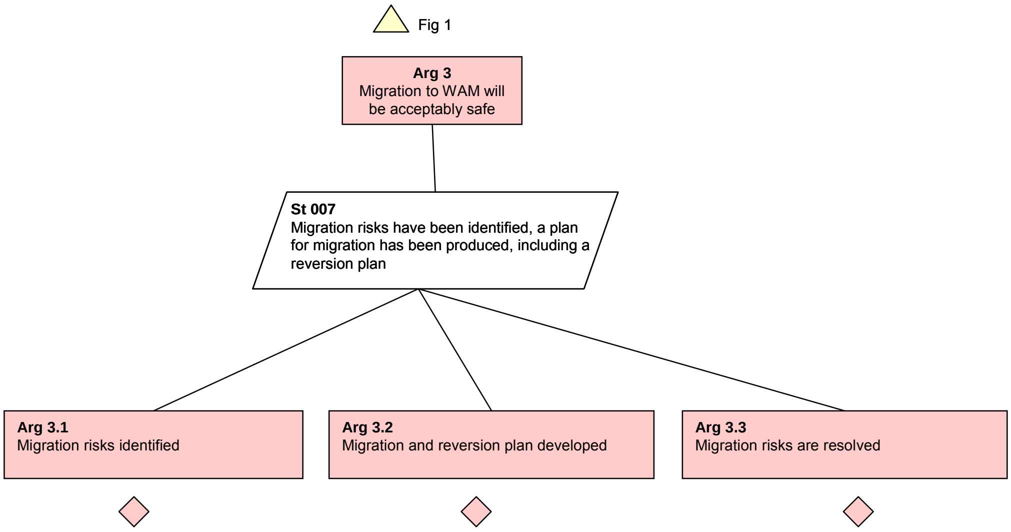


Fig 1
Arg 3
Migration to WAM will be acceptably safe
St 007
Migration risks have been identified, a plan for migration has been produced, including a reversion plan
Arg 3.1
Migration risks identified
Arg 3.2
Migration and reversion plan developed
Arg 3.3
Migration risks are resolved

Figure 5: Argument 3

Argument 4 - Ongoing operation

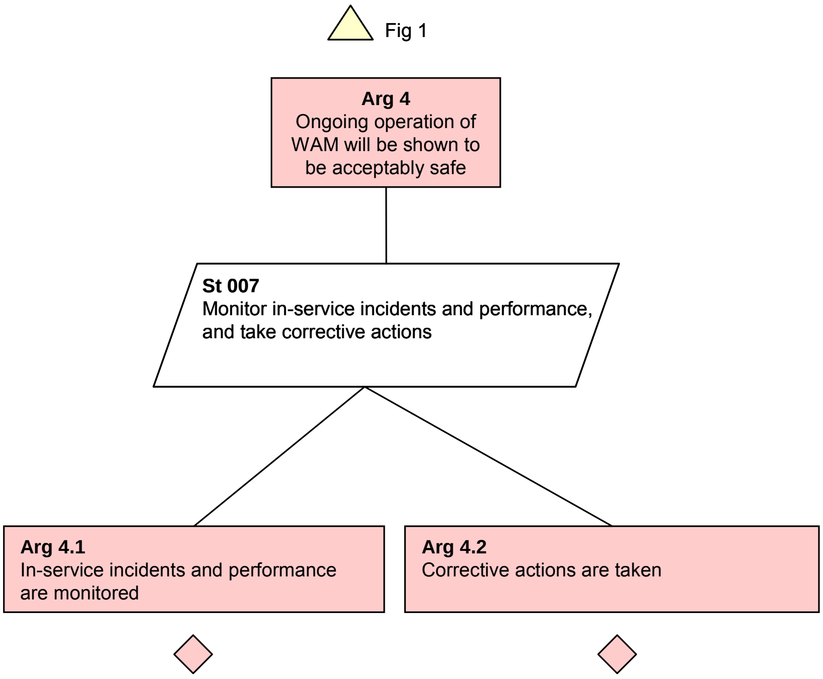


Fig 1
Arg 4
Ongoing operation of WAM will be shown to be acceptably safe
St 007
Monitor in-service incidents and performance, and take corrective actions
Arg 4.1
In-service incidents and performance are monitored
Arg 4.2
Corrective actions are taken

Figure 6: Argument 4

3. APPLICATION AND ENVIRONMENT DESCRIPTION

3.1 Background

This section summarises the application (i.e. provision of an ATC service incorporating vectoring, monitoring and separation) and the generic environment upon which the analysis was carried out. It describes at a high level the actors, procedures and functions necessary to carry out the application.

Both the operational application description and the environment description are drawn from ICAO documentation such as PANS-ATM [5] and PANS-OPS [6]. Detailed references to the relevant sections of these documents are given.

The full application and environment description is given in Annex E. The assumptions made in the OSED (and in the rest of the document) are summarised in Annex F.

This section (and the related Annex) fulfils the provision of evidence required under Argument 1.1 (shown in Figure 3 in section 2.3 above).

3.2 Application Description

3.2.1 Overview

The primary application under consideration in this safety assessment is the “ATC service, focusing on the provision of separation, using surveillance data.” This is chosen because the separation task is assumed to generate the most severe requirements on the system and human [ASSUMP01].

The ATCO operating procedures are intended to be technology independent. Therefore, the source of the surveillance data should not be a factor at the operational level [ASSUMP02].

The ATC service under consideration is detailed further in PANS-ATM [5], and includes:

- Separation (§ 8.7);
- Vectoring (§ 8.6.5); and
- Monitoring (§3.2.5).

Position information is gathered from presented surveillance information, with route information gathered through correlation with the flight plan.

The ICAO standard separation minima are assumed, with 3NM or 5NM laterally (2.5NM under certain conditions), and Reduced Vertical Separation Minima at 1000 ft vertically *(Sections 8.7.2, 8.7.3 and 8.7.4 of PANS-ATM).*

The following information elements are required from the surveillance sub-system for the provision of the ATC service:

- Horizontal (2D) position;

- Vertical position (barometric pressure altitude via Mode C) – for the controller, this will continue to be displayed in 100ft increments;
- Aircraft identity (ICAO aircraft call sign or Mode 3/A code and Special Position Indicator, SPI);
- Short Intent and Track History (derived by ground processing).

Additionally, flight status is defined in ICAO Annex 10 (Vol IV, Chapter 3), although it is not considered in the scope of this study.

Although a mandate for Mode S exists in core area Europe, it has not been assumed that Mode S transponders will be available and equipped for all aircraft operating in the en-route and TMA environment under discussion in this safety case. It is therefore assumed that the capabilities arising from Mode A/C surveillance is the minimum (baseline) level of surveillance capability available to the controller [ASSUMP03].

As per the scope of this study, if this assumption is used to establish the local Safety Case, it will become a Safety Requirement, because we rely upon the capability of the transponder as part of the safety analysis. Unique failures arising from Mode S transponder operation will need to be accounted for in the fault tree analysis. [Note that the technical analysis in the example PSSA in Annex L assumes 90% Mode S, 10% Mode A/C aircraft in the environment – measured figures for the local environment should be used in the local Safety Case.]

The roles and responsibilities of the controller and pilot will remain unchanged [ASSUMP02] from the current surveillance services provided to maintain a separation service under PANS-OPS [2] (parts 2-11 in Volume 1, parts 2-6 in volume 2).

Controller procedures for performance checks on the WAM surveillance data will be required (in particular barometric altitude verification procedures), in the same way to those specified for SSR surveillance (additional detail is provided in § 8.6.1 of PANS-ATM [1]).

Current procedures also apply in the event of an aircraft reporting an emergency situation. The control of aircraft in a state of emergency is covered in sections 9.2.1, 11.4.1 and 15.1.2 of PANS-ATM [1].

Any changes to ATCO procedures (regardless of the surveillance sub-system implementation and/or operational maturity at the time they are introduced) must first be designed and then validated (e.g. using simulation or flight trials) within a specified coverage volume [ASSUMP06, see also ASSUMP17].

Annex E.2 lists the range of services provided by ATC in en-route and TMA airspace. This list was compiled to help ensure no data items have been omitted by focusing on the separation task as part of the provision of an ATC service.

3.2.2 Fallback Modes

A critical characteristic of the operational description used in this safety assessment is the method of fallback used in case of loss of surveillance data.

In general, the fallback modes used in this safety assessment conform to those used in current ATC radar-based surveillance. It is therefore assumed that any equipment failure or service degradation (including for individual aircraft) must be recognised in the same time frame as for radar equipment failures today, so that reversion to the appropriate fallback mode can be achieved safely [ASSUMP04].

These fallback modes may include:

- Extrapolating the last “good quality” position data for a limited period or;
- Removing the degraded data from the display and moving to procedural control.

An issue was identified during this safety assessment of the ability of the controller to manage a high density traffic scenario if data on aircraft was lost. Therefore, the following conditions[2] were agreed:

- FHA14 – the controller is able to safely revert to procedural separation (for the affected aircraft) in the case of a continuous loss of all data for one aircraft;
- FHA15 – the controller is not able to safely revert to procedural separation in the case of a sudden continuous loss of all data for all aircraft (in the high density environment). However, in the case of loss of altitude data for all aircraft, it is assumed that controller may safely revert to procedural and 2D separation.
- Note that the “more than one” aircraft case is included in the consideration of hazards affecting “all aircraft” (as the worst cases will be similar).

3.3 Environment Description

The safety argument defines the operating environment under consideration as being the same as provided by radar according to PANS-ATM [5] §8 Surveillance Services, i.e. vectoring, monitoring and separation.

This generic safety assessment attempts to define an environment with enough detail to enable an adequate assessment to be conducted (i.e. such that effects of hazards can be clearly identified), without over-prescribing the environment in such a way as to unnecessarily restrict implementation options, impose excessive requirements, or make the analysis insufficiently widely applicable.

This section summarises the key characteristics, with more detail provided in Annex E.3.

The surveillance coverage and performances shall be in accordance with the EUROCONTROL Standard for Radar Surveillance in en-route and major Terminal Areas[7]. This Standard defines the required surveillance coverage in both Terminal Area and en-route airspace; it specifies that both areas must be covered by duplicated SSR, with PSR coverage also required in Terminal Areas. The coverage must be structured in order to provide continuity and availability of the surveillance service for the provision of a separation service across all airspace divisions (and remain in accordance with local requirements); including between en-route and Terminal areas (note that this may be difficult in the WAM

[2] Note that these are not formal assumptions, but rather form part of the hazard analysis and assessment. It was felt important to highlight them as part of the operational description. They must be validated with local controllers for the local Safety Case.

sole means scenario; in reality however, with multiple surveillance sources, continuity of surveillance performance should be the goal).

This safety assessment focuses on the likely environment within which WAM will provide data for the operational applications defined. Given the growth characteristics of the high density core-area European environment, the traffic densities currently managed are likely to increase in the future. Thus a "target environment" concept is used.

Key environmental characteristics include:

- All airspace classifications. It is assumed that for airspaces with mixed VFR and IFR traffic, current roles and operational procedures apply. Thus transponder equipage will be mandatory in the target environment where transponders are mandatory today for SSR and/or ADS-B surveillance [ASSUMP07] (section 8.5 of PANS-ATM).
- Flexible Use of Airspace: same requirement as for current SSR environment (as defined in sections 3.1.5 and 8.6.5 of PANS-ATM).
- Airspace structure and complexity: same requirement as for current SSR environment (as defined in sections 2.6.2, 8.6.5 and 10.4.1 of PANS-ATM).
- Route configuration and complexity: same requirement as for current SSR environment (as defined in sections 8.9, 8.10 and 8.11 of PANS-ATM).

CNS infrastructure (capabilities and performance):

- ATS communications (controller/controller): same requirement as for current SSR environment (as defined in section 8.3 of PANS-ATM);
- Navigation: same requirement as for current SSR environment (as defined in section 8.6.6 of PANS-ATM);
- Ground systems functions (e.g. FDP: same requirement as for current SSR environment; surveillance data tracker: must be able to process WAM-data) (as defined in section 8.10.2 of PANS-ATM); any further recommendations concerning functions are made in the worked example of a Preliminary System Safety Assessment in Annex L;
- ATC tools: a Short Term Conflict Alert tool (STCA) and Minimum Safe Altitude Warning (MSAW) will be present in the environment, as in the current SSR environment (as defined in section 15.6.2 of PANS-ATM);
- Airborne Safety Nets (ACAS): WAM has not degraded ACAS functionality (as defined in section *15.6.3 of PANS-ATM)*.

Secondary Surveillance Radar (and its operational use and environment) is used as a baseline because:

- SSR and WAM require similar onboard equipment (in terms of 1090MHz transponder, and supporting data registers) and adhere to similar standards. (The standards for SSR are defined in sections 8.1-8.5 and section 8.8 of PANS-ATM; and in ICAO Annex 10 Volume IV).
- The performance of WAM-derived surveillance data is assumed to be equal to (or better than) SSR radar [ASSUMP14] – this has been demonstrated in

early operational implementations of WAM and is discussed further in section 4 of this document.

- Differences in the performance characteristics for these surveillance technologies in the specified coverage area are minimal for the purposes of the end user application (see also section 4).

In order to derive the safety objectives and requirements, a set of quantitative assumptions needs to be made about the likely traffic characteristics of the environment within which WAM will operate. The aircraft mix is assumed to be the same as in a high density SSR environment (when considering transponder-mandatory requirements) [ASSUMP15].

As this study is focused on the ground-based ATC service being provided, the traffic density is assumed per sector for the en-route and TMA case [ASSUMP08 and ASSUMP09].

- The maximum instantaneous count of aircraft in an en-route sector is 20; in TMA, the value is 15 aircraft.
- Average duration of a flight is 20 minutes for en-route (0.33 hours) and 10 minutes for TMA (0.167 hours). On average 45 aircraft are managed per hour in the en-route while over the same period 40 are managed in the TMA.
- This makes 1 Air Traffic Service Unit (ATSU) hour equal to approximately 7 flight hours in the TMA and 15 flight hours for en-route sectors.

3.4 Applicability of the OSED scenario.

In order to be representative of a wide range of candidate implementation environments, the traffic figures used here are not necessarily the highest expected anywhere in Europe, but are considered to be typical of a busy en-route or TMA sector.

This assessment concentrates on WAM sole means surveillance. It is very unlikely that WAM sole means would be used for the busiest sectors in Europe, for business reasons just as much as for other reasons.

Considering these two aspects together, it is clear that the traffic scenario and WAM sole means infrastructure scenario are consistent with each other and suitable as a widely applicable example for the purposes of this assessment.

Real world examples of operational use of WAM surveillance are in the Innsbruck Valley TMA (Austria) and the Ostrova region of the Czech Republic. Information from these two implementations is included within this document.

4. NORMAL OPERATIONS (SUCCESS CASE)

4.1 Overview

The evidence for the success case was not developed as part of this assessment. Reliance was placed on existing material referred to in 4.5 below, which consists of extracts from recent ICAO SASP meetings and papers together with EUROCONTROL studies carried out under contract by industry experts and independent research organisations. The success case presented in the current document is confined to an elaboration and explanation of elements of the Safety Argument, supported by extracts from the existing material mentioned.

The ‘success case’ describes the operation of the sub-system when all its components are operating correctly and it fulfils its intended function. This, in combination with the failure case (see chapter 5), describes the performance of the WAM sub-system throughout its envelope. The assumptions made, the mitigations identified and the safety requirements derived can be found in Annexes F, H.4.4 and M respectively.

The success case is set out for the example WAM sub-system in the safety arguments 1.1 and 1.2. The components of these arguments are shown below.

4.2 Argument 1.1: Operational service and airborne equipment is the same as the reference system

The intended function is to provide an ATC (vectoring, monitoring and separation) service using an independent co-operative surveillance sub-system. The procedures used by the controller are the same when using WAM as when using the reference sub-system.

As described in the OSED (Annex E), air-ground interoperability requirements and functional requirements are unchanged from those described in ICAO Annex 10 and PANS-ATM [5].

The operational services, procedures and operational environment are also described in the OSED (Annex E). This demonstrates that the operational service is the same as for the reference sub-system. The use of aircraft transponders is as given in section E.5.2 of the OSED and remains unchanged.

The procedures for providing the service to the aircraft remain unchanged from those used in the reference radar service.

For this assessment, it is also assumed that the ground-ground interoperability requirements are unchanged [ASSUMP05]. In reality, this means that CAT 48 ASTERIX data interchange is used. CAT 48 enables the WAM sub-system to send data as if it comes from a radar sub-system, so that a “legacy” ATC processing and display sub-system can be used without needing (m)any special adaptations to handle WAM data.

Local considerations

Even if the data interchange format is unchanged, a number of areas need to be considered in the local analysis such as:

- WAM data update rates need to be correctly processed by the tracker. Typically these are much greater than for radar;
- Strictly speaking, WAM error distributions (rather than radar distributions) need to be processed by the tracker. However, if WAM is imitating a radar (by using Asterix CAT 48 for interoperability reasons) the tracker cannot know that the data has different characteristics. In this case, the WAM error distribution must be no larger than that of the radar that the tracker is "expecting" to process.
- If, on the other hand, WAM data is sent to the ATC processing and tracker using a specific WAM Asterix category, then the tracker must be capable of handling the data correctly. (Note that WAM processing is being added to ARTAS.)

4.3 Argument 1.2: WAM sub-system performance in success case

The argument for the success case of the safety argument focuses on the fact that, when working correctly, the WAM sub-system has equivalent or better performance than the reference sub-system (i.e. MSSR). This means that the controller interface at the CWP is the same for WAM and the reference sub-system in terms of [SR22, Annex M]:

- Data items presented;
- Update rates;
- Format of presentation.

The quality of data must also at least match that provided by MSSR, for example in the following ways;

- The quality of the presented WAM data is at least as good as the reference sub-system [ASSUMP14].
- The operational services volume is completely supported by the WAM sub-system [ASSUMP17].
- The update rate is at least as frequent as SSR. The update rate depends on the probability of correct message decode at each WAM sensor and the redundancy of WAM sensors [ASSUMP20].
- The WAM sub-system is capable of differentiating replies from aircraft with duplicated Mode A/S codes (including those that are closely spaced) [ASSUMP19].

These aspects are discussed in Argument 1.2.2 and elaborated in greater detail, especially in the SASP material summarised below.

The rest of this section will:

- define the reference sub-system performance (as per Argument 1.2.1)
- show that, in principle, the WAM can meet the specified performance (as per Argument 1.2.2).

Local considerations

Note that the assumptions above will all need to be validated as being true for the local environment. Although within this assessment they are "assumptions", in the local Safety Case they must be addressed in detail as part of providing evidence for the success case, and cannot be assumed de facto. The first two assumptions will require detailed measurement of coverage and performance by flight checks. This is particularly important because WAM performance varies according to the relative positions of sensors and aircraft in an entirely different way to SSR.

As an example, para 4.6.2 below summarises specific measurements of performance made by Austrocontrol.

4.4 Argument 1.2.1: Reference sub-system performance and interoperability is defined

WAM provides an independent co-operative means of surveillance as does MSSR. Therefore, the reference sub-system chosen is current MSSR.

The performance of the MSSR is assumed to be consistent with the current EUROCONTROL Standard for Radar Surveillance in en-route Airspace and Major Terminal Areas [7].

This document is currently undergoing an update to be presented as Required Surveillance Performance (RSP), which is technology-independent. However, the updated Surveillance Standard will be very largely "backwards compatible" with the current document. RSP is defined at the input to the Human Machine Interface (HMI), referred to as Controller Working Position (CWP) in the rest of this document. It is derived using operational expertise, mathematical analysis (e.g. collision risk models) and experience. The latter point relates to the experience gained from the use of radar-based surveillance data, and in particular its safe use for many years.

In conclusion the reference sub-system performance is fully defined. Note that, when available, the RSP based standard will give a direct reference for acceptable performance of WAM, rather than by comparison to a reference MSSR.

Local Considerations.

The implementing State may also choose to define its own reference sub-system performance. Considerations for this are described in Section 6.3 (Argument 2).

4.5 Argument 1.2.2: WAM sub-system can meet in principle the specified performance and interoperability

The following documents show that *in principle* a WAM sub-system can be designed to meet the reference sub-system performance in a specified coverage volume:

- "Wide Area Multilateration" Report (EATMP TRS 131/04). [8], which discusses design criteria and performance capabilities of WAM sub-systems in general.

- "Comparative assessment of SSR vs. WAM", Edition 1.3, 29-09-05, EATMP reference 05/10/05-1 [9], which makes an initial comparison of WAM performance vs. SSR performance requirements.
- "Technical Comparison between Reference SSR and MLAT", ICAO SASP [10], which makes a very detailed comparison of WAM vs. SSR, including discussion of the various data items available from both WAM and SSR.

Each of these is discussed in turn, in more detail. Collectively, they provide ample evidence of the "in principle" argument for WAM performance.

- Note also that EUROCAE WG-70 is developing a specification/MOPS [11] for WAM sub-system performance[3] which will be sufficient to meet the RSP and which may be used as a means of compliance to gain technical approval (note that operational approval will still be necessary to show the "in-service" performance).

It is also worth noting that WAM performance can be better than radar in some cases, e.g.:

- WAM does not suffer some of the failure modes of SSR/Mode S surveillance sub-systems. For example, WAM does not use the lockout protocol in Mode S which avoids one of the significant failure modes of that sub-system.
- WAM update rates can exceed those that of radar. For example, the update rate of aircraft plots from a WAM sub-system can be of order 1s compared to 6 to 12 s for MSSR.
- WAM position accuracy can be higher than MSSR, depending on the configuration of WAM ground sensors compared to the range from the MSSR.

4.5.1 Wide Area Multilateration Report

This report was commissioned by EUROCONTROL, quite early in the investigation of WAM as a surveillance sensor, in order to provide a balanced description of WAM and its technical characteristics.

The early sections of the Report describe WAM sub-systems, examining different architectures and concentrating on the most important ways of achieving good time synchronisation of receiving sites, which is a major constraint on WAM performance.

Chapter 7 of the Report and subsequent chapters describe performance characteristics, including the complex relationship of these to receiver locations, with several comparison plots of SSR accuracy behaviour vs. that of WAM. Altitude accuracy is also covered, but this is less critical as the Mode C height information contained in the transponder signal can be (and is) decoded by WAM surveillance sub-systems in order to provide complete compatibility with current (M)SSR radar surveillance. Although there are few quantified statements, the general indications, compatible with other references, are that WAM is as good or better than (M)SSR in performance terms.

[3] EUROCAE WG70 and the EUROCONTROL Multilateration Task Force both consist of EUROCONTROL, service provider and industry experts. The specification under development is therefore being designed to meet the requirements of service providers as well as being achievable by industry.

The document concludes with a brief survey of various WAM sub-systems; an indication of cost drivers for WAM compared to radar; and some conclusions which include recommendations for further work.

4.5.2 Comparative Assessment of SSR vs. Wide Area Multilateration.

The comparative assessment contained in this document is an early deliverable of the EUROCONTROL Multilateration Task Force (MLTF) and provides an initial comparison of SSR vs. WAM performance requirements, using the EUROCONTROL Surveillance Standard [7] as a comparison baseline. The conclusions state:

"WAM has the potential to be a surveillance instrument for the future. In order to make the deployment of WAM systems possible (either as supplement or replacement of existing SSRs) a standardisation of the necessary requirements – in a similar manner to the Radar Surveillance Standard [7] – is essential."

As noted above in 4.4, the development of RSP will meet the aim stated in the conclusions quoted immediately above.

4.5.3 "Technical Comparison of SSR, ADS-B and WAM"

This reference consists of three related items, namely the SASP Meeting Report [10/1], plus a draft Assessment document [10/2]; and the detailed technical comparison itself [10/3].

The context is that the ICAO Separation and Airspace Safety Panel (SASP) has recently been considering the use of both ADS-B and WAM as alternatives to radar surveillance. Project Team 13 was specifically tasked with this. The Report of SASP Working Group of the Whole/10 (WG/WHL/10) [10/1] in 2006 states that

"… provided a table of the characteristics and performance of an MLAT system in comparison to a reference SSR. The meeting was informed that the SSR used as the reference radar was the same used by SASP in the comparative assessment with ADS-B. … the table in [10/3] is aimed at demonstrating that MLAT has a technical performance "equal or better" than that of the reference SSR. The meeting … reviewed the table with a view to including it as a supporting attachment to the MLAT comparative assessment.

… given the interest from States in progressing work on separation minima for use with MLAT, PT13 was assigned the task of developing a comparative assessment in a similar way to that developed for ADS-B. … [10/2] was a draft of the main document for the MLAT assessment. The meeting …undertook a detailed review of the draft document. Of note, the meeting understood that the scope of the assessment as detailed in the draft was for the provision of 5 and 3 NM separation minimums for MLAT systems. During its review, the meeting was reminded of the fact that the reference radar used was the same reference radar used in the ADS-B assessment for a 5NM separation minimum. … the same reference radar is in use in Australia providing 3NM separation within 100 NM of the radar head, so by default the 3NM case had already been proven for both MLAT and ADS-B, provided suitable supporting comparative data was available.

Specifically, the meeting agreed that the assessment should focus on aligning with the new Chapter 8 of Doc 4444 … published in 2007 [5] and the air traffic surveillance services detailed therein, rather than focusing on any one particular separation minimum. To that end … a single comparative assessment document along the lines of that provided in [10/2] … was reviewed in detail by the project team. That draft is included … in this report."

The draft Comparative Assessment referred to above was included as Annex 1 to the SASP WG/WGWHL/10 PT13 Report [10/2]. In its draft form it is more than 40 pages. Some extracts are given below (in italics):

"The ICAO Separation and Airspace Safety Panel (SASP) undertook an assessment of the use of ADS-B and MLAT to provide surveillance to support Air Traffic Services. The basis of assessment was a comparison of ADS-B and MLAT to a reference Radar. This assessment has resulted in the identification of a number of performance requirements … which must be met for ADS-B or MLAT surveillance to be as good as or better than the reference Radar. SASP concluded that ADS-B and MLAT as technologies can be used as a means of supporting the provision of ATS surveillance, including separation, in accordance with the requirements of ICAO Doc 4444 PANS-ATM, Chapter 8."

The assessment includes the following elements, covering much more than just a technical comparison; references are to Chapters within the SASP Comparative Assessment. (Note that this document is "work in progress" so, although being a useful compendium of information, cannot be considered as definitive guidance.)

- *"An overview of ATC surveillance (Chapter 2)*
- *The rationale used by the SASP in developing the methodology and to arrive at its conclusions (Chapter 3 and Attachments A & B)*
- *The performance requirements attached to the conclusions reached by the SASP (Chapter 3, Attachment C);*
- *A Compendium of Hazards and Mitigation Measures identified during the development of safety case to support ADS-B and MLAT trials and implementation (Chapter 3 and Attachment E);*
- *Evidence of achieved ADS-B and MLAT surveillance performance during several State ADS-B trials and implementations (Chapter 3 and Attachment D);*
- *A State Implementation Roadmap (Chapter 4); and*
- *Frequently Asked Questions (FAQs), aimed at increasing controller awareness of ADS-B surveillance (Attachment F)."*

The technical comparison was included as Annex 2 to the SASP WG/WGWHL/10 PT13 Report [10/3]. Consisting of a 29 page table of comparison between MSSR, WAM (MLAT) and ADS-B, it discusses the following surveillance data elements:

- Position Estimate: Basic Operation, Accuracy, Integrity, Update rate, Latency, Reliability.
- Velocity vector: Basic Operation, Accuracy, Integrity, Update rate, Latency.

- Speed
- Identity: Accuracy, Integrity, Update rate, Latency.
- Emergency Alerting; Basic Operation.
- Specific limitations of SSR compared to WAM: Reflections and duplicate track, multiple target resolution.
- Coverage.
- Availability of service.
- Continuity of service.
- Reliability.

The table also surveys the technical application of the data, as used by tracker sub-systems, and the operational application of the data as used by a separation service. In the latter, it discusses: Manoeuvre detection, Vectoring service, Emergency navigation service and Emergency altimeter service.

The conclusions [of 10/3] concerning WAM (MLAT) are:

- *"MLAT compares as equal or better than the Reference SSR System if coverage by an adequate network (number of visible MLAT-RUs and geometry of aircraft and MLAT RUs) is provided. MLAT is a cooperative independent surveillance system.*
- *MLAT offers a "(n-1)" design. Also other system performance parameters are based on the system design.*
- *No common mode failure of navigation and surveillance possible.*
- *MLAT is vulnerable to transponder failure (same as SSR).*
- *Display of MLAT and SSR reports together on a display: Radars inherently measure the aircraft's slant range instead of its true range. On the other hand MLAT gives the aircraft's position in x-y coordinates relative to the system's centre (or already calculated into WGS-84 coordinates). Therefore for a common presentation the radar positions must undergo a slant range correction before a common presentation of radar and MLAT reports on a single display (this is state of the art for multi-radar displays).*
- *MLAT is susceptible to 1090 MHz interference similar to SSR."*

4.6 Relationship to Arguments 2, 3 and 4

4.6.1 Argument 2. "WAM implementation in the specified area is acceptably safe".

There is a Safety Requirement [ASSUMP17] in Argument 2 to correctly design and validate the WAM sub-system to meet the required performance in the specified coverage volume.

Design validation can be established in part by compliance with the specification/MOPS under production by EUROCAE WG70 [11].

An example of performance testing of the WAM sub-system in its operational environment is given in a working paper prepared by Austrocontrol and presented to ICAO SASP: “Collection of Multilateration Data vs. GNSS in Flight Data Recordings” [12].

4.6.2 Example of actual comparison: “Collection of Multilateration Data vs. GNSS in Flight Data Recordings”

The SASP Working Group of the Whole, in 2007, was presented with further information beyond that discussed in [10] above. WP04 from that meeting [12] provided a comparison of Flight Data Recordings of GNSS position measurements (as reference datum) vs. MLAT position measurements, from data collected during the Site Acceptance Testing for the Wide Area Multilateration Surveillance System at Innsbruck Valley which took place from May 10th until May 12th 2003 and August 2 until August 4 2004. Figures presented in the paper are summarised in Table 1below.

Measurement	Mode S targets	Mode A/C targets	Comment
No. of data points	18134	60764	
No. within 70m of reference	17895	60306	70m is the individual sensor requirement from [7]
% within 70m	98.4%	99.05%	
RMS position error	13.6m	10.7m	
Probability of update (Pd)	98.99%	99.41%	Pd requirement is 97% overall from [7]

Table 1: Summary of Innsbruck multilateration position measurements

The paper concluded that:

“Airborne accuracy in the Innsbruck terminal area is better than 70m for 99 % of all target reports and better than 30m for 93 % measured against high-precision differential GPS reference data.

The installed MLAT system of 9 Remote Units and 2 Reference Transmitters provides cooperative surveillance-coverage exhibiting performance better than the traditional Austrian MSSR (requirements listed in Eurocontrol Standard Document for Radar Surveillance in En-Route Airspace and Major Terminal Areas, [7]) and has exceeded all specification requirements, even if one remote unit fails.”

The analysis overview in the paper contains several plots of position error and track error. These distinguish between the MLAT accuracy as calculated from signals received from Mode S transponders and the accuracy as calculated from signals received from Mode A/C transponders.

4.6.3 Argument 3.

Of particular relevance to Argument 3 in regard to the success case is ensuring interoperability, during the migration processes, of all sub-system components (including the airborne equipment, the replacement WAM surveillance sub-system and the reversionary procedures/operations to the previous surveillance sub-system) [see example SR21].

As noted in para 4.3 above, WAM performance can exceed that of MSSR. This may assist in the introduction of WAM. However, *any* differences in performance between the two sub-systems also introduce migration risks which must be considered in argument 3.

4.6.4 Argument 4.

Argument 4 requires evidence of ongoing monitoring processes of the sub-system in its operational environment.

Continuous monitoring of safety performance [see the example SR24 in Annex M] is required to ensure that the Safety Requirements continue to be met. This includes ensuring that the Safety Objectives (SO) are satisfied and assumptions on the operational environment and their external mitigation means (made during the safety assessment process) are correct while the sub-system is in operation. Safety monitoring also allows identification of any trends in the evolution of safety performance.

4.6.5 Additional considerations

To meet the success case, there are several safety requirements that must be satisfied. In particular, the following result from the traffic description given in the OSED:

- The WAM sub-system can track both Mode A/C and S aircraft (SR26).
- The WAM sub-system can successfully distinguish and track aircraft transmitting the same Mode A or S codes in the same airspace (SR27).

4.7 Recommendations

The positioning principles and accuracy achieved by WAM are sufficient to meet surveillance performance as specified in the surveillance standard. This has also been demonstrated on operational sites, for example [12].

However the performance of WAM sub-systems is very dependent on implementation (i.e. siting of receivers). WAM users must therefore perform a thorough analysis of the performance of their installation to determine the volume of airspace in which surveillance standard compliant performance is met. The data shall be used operationally only in the volume where the performance has been verified. Data from volumes of airspace where the performance has not been verified shall not be provided to the controller for operational use.

Verification of performance may be achieved by combining analysis of traffic of opportunity, test flights and use of predicted performance and coverage.

Attention shall be focused on the borders of the 3D volume where the performance can vary very rapidly.

The way that data are output from a WAM sub-system can also be different from radar. Because a WAM sub-system has to maintain internal tracking for its own operation, it can be that a smoothed position is output. Therefore, extrapolation by a tracker shall be limited to a short period of time and the behaviour of MRT in this situation shall be analyzed.

Altitude could come from a measurement made at a different time to the position. This issue shall be understood and consequences analyzed. The possible maximum time difference between position and altitude must be defined.

As usual, Integration with data of other nature shall be checked (e.g. bias between WAM and radar).

The fall back mode, where the data coming from the WAM sub-system are directly displayed on the CWP, must be analyzed and necessary actions shall be taken. Specific training of the controllers must be put in place, to understand the behaviour of the WAM sub-system when the update rate could be different (typically more frequent than what they are used to), as well as being not systematic in the same way as a radar update.

5. ABNORMAL OPERATIONS (FAILURE CASE)

5.1 Introduction

This section looks at the consequences of failures. For the failure case, the acceptable level of risk is defined as being within the Target Level of Safety (TLS) defined in ESARR4.

The failure case is demonstrated for the WAM concept described in the generic OSED (Annex E). It is referred to in the safety argument, section 1.3.

The emphasis in Volume 1 of this assessment document is on the principles and the factors to be taken into account in the safety assessment process, rather than on specific numeric values. Also, in practice, all conditions and assumptions must be revalidated in the local situation, so it is not directly useful to give quantitative results here. They are provided in the referenced Annexes as part of the example.

The process was as follows (in line with ESARR 4 [1], EUROCONTROL Safety Assessment Methodology [2] and ED-125 [4]):

- Identify hazards associated with the information displayed on the controller working position (Annex I);
- Assess the worst credible effect arising from each hazard, and assign severity (Annex I);
- Apportion an appropriate proportion of the target level of safety (TLS) per hazard, according to the severity of the effects of hazards (Annex H);
- Derive a Safety Objective per hazard, taking into account the probability of effect (i.e. the mitigations that form barriers between the hazard and the effect occurring) and apportionment of the TLS (Annex H.5.3);
- Identify possible causes for each hazard through construction of a fault tree and assess the top level result of the fault tree analysis against the hazard's safety objective (Annex L);
- Where a fault tree result does not meet safety objectives, set extra safety requirements in order to satisfy the objective. (*A worked example is given in this document. Local safety requirements would need to be derived according to specific conditions and equipment. Annex L and M)*.

A series of conditions were also identified during the safety assessment and these are shown in detail in Annex F, identified as FHAxx. Several of these are also listed below in Table 3: .

5.2 Example Functional Model

An example functional model has been developed to support the example PSSA analysis. The baseline functional model, where WAM is the only surveillance sub-system present, is presented in Figure 7 below.

It can be seen that many functions are outside the scope of WAM sensor equipment, as is to be expected, because the scope of the safety assessment is the complete en-to-end surveillance system from aircraft transponder to Controller Working Position (CWP). The interface with the controller (represented in Function 04) is of particular interest, since all operational hazards were identified at this point. In other words, hazards were expressed in terms of what happened at the controller's display (e.g. incorrect display of aircraft position).

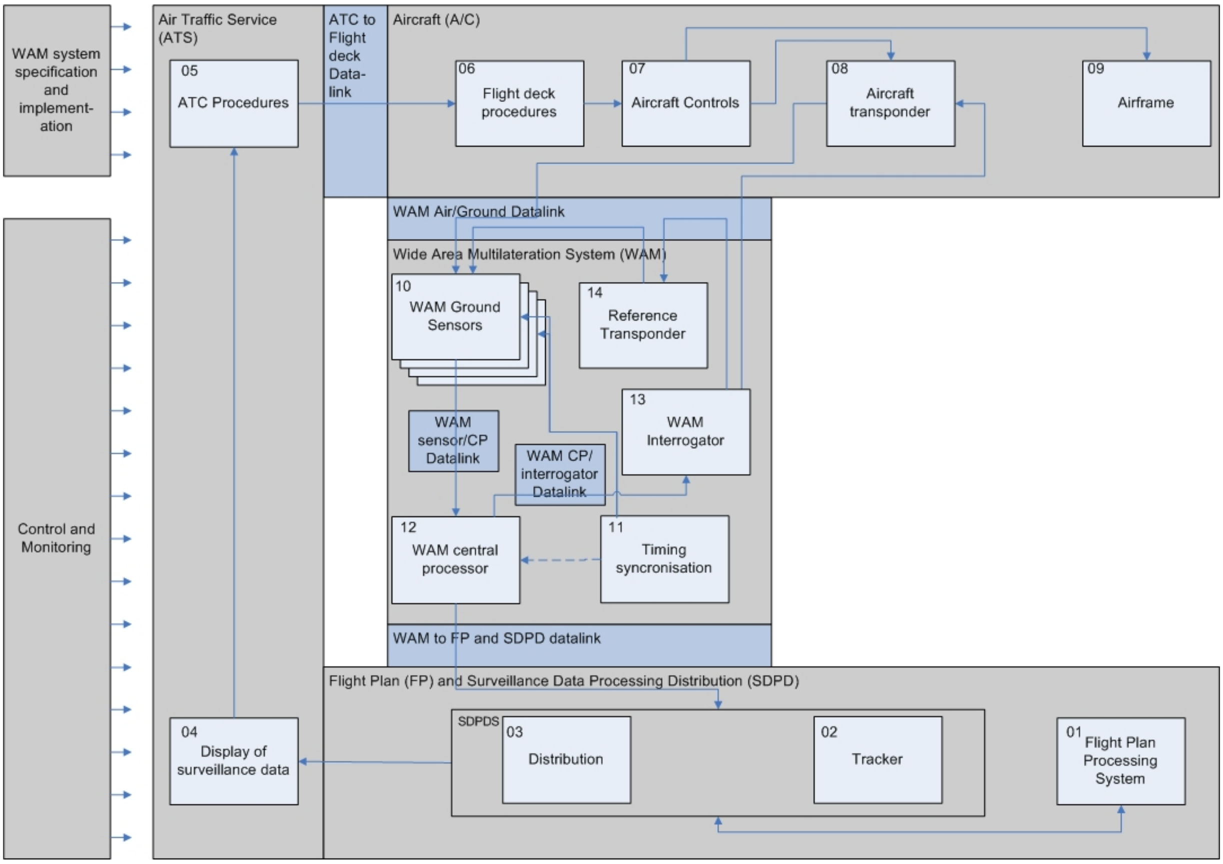

WAM system specification and implement-ation
Control and Monitoring
Air Traffic Service (ATS)
05
ATC Procedures
ATC to Flight deck Data-link
Aircraft (A/C)
06
Flight deck procedures
07
Aircraft Controls
08
Aircraft transponder
09
Airframe
WAM Air/Ground Datalink
Wide Area Multilateration System (WAM)
10
WAM Ground Sensors
14
Reference Transponder
13
WAM Interrogator
WAM sensor/CP Datalink
WAM CP/ interrogator Datalink
12
WAM central processor
11
Timing syncronisation
WAM to FP and SDPD datalink
Flight Plan (FP) and Surveillance Data Processing Distribution (SDPD)
04
Display of surveillance data
SDPDS
03
Distribution
02
Tracker
01
Flight Plan Processing System

Figure 7: Baseline functional model (WAM sole means of surveillance)

Other functional models, describing the addition of other surveillance sources (SSR, PSR or ADS-B) to WAM were also developed and can be found in Annex K. These other models, however, were not used further, so as to concentrate on WAM sole means, as being the most stringent assessment. The WAM sole means model is used in the example PSSA (Annex L).

5.3 Generic Functional Hazard Analysis (FHA)

Hazards were identified at the controller controller working position (CWP) i.e. procedures used by the controller are mitigations to the failure of the surveillance system. The consequences of each hazard were assessed to determine the potential outcomes, and the severity of these outcomes was determined by operational staff. It was then possible to set safety objectives on each hazard.

A semi-quantitative model was used to derive the safety objectives, based on ED-125 [4] recommended processes. The driving factors taken account of in these processes are the severity of the worst credible effect of the hazard, and the external mitigation means (EMM) that may prevent the hazard effects occurring. Conservative assumptions were made on the worst credible effects and probabilities of those effects. Probabilities were dependent on environmental conditions, such as the vicinity of traffic (based on route structure, airspace complexity and traffic density) and the probability that the controller would detect the hazard at the CWP and execution of procedures (thus moving the hazard from the undetected case to the detected case).

The study did not investigate hazards present in the controllers or aircrew procedures, as these are assumed unchanged from the current SSR surveillance environment.

Tables below summarise these various factors as briefly described here and expanded in the Annexes:

- Annex H, which provides the detail of the FHA, based both on the results of workshops held for this study and previous work in this area.
- Annex I, which shows the traceability in the decisions made by operational experts assigning worst credible effects to each hazard through a series of severity classification tables.
- Annex J which describes the severity classification systems used in this study, taken from ESARR 4 [1] and EUROCONTROL SAM [2].

The complete set of assumptions, environmental mitigation means (EMM) and environmental conditions circumscribe the conditions under which the results of the assessment are valid. The results of this example assessment are applicable to a specific local assessment only if the factors described in the various tables below also apply in the local operational situation.

5.3.1 Hazards and Severities

In essence, the operational hazards identified at the CWP were the failure of the system to deliver surveillance information, and the possible corruption of such information (display of erroneous data). Hazards and safety objectives are defined for the following data items, identified in the OSED, which are displayed on the controller interface:

- 2D position,
- Mode C barometric altitude,
- aircraft identity (e.g. call sign and SPI)
- short intent / history and
- all parameters together.

Loss and corruption were treated as two different hazards, so initially there were 10 main hazards (2 for each of 5 parameter situations). However, loss and corruption hazards affecting “short intent” were treated together, and hazards for “all parameters” were considered to have almost identical effects as hazards for 2D position and assessed as having the same severity. This reduces the list to 7 main hazards.

Each parameter has nominally 8 failure mode variants as listed below. However, only 5 need separate consideration, for the reasons indicated.

Loss, undetected, one aircraft.

Loss, undetected, many aircraft. *Not credible.*

Loss, detected, one aircraft.

Loss, detected, many aircraft.

Corruption, undetected, one aircraft.

Corruption, undetected, many aircraft.

Corruption, detected, one aircraft. *Treated as for loss as data not used.*

Corruption, detected, many aircraft. *Treated as for loss as data not used.*

The differences between En Route and TMA were also examined. Table 1 below lists the hazards and their assessed severity, as a result of the considerations summarised. Annex H provides a detailed rationale for this.

Parameter	ID	Hazard – short description	Variant	Severity (worst credible case)

2D position or all parameters	H01	Loss of 2D position (or of all parameters)	One aircraft, undetected	ER=3
				TMA=2

			One aircraft, detected	4

			Many aircraft, detected	ER=3
				TMA=2

	H02	Display of erroneous 2D position (i.e. corruption, of position or of all parameters)	One aircraft, undetected	ER=3
				TMA=2

			Many aircraft, undetected	ER=3
				TMA=2

Pressure altitude	H03	Loss of pressure altitude	One aircraft, undetected	5
			One aircraft, detected	4
			Many aircraft, detected	3

	H04	Display of erroneous pressure altitude (i.e. corruption)	One aircraft, undetected	ER=3
				TMA=2

			Many aircraft, undetected	2
Aircraft ID / call sign	H05	Loss of aircraft identity (Call sign)	One aircraft, undetected	5
			One aircraft, detected	4
			Many aircraft, detected	3
	H06	Display of erroneous aircraft identity (Call sign) (i.e. corruption)	One aircraft, undetected	3
			Many aircraft, undetected	2
Short intent	H07	Loss of, or display of erroneous, short intent	All variants	4

Table 2: Overview of hazards and assigned severities

The greatest severity assessed was value 2. In ESARR 4 terms [Annex A of Ref 1], a large reduction in separation (e.g. less than half the separation minima) with ATC and or crew able to recover the situation is nominally classed as severity 3. A conservative view regarded the worst credible case as being severity 2, in a complex TMA, because of the complex route structure together with more climbing and descending traffic. In this case an abrupt manoeuvre may be required to avoid collision with other aircraft.

5.3.2 Assumptions, including External Mitigation Means.

In drafting the FHA of the generic OSED, several assumptions were made, shown below and listed in Annex F. These assumptions, if used in the local safety case, will become Safety Requirements.

Some of these assumptions are regarded as External Mitigation Means, identified as “EMM” in the table, and are used when considering the probability of the hazard actually resulting in the effect, (Pe).

ID	Assumptions	Section	Where explained
FHA01	There is an assumption that the worst credible effect for combinations of the data elements occurs when ALL data elements are affected.	FHA	H.3.1
FHA02	If the controller detects the corruption, it is treated as loss (since the controller will not use the data).	FHA	Table 17 H.3.2
FHA03	The ground system includes some form of track extrapolation over a short-time period (assumed to be 30 seconds, or approximately 3 updates). In many systems, track extrapolation is shown by a different position symbol, alerting the controller to the failure in the surveillance data. In such cases, a failure will be displayed to the controller for up to 30 seconds, allowing him to prepare for the possible loss of the track from the display.	FHA	Table 17 H.3.2 H.4.2.2
FHA04	In conjunction with FHA03, and/or as part of his normal scan, the controller will detect lost data on the CWP 999 in 1000 times (i.e. there is a 0.1% chance that the loss of the data element will remain undetected long enough to cause a safety-related effect).	FHA	H.4.2.3 H.4.3
FHA05	It is assumed that, in the undetected case, the hazard lasts long enough for the worst credible effect to occur.	FHA	H.4.2.3 H.5.2
FHA06	It is assumed that the loss of call sign would mean it is replaced by the Mode A code (i.e. assumptions on the system are made in the fault tree analysis that Code-Call sign Correlation is available, and that standard reversion techniques are used). If Mode A code is lost, it is assumed that flight strips are maintained.	FHA	I.4 (severity classification tables)

FHA07	It is assumed (based on track structure, airspace complexity and traffic density) that for 1% of the time, aircraft will be in close enough proximity such that a separation-related effect will occur. An analysis of traffic in a busy radar sector provided evidence for this (conservative) assumption. [13]	FHA	H.5.2
FHA08	It is assumed that fusion is present in the ground data processor, such that the delivery of dual tracks for one aircraft to the controller will not occur.	FHA	H.3.2
FHA09 EMM1	Experience and ability of controllers is present, which enables them to identify that the failure has occurred. *(This is a general statement which is amplified in FHA03 and FHA04 above.)*	FHA	H.3.2
FHA10 EMM2	Procedural control can be established by controllers in the event of loss of data for one aircraft. The procedures are available (PANS-ATM, ANSP Manuals of ATC), training is given to the controllers in the use of procedural control, and the aircraft can successfully apply procedural control operations (R/T is available to make voice position reports, and flight crew procedures exist (PANS-OPS)).	FHA	H.3.2 Table 17
FHA11 EMM3	Experience and ability of flight crew is present, which enable them to identify that something is not nominal.	FHA	H.3.2 Table 17
FHA12 EMM4	Sector transfer procedures ensure that when an aircraft enters a sector, they contact the controller via R/T.	FHA	H.3.2 Table 17
FHA13 EMM5	It is assumed that procedural control when altitude data is missing is safe (through controller training, experience etc).	FHA	H.3.2 Table 17
FHA14	The controller is able to revert to procedural separation (for the affected aircraft) in the case of a continuous loss of all data for one aircraft (this also applies to individual data element loss).	OSED	3.2.2
FHA15	The controller is not able to safely revert to procedural separation in the case of a continuous loss of all data for all aircraft (in the high density environment). However, in the case of loss of altitude data for all aircraft, it is assumed that controller may safely revert to procedural separation.	OSED	3.2.2

Table 3: FHA-specific assumptions

5.3.3 Environmental Conditions

Several Environmental Conditions are shown below and were referred to in Section 3 above. They are described and explained more fully in the OSED (Annex E). These provide a minimum set of conditions which should be generally applicable to any local environment.

The traffic conditions listed in ASSUMP08 and 09 are appropriate to a busy sector. A local environment with less traffic is expected to experience hazards of a worst credible severity less than shown above in Table 2.

Environmental Condition	Environmental Condition
ASSUMP03	The capabilities arising from Mode A/C surveillance are the default level that can be assumed for the airborne domain.
ASSUMP08	Traffic conditions for the ENR airspace are: Average duration of a flight in the sector = 20 minutes Average number of aircraft managed per ATSU hour = 45 Maximum instantaneous count of traffic = 20 aircraft Average traffic in the sector = 15 aircraft.
ASSUMP09	Traffic conditions for the TMA airspace are: Average duration of a flight in the sector = 10 minutes Average number of aircraft managed per ATSU hour = 40 Maximum instantaneous count of traffic = 15 aircraft Average traffic in the sector = 7 aircraft.
ASSUMP10	Direct R/T is available to the controller and flight crew in the airspace being considered
ASSUMP11	Flight strips are maintained for all aircraft at all times to ensure that all the information usually displayed on the screen is retained by the controller for all aircraft. There is a fallback system which provides a basic static list of aircraft data should something else fail; this only helps in the short timeframe after a hazard occurs (after which the list becomes useless as it is out of date).
ASSUMP12	Controllers will always retain some level of 'mental' picture regardless of the amount of information lost as a result of flight strips being retained and used as required. The increased use of such strips will however increase controller workload
ASSUMP13	The controller is applying the minimum separation standard applicable for the airspace (e.g. 5NM en-route, 3NM in TMA)

Table 4: Environmental Conditions

5.4 Example PSSA

The PSSA involved the creation of fault trees that show how combinations of faults lead to the most critical hazards. The likelihood of faults has been assessed for the example WAM sub-system based on the study team experience, but any values used are only illustrative and should be replaced in an actual PSSA with justified values based on evidence of actual sub-system behaviour (for example from manufacturers' data or industry norms).

Fault trees were built for hazards with the most severe safety objectives. The study also looked at some causes of faults for the Identification parameter (following concerns over understanding the failure modes), and built fault trees to see if the safety objective was satisfied.

Each fault tree outcome was assessed against the safety objective of the hazard. Where the fault tree did not meet the safety objective, additional safety requirements were defined to ensure that the safety objective was met.

The final fault trees including additional safety requirements defined are shown in Annex L.4, and the results from their analysis are given below in Table 5.

Most hazards met the safety objective by a good margin and no additional safety requirements were required.

However, in the case of Hazard 01 *"Loss of 2D position (or of all parameters)"* for the variant *"detected hazard, affecting many aircraft"* additional safety requirements were required to meet the safety objective at the top of the fault tree. In the example, additional ground system redundancy was added. (Redundant data links between WAM ground receivers and central processing.) In an actual implementation, alternative safety requirements might have been proposed. These were chosen to illustrate the principle.

ID	Hazard – short description	Variant	Achievement
H01	Loss of 2D position (or of all parameters)	One aircraft, undetected	Achieved by more than order of magnitude
		One aircraft, detected	Achieved by more than order of magnitude
		Many aircraft, detected	***Achieved with additional requirements added***
H02	Display of erroneous 2D position (i.e. corruption, of position or of all parameters)	One aircraft, undetected	Achieved by more than order of magnitude
		Many aircraft, undetected	Achieved by more than order of magnitude
H03	Loss of pressure altitude	One aircraft, undetected	FHA15 assumes that reversion to procedural altitude separation is safe. This hazard was therefore not assessed further.
		One aircraft, detected	
		Many aircraft, detected	
H04	Display of erroneous pressure altitude (i.e. corruption)	One aircraft, undetected	
		Many aircraft, undetected	
H05	Loss of aircraft identity (Call sign)	One aircraft, undetected	Low severity, not analysed further
		One aircraft, detected	Achieved by about order of magnitude
		Many aircraft, detected	Not assessed in detail
H06	Display of erroneous aircraft identity (Call sign) (i.e. corruption)	One aircraft, undetected	Achieved by more than order of magnitude
		Many aircraft, undetected	Achieved by more than order of magnitude
H07	Loss of, or display of erroneous, short intent	All variants	Achieved by more than order of magnitude

Table 5: Results of fault tree analysis

5.4.1 Observations from the PSSA.

Each tree was analysed in detail in Annex L.4, including a discussion of the results. The following observations are a summary of these discussions, and are expected to be generally applicable to any WAM sub-system analysed and to any likely local environment:

- In each hazard case, the example WAM sub-system could be shown to meet the safety objectives through the definition of reasonable safety requirements. For example, a problem with low-decode probabilities of aircraft message could be solved either by additional receivers, sectorised receivers or alternative ground processing techniques.

- The main difficulty in the analysis was the failure rate of the airborne transponder. It is very hard to mitigate against some transponder failures in the WAM sub-system. (This is not only true for WAM – exactly the same applies to SSR/Mode S and ADS-B.) Therefore this remains a critical failure area for all cooperative surveillance technologies.

- WAM sub-systems have some components (e.g. central processor and interrogator) which are similar to conventional SSR sub-systems. These components must be monitored in a similar way to SSR. The role of the interrogator / transmitter to support the 'elliptical ranging' function of WAM (explained in K.2.6), which is essential to provide the necessary accuracy in some locations and configurations of WAM receivers, must be thoroughly understood. An undetected failure of this interrogator / transmitter will affect the accuracy of the data. This failure is identified as a cause for certain hazards (Annex L).

- WAM also has some unique components (e.g. the timing synchronisation function) that must be carefully evaluated during the local PSSA and SSA. It is important to understand the criticality of the timing synchronisation, which is fundamental to the Time Difference Of Arrival (TDOA) calculation of position. This is explained in more detail in E.5.3.1. The possible dependence on GPS time, as well as on other possible timing sources in the architecture of the selected WAM sub-system, should be completely understood. As there are several possible architectures, this Report does not analyse in detail the failure modes of all of them, although it does identify timing failure as a cause for certain hazards (Annex L).

- The example WAM sub-system analysed is 'minimal' – in particular this refers to non-redundancy of receivers, so that if one receiver fails, there is not enough information to form a position estimate. This approach was taken specifically to highlight the importance of multiple coverage of the entire volume of airspace for which the specified performance is required to support the operational service. The hazard caused by a receiver failure is analysed and it shown that adding redundancy reduces the hazard to an acceptable level. (Annex L). WAM manufacturers are very aware of this and would not usually install such a minimal WAM sub-system – they normally plan the siting of receivers so that one or more can fail without causing an unacceptable degradation of positioning performance. If one receiver can fail in this way, this is often called an 'N-1' scenario – meaning that N receivers are covering the volume and one may be fail.

- The non-WAM elements of the ground surveillance system (e.g. the tracker) also remain a source of hazard and must be carefully considered, as in today's surveillance systems.

6. GUIDANCE TO IMPLEMENTERS

6.1 Introduction

This section provides some elements of specific guidance for implementers to assist the creation of the local safety case (i.e. re-assessing argument 1 in their own environment, and fulfilling arguments 2, 3 and 4 of the safety argument).

Further general guidance to implementers is contained in Annex N that gives guidance on:

- the scope and limitations of this assessment;
- the roles and responsibilities of EUROCONTROL, ANSPs and regulators; and
- using the OSED and FHA within this assessment, including key questions to ask;
- transition to operations.

6.2 Argument 1

Implementers must satisfy themselves that the WAM concept is acceptably safe *in principle* for their local environment and application. This will entail taking this generic assessment and validating all assumptions and findings, in order to derive Safety Requirements for the local situation.

6.3 Argument 2

6.3.1 Arg 2.1: Local OSED has been defined

Specific characteristics of the local environment and operation, where they differ from the generic OSED (Section 3 and Annex E), must be assessed to decide if the differences have any impact on the analysis so as to render invalid the generic assessment in this Report.

6.3.2 Arg 2.2.1: The system design meets the success case requirements

To satisfy this argument, implementers should ensure that the Safety Requirements in Argument 1 are achieved:

- That the proposed WAM sub-system is designed to meet required performance in the specified airspace volume, when in a fault free situation.
- That it meets ICAO Annex 10 Volume IV (Surveillance and Collision Avoidance Systems) requirements [14]. Meeting these requirements is essential to ensure correct interoperation with aircraft transponders.
- That the impact on legacy systems is taken into account (interoperability). Here, it must be shown that the legacy systems will continue to operate with the new WAM sub-system. The interfaces between WAM and legacy systems are critical. Successful operation must be assured even in

fallback or downgraded modes of operation. Typical issues to be considered are data interface formats and data update rates.

6.3.3 Arg 2.2.2: The system design meets the failure case requirements

To satisfy this argument, implementers should ensure that the Safety Requirements referred to in Argument 1 are achieved:

- refine the generic FHA to provide local safety objectives;
- refine the generic PSSA analysis to provide local safety requirements;
- create specific system safety requirements and ensure they are met by the design.

From both the safety and interoperability point of view, implementers must again consider the interaction between WAM and legacy or external systems. For example, some WAM architectures use GPS as a timing source (as discussed in Annex L). This can make GPS a single point of failure for the WAM sub-system and therefore some mitigation is needed. If GPS is used by other ATC systems then the consequences of its failure must be considered in the analysis to avoid a common cause failure affecting the whole ATC system. Typically this may be achieved by addition of an alternate high accuracy clock in the WAM sub-system or ATC system as a whole.

6.3.4 Arg 2.3: The system implementation meets the safety, performance and interoperability requirements

To satisfy this argument, implementers should use the system acceptance tests to gather evidence to verify that all requirements are met, especially:

- coverage volume/performance verification in the nominal situation, with all components operating correctly;
- verification of performance in case of loss of redundancy;
- verification of performance in case of reference transponder failure;

At this stage of verification, two assessments are required:

- that the performance of WAM alone is as expected;
- that the performance of the overall surveillance system is as expected.

6.3.5 Arg 2.4: Local engineering, maintenance and operational procedures are defined where necessary

To satisfy this argument, procedures must be defined to meet the safety requirements identified elsewhere.

6.4 Argument 3

6.4.1 Arg 3.1: Migration risks identified

Migration risks may be identified through brainstorming and expert groups. Particular consideration must be given to the period of shadow mode operation during which the WAM performance is assessed before its operational introduction. This is very much a local activity, depending on the details of the current local operation.

6.4.2 Arg 3.2: Migration and reversion plan developed

A migration and reversion plan must be developed that describes (not an exhaustive list):

- Transition steps, e.g. starting with shadow mode operation at low traffic periods, e.g. at night;
- Reversion mode to previous (radar) sub-system operation and procedures for this;
- Training for both new operations and reversion modes;
- Reporting of incidents and gathering feedback;
- Timetable for introduction;
- Decision points and criteria for going forward;
- Co-ordination with neighbouring centres;
- Dissemination plans to airspace users and new procedures for them (if any).

Again, this activity is specific to the local manner of operation.

6.4.3 Arg 3.3: Migration risks resolved

Evidence should be gathered to show that all migration risks have been resolved. One way in which they may be resolved is through training staff on new procedures.

6.5 Argument 4

6.5.1 Arg: 4.1 In-service incidents and performance are monitored

Procedures in the local Safety Management Scheme (SMS) should be used to ensure that in-service incidents and performance are monitored. Specific measures here can include:

- Establishing an incident reporting system (this may be established already as part of an existing local SMS);
- Participation in the WAM community, e.g. by attending international groups where other States report their issues;
- Periodic performance checks, e.g. flight tests;
- Monitoring the quality of airborne equipment (e.g. incidence of duplicate addresses).

6.5.2 Arg 4.2: Corrective actions are taken

Procedures in the local SMS should be used to ensure that corrective actions are taken in the event of an incident or fault. Necessary feedback should also be provided to manufacturers, operations and users.

7. SUMMARY AND CONCLUSIONS

7.1 Introduction

This section presents a summary and conclusions.

Because all these conclusions are formulated for a generic environment and example WAM sub-system, they may not apply in a particular implementation.

This is NOT a formal safety case for the use of WAM derived data.

7.2 Summary

This document presents a generic safety assessment for the provision of WAM surveillance within an ATC system in the en-route and terminal airspace in core area Europe. It is intended to support European ANSPs that are implementing WAM either as a sole means of surveillance or in conjunction with other surveillance sensors.

The document shows that WAM can, in principle, be as good as radar in providing data for the provision of an ATC (vectoring, monitoring and separation) service in terminal and en-route airspace.

It also provides guidance to ANSPs to help them complete their own safety case, by offering a safety argument, together with some evidence, that ANSPs may use as a basis for the structure of their own safety cases.

The following approach is taken to demonstrating that WAM is ‘safe in principle’:

- The assumption is made that WAM will be used to support the same services that radar supports - specifically aircraft vectoring, monitoring and separation. The presentation of WAM information to the controller will be very similar (or identical) to radar presentation. Controller procedures will be unchanged from radar procedures.
- Airborne equipment and procedures are assumed to be the same for WAM as for a radar service.
- A generic OSED is defined for the assessment. This is a high-density environment based on future expected core-European traffic levels.
- A safety argument is defined, laying out the logic and evidence to show the system is ‘safe’. A core part of this argument is demonstrating compliance with the ESARR4 Target Level of Safety (TLS).
- An example minimal WAM sub-system is defined. This illustrates the WAM functions that may be present in an ATC surveillance system of which WAM is a component.
- A generic Functional Hazard Assessment (FHA) and example Preliminary System Safety Assessment (PSSA) are undertaken. The FHA examines possible hazards associated with the presentation of information to the controller and their possible consequences. The PSSA examines possible failure modes of the example WAM sub-system.

- From the FHA and PSSA, example safety requirements are identified that would need to be implemented for the example WAM sub-system to be considered ‘safe’ in the defined environment.

When following the assessment, it must be noted that, although operationally WAM ‘looks’ similar to SSR, it is technically very different. For example, WAM surveillance coverage is highly dependent on the relative positions of the WAM receivers. This affects the process to be followed when showing that the “success case” is met. Careful validation of the WAM coverage is therefore required to ensure that it is as good as radar in the volume of airspace where an operational service is provided.

7.3 Conclusions for the safety assessment process

An important conclusion is that following the SAM and SCDM / safety argument process has led to the derivation of achievable safety requirements for WAM surveillance implementation.

The approach of considering a minimal example WAM sub-system highlighted major weak areas where additional safety requirements were necessary. For example, redundant ground stations were required to meet the safety objectives. It is noted that this is normal practice for the installation of actual WAM sub-systems that have been accepted for ATC use.

7.4 Conclusions on WAM

The example analysis has shown that a WAM sole means surveillance sub-system can meet the safety objectives to support ATC services (vectoring, monitoring and separation) in a high-density traffic environment. Even a relatively minimal WAM sub-system can meet most of the safety objectives. By adding redundancy and other performance measures, all safety objectives are met.

Although this report has focused on possible failure mechanisms for WAM, it is worth noting that WAM performance can be better than radar in some cases, e.g.:

- WAM does not suffer some of the failure modes of SSR/Mode S sub-systems. For example, WAM does not use the lockout protocol in Mode S which avoids one of the significant failure modes of that system.
- WAM update rates can exceed those that of radar. For example, the update rate of aircraft plots from a WAM sub-system can be of order 1s compared to 6 to 12 s for MSSR.
- WAM position accuracy can be higher than MSSR, depending on the configuration of WAM ground sensors compared to the range from the MSSR.

The airborne transponder is the major weakness in the WAM safety assessment because it has a relatively low availability and cannot be modified. The transponder is a common point of failure for all cooperative dependent surveillance techniques, including MSSR, Mode S and ADS-B, so this issue is not exclusive to WAM.

7.5 Conclusions for the local safety case process

There are many issues to consider when the generic safety assessment is translated into a local safety case. These include:

- Local traffic and environmental conditions, which (for lower density traffic) may result in more relaxed safety objectives. Related to this is a review of the severity of all identified hazards.
- WAM cannot be considered in isolation from any other surveillance sources that are combined in the tracker. In other words, the surveillance system should be considered as a whole, including *all* the surveillance sources that are used. A particular consideration should be the chance of common mode failures between systems, depending on the specific local equipment.
- The local use of surveillance data must be taken into account. Controller tools using surveillance data are becoming more common and must be considered if they are part of the implementation.

7.6 Recommendations for the local safety case process

Some specific points have been highlighted above, that originate from the different behaviour and architecture of WAM sub-systems as compared to radar sub-systems. They are repeated here, because of their importance as part of the analysis to support the local safety case.

<u>WAM sub-systems performance dependence on receiver siting.</u>

The performance of WAM sub-systems is very dependent on implementation (i.e. siting of receivers). WAM users must therefore perform a thorough analysis of the performance of their installation to determine the volume of airspace in which surveillance standard compliant performance is met. The data shall be used operationally only in the volume where the performance has been verified. Data from volumes of airspace where the performance has not been verified shall not be provided to the controller for operational use. An example of such analysis was given in [12].

Verification of performance may be achieved by combining analysis of traffic of opportunity, test flights and use of predicted performance and coverage. Attention shall be focused on the borders of the 3D volume where the performance can vary very rapidly.

<u>WAM data interaction with tracking process.</u>

The way that data are output from a WAM sub-system can also be different from radar. Because a WAM sub-system has to maintain internal tracking for its own operation, it can be that a smoothed position is output. Therefore, extrapolation by a tracker shall be limited to a short period of time and the behaviour of MRT in this situation shall be analyzed. WAM data rate and error characteristics should also be considered.

Altitude and position update synchronism.

Altitude could come from a measurement made at a different time to the position. This issue shall be understood and consequences analyzed. The possible maximum time difference between position and altitude must be defined.

Bias errors.

As usual, Integration with data of other nature shall be checked (e.g. bias between WAM and radar).

Fall-back mode – bypass of ATC processing system.

The fall back mode, where the data coming from the WAM sub-system are directly displayed on the CWP, must be analyzed and necessary actions shall be taken. Specific training of the controller must be put in place, to understand the behaviour of the system when the update rate could be different (typically more frequent than what they are used to), as well as being not systematic in the same way as a radar update.

Elliptical Ranging function

The suitability and correct design of the Elliptical Ranging function should be scrutinised and assurance obtained that necessary measures are in place to mitigate possible failures. See Annex L for details.

Timing Function.

The timing function architecture of the installed system should be analysed in detail, together with its specific failure modes and mitigations for these. This issue is not treated in detail in this Report, because there are several possible architectures. [8] discusses this aspect, as summarised earlier.

Receiver redundancy.

The design and installation redundancy of WAM receivers in the airspace for which the operational service is provided must be analysed and the desired level of redundancy should be specified. Planning for one or more receivers to be able to fail without causing an unacceptable degradation of positioning performance must be undertaken – the ‘N-1’ scenario.

A Acronyms

A/C	Aircraft
ACAS	Airborne Collision Avoidance System
ADS-B	Automatic Dependant Surveillance - Broadcast
AF	Ambition Factor
AFARP	As Far As Reasonably Practicable
ANS	Air Navigation Service
ANSP	Air Navigation Service Provider
AO	Aircraft Operators
ASAS	Airborne Separation Assurance System
ASTERIX	All purpose STructured EUROCONTROL suRveillance Information eXchange
ATC	Air Traffic Control
ATCo	Air Traffic Control officer
ATM	Air Traffic Management
ATS	Air Traffic Service
ATSU	Air Traffic Surveillance Unit
CASCADE	Co-operative Air Traffic System through Surveillance and Communication Applications Deployed in ECAC
CCCD	Code Call sign Correlation Database
CONOPS	CONcept of OPerationS
CP	Central processor
CWP	Controller Working Position
ECAC	European Civil Aviation Conference
EASA	European Aviation Safety Agency
EATMP	European Air Traffic Management Programme
EC	Environmental Condition
ECAC	European Civil Aviation Conference
ED-XXX	Eurocae Document XXX (e.g. ED-78A)
EMM	External Mitigation Means
ENR	En-route
ESARR4	EUROCONTROL Safety Regulatory Requirement 4 (Risk Assessment and Mitigation in ATM)
EUROCAE	EUROpean organisation for Civil Aviation Equipment
EUROCONTROL	European Organisation for the Safety of Air Navigation
FAA	Federal Aviation Administration
FDP	Flight Plan Data Processing
FHA	Functional Hazard Assessment
FRUIT	False Replies Unsynchronised In Time
FTA	Fault Tree Analysis
GNSS	Global Navigation Satellite System
GSN	Goal Structured Notation
HITT	Netherlands based safety and security company.
HMI	Human Machine Interface
ICAO	International Civil Aviation Organisation
IFR	Instrument Flight Rules
IMM	Internal Mitigation Means
JAA	(European) Join Aviation Authorities
MLAT	MultiLATeration
MOPS	Minimum Operational Performance Specification
MSAW	Medium Safe Altitude Warning
MSSR	Monopulse Secondary Surveillance Radar
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair

N/A	Not Applicable
NM	Nautical Mile
OE	Operational Effect
OSED	Operation Service and Environment Description
PANS	(ICAO) Procedures for Air Navigation Services
PANS-ATM	(ICAO) Procedures for Air Navigation Services - Air Traffic Management
PANS-OPS	(ICAP) Procedures for Air Navigation Services - OPerationS
Pe	Probability a hazard generates its worse credible effect
PSR	Primary Surveillance Radar
PSSA	Preliminary System Safety Assessment
R/T	Radio Telephony
RCS	Risk Classification Scheme
RF	Radio Frequency
RFG	Requirements Focus Group
RNAV	Radio Navigation
RNP	Required Navigation Performance
RSP	Required Surveillance Performance.
RTCA	Radio Technical Commission for Aeronautics
SAM	Safety Assessment Methodology
SASP	Separation and Airspace Safety Panel
SDP	Surveillance Data Processing
SDPS	Surveillance Data Processing System
SO	Safety Objective
SPI	Special Position Indicator
SPR	Surveillance Performance Requirements
SR	Safety Requirement
SSA	System Safety Assessment
SSR	Secondary Surveillance Radar
SSTF	Secondary Surveillance Task Force
ST	Safety Target
STCA	Short Term Conflict Alert
STi	Safety Target for severity class i
TDOA	Time Difference Of Arrival
TF	Task Force
TLS	Target Level of Safety
TMA	Terminal Manoeuvring Area
TOA	Time of Arrival
VFR	Visual Flight Rules
WAM	Wide Area Multilateration

B Glossary and Definitions

Term	Explanation
Acceptably safe	The risk of an accident / incident is: 1 No greater than for the reference system 2 Within the Target Level of Safety and 3 Further reduced as far as reasonably practicable (AFARP)
Receiver	An electronic circuit that receives a radio signal from an antenna and converts the signal into a protocol understood by WAM sub-system which, in turn, can be used by the central processor to produce surveillance information (e.g. position).
Reference system	A system against which the newly installed WAM sub-system is compared. In this generic case the reference sub-system is assumed to be based upon mono-pulse SSR technology.
Safety objective	A desired level of safety for a particular hazard derived from ESARR 4 [1] & [4].
Safety requirement	Requirements placed upon hazards in order for them to meet the Safety Objective stipulated for them (e.g. this may require a system to have in-built redundancy or be gold plated).
Sensor	The ground station component of a WAM sub-system. Is comprised of a receiver and a transmitter that relays the decoded information from an aircrafts transponder to the central processing unit.
Success case	Describes the operational performance of the system under normal operations (i.e. when its all components are operating correctly and they fulfil their intended function).
System	Within the context of this document a system is taken to mean the people, procedures and equipment considered as a single entity.
Failure case	Describes the performance of the system after it has suffered a failure (i.e. conditions imposed on the system are considered to be outside the scope of 'normal operations').

C References

1 ESARR 4 “Risk Assessment and Mitigation in ATM”, Edition 1.0 05/04/2001.

2 EUROCONTROL ANS Safety Assessment Methodology, v2.1 (electronic), November 2006.

3 EUROCONTROL Safety Case Development Manual v2.2, November 2006.

4 ED-125 “Process for Specifying Risk Classification Scheme and Deriving Safety Objectives in ATM “in compliance” with ESARR4,” DRAFT version 7, 10th October 2006 http://www.eurocae.org/.

5 ICAO PANS-ATM “Procedures for Air Navigation Services – Air Traffic Management,” Fourteenth Edition (Doc 4444).

6 ICAO PANS-OPS “Procedures for Air Navigation Services – Aircraft Operations,” Fifth Edition (Doc 8168).

7 EUROCONTROL Standard Document for Radar Surveillance in en-route Airspace and Major Terminal Areas, SUR.ET1.ST01.1000-STD-01-01, Edition 1.0, March 1997.

8 “Wide Area Multilateration” Report, EATMP TRS 131/04 Version 1.1, August 2005, produced for EUROCONTROL by Roke Manor Research, HITT Traffic and the National Aerospace Laboratory of the Netherlands.

9 “Comparative assessment of SSR vs. WAM”, Edition 1.3, 29-09-05, EATMP reference 05/10/05-1.

10 “Technical Comparison of SSR, ADS-B and Wide Area Multilateration”, Annex F, Report of Project team 13, ADS-B and MLAT. Separation and Airspace Safety Panel, (SASP), Tenth Meeting of the Working Group of the whole, 27 November – 8 December 2006. (This reference consists of Annex F, together with Attachments 1 and 2, separately identified as [10/1], [10/2] and [10/3].)

11 “Technical Specification for Wide Area Multilateration based on the existing and planned requirements defined by the EUROCONTROL Multilateration Task Force”, Document in preparation, EUROCAE Working Group WG-70, http://www.eurocae.org/.

12 “Collection of Multilateration Data vs. GNSS in Flight Data Recordings”. Separation and Airspace Safety Panel, (SASP), Eleventh Meeting of the Working Group of the whole, 21st May to 1st June 2007. SASP-WG/WHL/11-WP/04.

13 RFG working paper “Use of Separation Minima in typical UK High Density airspace,” QinetiQ and NATS, September 2005.

14 ICAO Annex 10 Volume IV, Surveillance Radar and Collision Avoidance Systems, Amendment 77, www.icao.int.

15 Safety, Performance and Interoperability Requirements Document for ADS-B-NRA Application (ED-126), EUROCAE, December 2006.

16 Operational Hazard Assessment of Elementary and Enhanced Surveillance, EUROCONTROL, 7th April 2004.

17 EUROCONTROL Mode S Programme, Preliminary System Safety Analysis for the Controller Access Parameter service delivered by Mode S Enhanced Surveillance, Pascal Dias and Eric Potier, 2004.

18 “RNP RNAV Requirements: Safety discussion”, Document reference D368007, Helios Technology Ltd for EUROCONTROL, 1 December 2003.

19 “CASCADE 1090MHz interference study”, Edition 2.3, Document reference Ref D533D008, Helios Technology Ltd for EUROCONTROL, July 2006, R. McDonald.

20 “A-SMGCS Level 1 and 2 - Guidance Material in support of the Preliminary Safety Case,” EUROCONTROL, version 0.6 (draft), 2006.

D Explanation of the Goal Structured Notation (GSN) used for the Safety Argument

D.1 Introduction

The Goal-structuring Notation (GSN), developed by the University of York, provides a graphical means of developing hierarchical safety arguments.

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

D.2 GSN Principles

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.

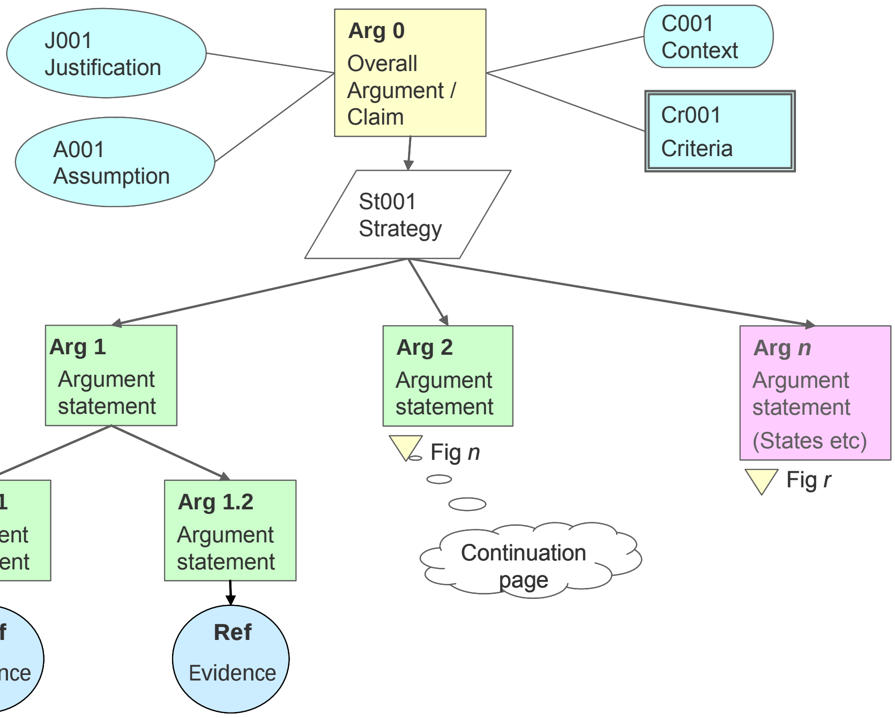


Figure 8: Specimen Goal Structured Notation argument

D.2.1 Arguments

An *Argument* should always take the form of a simple predicate - i.e. an atomic 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 **Arg1** is satisfied by the combination of **Arg1.1** and **Arg1.2**, then we need to show that **Arg1.1** and **Arg1.2** are true in order to show that **Arg1** 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*.

D.2.2 Evidence

It follows from the above that, for an *Argument* structure to be considered to be complete, every branch must be terminated in an item of *Evidence* that supports the *Argument* to which it is attached.

Evidence therefore must be:

- appropriate to, and necessary to support, the related *Argument* - spurious *Evidence* (i.e. information which is not relevant to, and or does not support, an *Argument*) should be avoided since it would serve only to confuse the "picture".
- sufficient to support the related *Argument*; inadequate evidence undermines the related Argument and, potentially all higher levels of the Argument structure.

D.2.3 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.

D.2.4 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.

D.2.5 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.

D.2.6 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.

D.2.7 Criteria

Criteria are the means by which the satisfaction of an *Argument* can be checked.

D.2.8 Numbering

It is recommended that *Arguments* be numbered hierarchically (e.g., **Arg1.1**) to reflect their logical structure.

Strategies, *Assumptions*, *Context*, and *Criteria* should be numbered sequentially (e.g., **St0001**) since they embellish, but do NOT form part of, the logical structure.

It is recommended that *Evidence* be numbered according to its source reference and that the *Evidence* ‘bubble’ contains a brief indication of the form that the *Evidence* takes.

EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

Generic Safety Assessment for ATC Surveillance using Wide Area Multilateration *Volume 2*

Edition Number	**:**	**5.0**
Edition Date	**:**	**23 October 2008**
Status	**:**	**Proposed Issue**
Intended for	**:**	**EATMP Stakeholders**

DOCUMENT CHARACTERISTICS

TITLE
Generic Safety Assessment for ATC Surveillance using Wide Area Multilateration

	EATMP Infocentre Reference:	
Document Identifier	**Edition Number:**	4.1
	Edition Date:	29.07.2008

Abstract

This document presents a generic safety assessment of the use of Wide Area Multilateration (WAM) for ATC surveillance. The assessment considers WAM in support of an ATC service (vectoring, monitoring and separation) in en-route and terminal airspace.

This safety assessment is a starting point for ANSPs developing a safety case for WAM systems. It also contains guidance for those undertaking such safety cases.

Keywords

Contact Person(s)	Tel	Unit

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:	\\HHBRUNA04\darbyb$\WAM\WAM CONTRACT Generic Safety (T06-11093EB)\2008 Final-final review	
Host System	Software	Size
Windows_NT	Microsoft Word 10.0	4218 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.		

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

INTRODUCTION TO VOLUME 2

Introduction.

Volume 2 of the WAM Generic Safety Assessment consists mostly of material that has been developed to provide a worked example. The intention is that ANSPs wishing to install WAM and therefore required to prepare a safety case for their Regulators, in order to obtain approval, can model at least part of their safety case on the material included in this document.

It should be understood that, whereas Volume 1 is a summary of the whole assessment with an emphasis on the “success case”, Volume 2 concentrates on the details of the “failure case” – i.e. analysis of what can go wrong and what safety requirements are derived to constrain failures and their effects to an acceptable level, so that a system can be approved for operational use.

The main elements of the worked example of the failure case safety analysis are the Functional Hazard Analysis (Annex H) and the Preliminary System Safety Analysis (Annex L). Other annexes are provided as support for these. The material in Volume 2 is organised as follows.

Annex E.

This contains the detailed OSED and is an expansion of Volume 1, Section 3. As well as the assessed “sole means” WAM sub-system, the Annex also discusses other possible technical scenarios and their safety, capacity/efficiency and cost effectiveness benefits, providing justifications for choices other than WAM alone. Some technical considerations on aircraft transponders and WAM timing systems are also included. .

Annex F.

Throughout the entire assessment, the precise scope of the system and sub-systems that are being examined is defined. In many cases, this depends on a variety of assumptions – about the operational traffic environment, the infrastructure other than the WAM sub-system, some details of the functional use of the system and specific quantified assumptions for the PSSA. Annex F gathers together all assumptions made at any point in this example assessment.

Note: *if re-using this material in any way, ANSPs must ensure that the assumptions and conditions about their own systems, sub-systems and operational or technical environments are the same or sufficiently similar to the conditions of this example, so that the work of the example may legitimately be re-used.*

Annex G.

A full quantitative safety assessment, of which this study provides a model of the stages up to and including the Preliminary System Safety Assessment (PSSA), is a lengthy and complex task. Detailed guidance is provided in EUROCONTROL

SAM [2], the Safety Case Development Manual [3] and EUROCAE ED-125 [4]. So as to make the current Report self-contained, a summary of the process applied is given in Annex G. This summary is drawn largely from ED-126 *"Safety, Performance & Interoperability Requirements document for the ADS-B NRA Application"*, [15] some parts of which were a reference for the current study.

Annex H.

Annex H, the Functional Hazard Assessment (FHA), is one of the two main elements of Volume 2. This Annex (expanding on Section 5.3 of Volume 1) consists of the step-by-step development of Safety Targets (from ED-125) appropriate to various severities of hazard. This includes a discussion of the functional or operational hazards to be assessed with their qualifying conditions and circumstances to more precisely describe them, and leads to the possible effects of each hazard. (Many of these conditions and circumstances are documented as assumptions in Annex F.) It is these possible (credible) effects that lead to the severity that is assigned to each hazard. This is the first step in calculating the safety objective.

There follows a discussion of various mitigations which may prevent the hazard actually resulting in the associated effect. These are quantified to the extent possible. The result is the Pe – the probability that the hazard will result in the effect.

In this Study, and equally well in an ANSP assessment, the functional or operational hazards are usually derived from workshops in which the operational users of the system as a whole identify what could go wrong with the system at the user interface (the CWP) and what could be the effects on their operational function or capability, taking account also of the available mitigations. The outcome of the workshop activity is given in Annex I.

An example calculation of the safety objective for a hazard is then given, taking into account the mitigations and the environmental conditions. It is the safety objective that is the numeric value to which the surveillance system, including the WAM sub-system, must be designed, in order that the occurrence of the hazard is reduced to an acceptable level (for the ANSP) and a tolerable level (for the Regulator).

***Note** again that the calculations given in this section cannot be taken directly into an ANSP safety assessment; they are examples of the process.*

Annex I.

The operational workshop process mentioned above was carried out for this Study, supported also by comparison with other surveillance safety studies, as well as advice on the assessment overall from safety experts within the EUROCONTROL Agency. The outcome is documented in Annex I.

Annex J.

For convenient reference, as they were used in the operational workshop documented in Annex I, the severity classification scheme from ESARR4 [1] and the severity indicators from SAM [2] are included in Annex J.

Annex K.

So as to be able to carry out the other main part of the assessment process, the Preliminary System Safety Assessment (PSSA), it is necessary to have a description (at a fairly high “block diagram” level) of the system that is being assessed. This is the complete system (remembering that ESARR4 calls for end-to-end assessment) with the WAM sub-system embedded in context.

Annex K (expanding on Section 5.2 of Volume 1) concentrates on a functional model of a WAM sole-means surveillance subsystem in the context of the overall ATM system. It also develops the identification and flight plan correlation function to a further level of detail, as there are hazards associated with identification that were identified in the FHA. A summary of the variety of timing architectures of WAM systems and the “elliptical ranging” function of active WAM systems are also provided, so as to aid understanding of these, to the extent that they are examined in the PSSA. In order to cover all the technical system scenarios considered in Annex E, overall system block diagrams of WAM plus ADS-B, WAM plus SSR and WAM plus PSR are also shown.

Annex L.

This is the Preliminary System Safety Assessment (PSSA) and is the second main element of Volume 2, expanding on Section 5.4 of Volume 1. It is provided to illustrate the PSSA process by means of a worked example.

The purpose of the PSSA is to take the quantified safety objectives (from Annex H) and to analyse the proposed (preliminary) system design incorporating the WAM surveillance sub-system, to see if the safety objectives can be met. Fault tree analysis (FTA) is the technique adopted, supported by software tools (mentioned in the Annex) for the process and manipulation of the fault trees and by reasonable quantified estimates of the failure rates of the components of the system examined. In an actual ANSP assessment, the values used for the PSSA would come largely from their own technical department (based on monitored behaviour of their existing system) and from the WAM system supplier (based on actual demonstrated performance of installed systems, or the qualification of systems to industry standards).

***Note** that there is no suggestion that the content of this Annex can be directly re-used in an ANSP assessment; it is the process and principles that are important.*

Annex M.

From the results of the PSSA, safety requirements for this assessment are summarised. An important principle is that, assumptions which are used (relied upon) in the assessment of any failure probabilities, become requirements to achieve those failure probabilities. This is one reason why it is so important to explicitly and clearly identify all assumptions.

***Note** again, it must be emphasised that the requirements in Annex M cannot be taken directly into an ANSP analysis; they are applicable only to the example developed in this document to illustrate the process. Nevertheless, the considerations that are highlighted by the safety requirements presented here identify most of the issues that ANSPs may come across in an actual safety assessment.*

Annex N.

The final Annex places the safety assessment within the overall Safety Case development process. It also includes some guidance on the details of the various steps embodied in the previous annexes, in the form of key questions that the ANSP should ask as the process proceeds.

E Generic Operational Service and Environment Description (OSED)

E.1 Introduction

This annex contains the full Operational Service and Environment Description (OSED), included here for ease of reference. A summary of the application and environment description is given in section 3.

Sections E.2 to E.4 present those characteristics of the OSED that are common to all surveillance scenarios, such as procedures and operational environment.

Section E.5 (together with more detail in Appendix 1 to this Annex) considers the technical characteristics of surveillance scenarios, as well as the aircraft transponder and WAM timing issues, in order to provide an understanding of how failures could occur and what they may be, as background for the subsequent Functional Hazard Assessment process.

E.2 Application Description

E.2.1 Introduction

This application description is written to show the context within which surveillance data (in this case, generated from WAM sub-systems) is expected to be used.

The operational procedure is intended to be technology-independent. Evidently, this affects the assessment of benefits to be gained from the implementation of specific technologies such as WAM, along with the identification of specific alterations to the overall system. This assessment therefore appears in Annex E.5 as a series of specific surveillance scenarios. The core application of providing ATC services in en-route and TMA airspace does not change.

The applications described are the following ICAO Air Traffic Services (as found in the relevant section of PANS-ATM as indicated): Air Traffic Control, Flight Information and Flight Alerting Service, principally for the following services:

- Operation of air traffic control service:
  - Vectoring *(Section 8.6.5);*
  - Separation *(for radar controlled airspace the coordination of traffic is detailed in section 8.7.2,, the application of radar separation minima in section 8.7.3 and the minima themselves in section 8.7.4)*;
  - Monitoring *(Safety level management in section 2.4, controller functions in tactical operations section 3.2.5)*.
- Flight information service:

  - Provide traffic information *(essential traffic information detailed in section 5.10; the type of information provided in 5.10.2, the advisory service in section 9.1.4; and other traffic information messages in section 11.4.3.1).*
  - Provide navigational assistance *(vectoring in section 8.10.1, departure from radar controlled airspace in 10.4.2.5; procedures for strayed VFR flights and VFR flights encountering adverse weather conditions in section 15.3.1)*.
- Alerting Service, principally for the following functions:
  - Notification of rescue co-ordination centres *(Sections 7.1.2.1, 9.2.1.1, 9.2.2, 11.4.1 and 15.1.3)*;
  - Plotting of aircraft in a state of emergency *(Sections 9.2.1, 11.4.1 and 15.1.2)*.

E.2.2 Procedure Description

This document assumes that proposed PANS-ATM procedures will be essentially unchanged when using WAM derived data, subject to approval by ICAO.

In particular, this is important from the controller perspective, as there should be no requirement to make them aware of the technology source when using data on the working position for ATC service provision.

A technical comparison between WAM, ADS-B and a reference SSR environment, performed by the ICAO SASP group, has been carried out in a document entitled a “Technical Comparison between Reference SSR, ADS-B and WAM” [7]. This document indicates that ADS-B and WAM represent an improvement in surveillance coverage compared to that that offered by SSR, however the quality and extent of the coverage depends upon the design of the surveillance sub-system.

Any changes to ATCO procedures (regardless of the surveillance sub-system implementation and/or operational maturity at the time they are introduced) must first be designed and then validated (e.g. using simulation or flight trials) within a specified coverage volume [ASSUMP06, see also ASSUMP17].

The differences that exist between the surveillance technologies are related solely to the technical aspects. Some of these aspects relating specifically to WAM and the use of aircraft transponders are indicated in section E.5.3 (technology considerations). It has been assumed for the purposes of this document that these differences do not affect their use operationally. [ASSUMP02]

Note that this assumption may not be fully true for transition to service of new technologies, where trust in the system has not been fully gained through experience. Therefore in the early operation of the new system, even though it enables the same service as legacy surveillance technologies, there may be some operational procedures introduced to mitigate this issue (see 2.4 for more on transition to operations).

Provision of ATC Services

Separation is provided by the ATCO, vectoring aircraft if required. Position information is gathered from presented surveillance information, with intent information gathered through correlation with the flight plan.

The following information elements are required from the surveillance sub-system for the provision of the services specified in E.2.1. This list does not include flight plan elements.

The availability of some of the elements are dependent on the type of interrogation in the airspace (for passive WAM sub-systems), or on the capability of the aircraft transponder.

Although a mandate for Mode S exists in Europe, it has not been assumed that Mode S transponders will be available and equipped for all aircraft operating in the en-route and TMA environment under discussion within this OSED.

It is therefore assumed that the capabilities arising from Mode A/C surveillance is the minimum (baseline) level of surveillance capability available to the controller [ASSUMP03].

Operational information used by the controller for the provision of a separation service includes:

- **Horizontal (2D) position**;
- **Vertical position** (barometric pressure altitude via Mode C) – for the controller, this will continue to be displayed in 100ft increments;
- **Aircraft identity** (ICAO aircraft call sign or Mode 3/A code, and SPI);
- **Short Intent and Track History** (derived within the tracker).

Additionally, flight status is defined in ICAO Annex 10 (Vol IV, Chapter 3), although it is not considered in the scope of this study.

Roles and Responsibilities

The role of the controller and pilot remain unchanged [ASSUMP02] from the current surveillance services provided to maintain a separation service as described under PANS-OPS (parts 2 to 11 in Volume 1 and parts 2 to 6 in Volume 2).

There are no changes in responsibilities of the aircrew or controllers. The controller remains responsible for the management of the airspace, maintaining separation and providing information to aircrews, whilst the aircrews are responsible for acting upon ATC instructions and providing information to ATC.

Impact on Phraseology

It is anticipated that there will be no changes in phraseology for aircraft under WAM surveillance compared to that used today in radar surveillance services. This includes the continued use of the term “radar contact” (with the assumption that neither the controller nor the flight crew will be concerned whether it is actually radar providing the data [cf. ASSUMP02]).

Performance Checks for System

Controller procedures for performance checks on the WAM surveillance data will be required (in particular barometric altitude verification procedures) in the same way to those specified for SSR surveillance (additional detail is provided in section 8.6.1 of PANS ATM).

Emergencies, Hazards and Equipment Failures

In the event of an aircraft reporting an emergency situation, then the current emergency procedures as for radar control will apply.

Emergency modes in the Surveillance report are expected to signify, as a minimum, the same emergency conditions as are presently signified by Mode A emergency codes (i.e. 7700 general emergency, 7600 communications failure and 7500 unlawful interference). Emergency modes shall be used and displayed by the system in the same way as the present case. It should be noted that some of the current avionics systems are only capable of transmitting an ‘emergency’ indicator. However whenever the capability for the pilot to select discrete emergency codes is present, the system shall be able to transmit the appropriate discrete emergency modes.

The same procedures for the failure of an aircraft transponder are required as for SSR-based services in airspace where transponder equipage is mandatory.

Procedures in the event of a complete failure of the WAM sub-system (in the WAM SOLE MEANS scenario) will be the same as procedures for SSR equipment failure (for an example of such procedures, see EUROCONTROL document “Operational Elementary and Enhanced Surveillance“ by the Mode-S Task Force Sections 7.5.3 and 7.5.4). Where any commonly accepted procedural aspects become a mitigating factor for the effect of a complete failure of the surveillance function, they are identified in the External Mitigation Means.

In situations where more than one data link type operation is supported within the surveillance environment (e.g. WAM and ADS-B), the complete failure of one of these links (but not the others) may also need to be considered. Within this analysis, the failure of the WAM sub-system is considered. Failure of other systems defaults the overall architecture to the “WAM only” case. See the functional architecture diagrams in Annex K for more details.

Sector Boundaries

It was noted during the analysis that some hazards may be specific to sector-sector transfer of aircraft (or appearance of aircraft in a sector during the climb). In particular, the severity of the hazard may increase due to the controller not having previously positively identified the aircraft.

This was taken into account when defining the worst credible effect for each hazard (i.e. the possibility of effects at the sector boundary were examined).

Abnormal Modes

In general, the abnormal modes to be identified during the Functional Hazard Analysis will conform to those apparent during ATC surveillance today using radar control. Differences that do exist between the operations and functions available from radar, ADS-B or WAM are outlined through the Preliminary System Safety Assessment, and their abnormal modes or hazards arising are examined.

Use of Procedural Separation During Abnormal Modes

A critical characteristic of the operational description used in this safety case is the method of fallback used in case of loss of surveillance data.

In general, the fallback modes used in this safety case conform to those apparent in current ATC radar-based surveillance. It is therefore assumed that any equipment failure of service degradation (including for individual aircraft) must be recognised in the same time frame as for radar equipment failures today, such that reversion to the appropriate fallback mode can be achieved safely [ASSUMP04].

The quality of the overall surveillance picture presented will be continuously monitored by the system and performance indicators presented to the supporting technical staff. When this quality drops below a given standard (e.g. due to a degradation in ground station performance or a planned outage), the data will be considered as of insufficient quality to meet requirements and current procedures will apply.

These procedures are specific to local environments but may include: extrapolating the last “good quality” position data for a set amount of time; removing all data from the display and moving to procedural control.

Although it is assumed that the performance of the system will be as good as or better than the reference environment (in terms of system capabilities), during certain abnormal modes the controller may be required to fall back to procedural separation. It is then important to note that this OSED assumes that the existing navigational infrastructure does not change following the implementation of WAM.

An issue was identified during this safety case of the ability of the controller to manage a high density traffic scenario if data on all aircraft was lost. Therefore, the following conditions were agreed:

- FHA14 – the controller is able to safely revert to procedural separation (for the affected aircraft) in the case of a continuous loss of all data for one aircraft;
- FHA15 – the controller is not able to safely revert to procedural separation in the case of a sudden continuous loss of all data for all aircraft (in the high density environment). However, in the case of loss of altitude data for all aircraft, it is assumed that controller may safely revert to procedural separation.
- Note that the “more than one” aircraft case is included in the consideration of hazards affecting “all aircraft” (as the worst cases will be similar).

E.3 Environment Definition

The following section provides details about the environment within which the surveillance application will be applied. The level of granularity of the description balances the need to provide enough guidance to enable an adequate safety and performance assessment to be conducted, without over-prescribing the environment in such a way as to unnecessarily restrict implementation options and impose excessive requirements.

At this stage, there is no distinction made between surveillance sources for the environment in question. Section E.5 contains a breakdown of the possible scenarios for the introduction of WAM sub-systems into the airspace of interest (with various combinations of existing surveillance infrastructure).

There is thought to be no difference between en-route and TMA operational applications; for these environments, the actual surveillance coverage and performances shall be in accordance with the EUROCONTROL Standard for Radar Surveillance in en-route and Major Terminal Areas. This standard defines the required surveillance coverage in both Major Terminal Area and en-route airspace; it specifies that both areas must be covered by duplicated SSR in addition to PSR coverage in Major Terminal Areas. The coverage must be structured in order to provide a continuity of surveillance service for provision of a separation service across all airspace divisions (and remain in accordance with local requirements); including between en-route and Terminal areas.

For the safety assessment, there is a need to understand:

- the current (pre-implementation) environment and;
- the environment post-implementation, known as the target environment.

Current Environment

As this document is concerned with the operational deployment of WAM for surveillance in a radar-like environment, the definition of a typical radar coverage area is useful. *This environment definition is not used directly during the safety requirement development process*; however it does provide the process with an appreciation of the changes that may be required within the environment to achieve benefits through implementing WAM. Definition of the current environments is provided in Table 9.

Target Environment

The definition of the post-implementation environment will be used during the safety requirements derivation process, and in particular the FHA. In conducting a hazard analysis the target environment is used to determine the severity of hazards taking into account any available environment mitigations.

The target environment will also be used for the derivation of performance requirements for the overall system, and the WAM sub-system in particular. In order to accomplish this, it will be in line with the 'EUROCONTROL Standard for Radar Surveillance in En-route and Major Terminal Areas [8] requirements for surveillance system performances.

Target Environment Components

This section outlines the generic environment into which the surveillance service (using the WAM concept) will be introduced. Where these assumptions have a specific impact upon the Safety Assessment, the reference to Annex F is given.

Operational and airspace characteristics:

- All airspace classifications are to be included. It is assumed that for airspaces with mixed VFR and IFR traffic, current roles and operational procedures apply [ASSUMP02]. Thus transponder equipage will be mandatory in the target environment where transponders are mandatory today for SSR and/or ADS-B surveillance [ASSUMP07]. *(as defined in section 8.5 of PANS-ATM with the procedures for handling aircraft between radar and non-radar airspace detailed in 10.4.2.5);*
- ATS services included are: Air Traffic Control Service, Flight Information Service and Alerting Service; *(for PANS-ATM function references please refer to paragraph 0 of this document).*
- Separation method (and minima): ICAO-standard - Vertical: 1000 ft and Lateral: 3NM or 5 NM (2.5 NM under certain conditions) [ASSUMP13]; for radar controlled airspace*, (Sections 8.7.2, 8.7.3 and 8.7.4 of PANS-ATM)*. By comparison those standards applicable to non-radar airspace are greatly increased *(they are described in sections 5.4.1 and 5.4.2 of PANS-ATM in terms of time as well as distance).*
- Vectoring (ATC responsibility for navigation of the aircraft) *(as defined in section 8.6.5 of PANS-ATM);*
- FIS: Surveillance might be required, but coverage requirement not as stringent as for ATC-use *(as defined in section 9.1 of PANS-ATM);*
- Alerting: same requirement as for current SSR environment *(as defined in section 9.2 of PANS-ATM; Notification of rescue co-ordination centres,*

Sections 7.1.2.1, 9.2.1.1, 9.2.2, 11.4.1 and 15.1.3, Plotting of aircraft in a state of emergency, Sections 9.2.1, 11.4.1 and 15.1.2.;

- Air Traffic Advisories: same requirement as for current SSR environment *(as defined in section 9.1.4 of PANS-ATM)*;
- Flexible Use of Airspace: same requirement as for current SSR environment *(as defined in sections 3.1.5 and 8.6.5 of PANS-ATM)*;
- Airspace structure and complexity: same requirement as for current SSR environment *(as defined in sections 2.6.2, 8.6.5 and 10.4.1 of PANS-ATM)*;
- Route configuration and complexity: same requirement as for current SSR environment *(as defined in sections 8.9, 8.10 and 8.11 of PANS-ATM)*.

Traffic characteristics:

- Per sector (en-route): average sector flight length, average flights per hour, and traffic numbers in sector: same environment as for SSR. *Some quantitative examples have been created for the safety analysis – these are shown in the Environmental Conditions below;*
- Aircraft mix: same environment as for SSR (as far as transponder-mandatory considerations are concerned) [ASSUMP07, ASSUMP15].

CNS infrastructure (capabilities and performance):

- ATS communications (controller/controller): same requirement as for current SSR environment [ASSUMP10] *(as defined in section 8.3 of PANS-ATM)*;
- Navigation: same requirement as for current SSR environment *(as defined in section 8.6.6 of PANS-ATM)*;
- Ground systems functions (e.g. FDP: same requirement as for current SSR environment; surveillance data tracker: must be able to process WAM-data, and the WAM data must therefore be interoperable [ASSUMP09]) *(as defined in section 8.10.2 of PANS-ATM)*;
- ATC tools: a Short Term Conflict Alert tool (STCA) and Minimum Safe Altitude Warning (MSAW) will be present in the environment, as in the current SSR environment. Any further definition of tools will be part of the mitigation identification in the safety case derivation *(as defined in section 15.6.2 of PANS-ATM)*;
- Airborne Safety Nets (ACAS): WAM has not degraded ACAS functionality *(as defined in section 15.6.3 of PANS-ATM)*.
- SSR will be used as a baseline as:
  - SSR, ADS-B and WAM require similar onboard equipment (in terms of 1090MHz transponder, and supporting data registers) and adhere to similar standards *(The standards for SSR are defined in sections 8.1-8.5 and section 8.8 of PANS-ATM; ED-126/DO-303 defines the ADS-B standard; standards for WAM are not yet available)*;

- The performance of WAM-derived surveillance data is assumed to be equal to (or better than) SSR radar (verification of this assumption is critical) [ASSUMP 14];
- Differences in the performance characteristics for these surveillance technologies are minimal for the purposes of the end user application. For further details, refer to the SASP paper, prepared by Austro Control, undertaking a comparative assessment of SSR, ADS-B and MLAT (presented at the ICAO SASP-WG/WHL/10) [7].

E.4 Specific Environmental Conditions used in Safety Assessment

The table below shows the specific Environmental Conditions used in the Safety Assessment. Some of these ECs affect the likelihood of hazards (such as corrupted data on the CWP) developing into effects (such as workload increase) which lead to the assignment of a particular severity and corresponding safety objective. Such ECs can be regarded as barriers (or mitigation means) used for the derivation of the Severities and Safety Objectives. If they are used in the assessment, then they are necessary to achieve the SO, and therefore become Safety Requirements. The specific ECs identified in a local safety case, should be captured as Safety Requirements to ensure the Safety Assessment is valid.

For the purposes of this example assessment, they act as a guideline to the implementer of the key elements of the environment that may impact upon the Functional Hazard Analysis.

Environmental Condition	Environmental Condition
ASSUMP03	The capabilities arising from Mode A/C surveillance are the default level that can be assumed for the airborne domain.
ASSUMP08	Traffic conditions for the ENR airspace are: Average duration of a flight in the sector = 20 minutes Average number of aircraft managed per ATSU hour = 45 Maximum instantaneous count of traffic = 20 aircraft Average traffic in the sector = 15 aircraft.
ASSUMP09	Traffic conditions for the TMA airspace are: Average duration of a flight in the sector = 10 minutes Average number of aircraft managed per ATSU hour = 40 Maximum instantaneous count of traffic = 15 aircraft Average traffic in the sector = 7 aircraft.
ASSUMP10	Direct R/T is available to the controller and flight crew in the airspace being considered
ASSUMP11	Flight strips are maintained for all aircraft at all times to ensure that all the information usually displayed on the screen is retained by the controller for all aircraft. There is a fallback system which provides a basic static list of aircraft data should something else fail; this only helps in the short timeframe after a hazard occurs (after which the list becomes useless as it is out of date).

ASSUMP12	Controllers will always retain some level of 'mental' picture regardless of the amount of information lost as a result of flight strips being retained and used as required. The increased use of such strips will however increase controller workload
ASSUMP13	The controller is applying the minimum separation standard applicable for the airspace (e.g. 5NM en-route, 3NM in TMA)

Table 6: Environmental Conditions (EC)

These environmental conditions are replicated as assumptions in the summary provided in Annex F.

E.5 Discussion on Alternative Scenarios

E.5.1 Identification of Scenarios

This section discusses the various scenarios that could be addressed by the implementer, and provides details of the current environment(s) to which they apply as well as the foreseen target environments.

The basis used for this scenario definition is the operational service and environment description described above.

Considering the focus is on radar airspace, relevant surveillance technologies for the baseline situation for WAM introduction are:

- PSR;
- SSR;
- ADS-B.

These technologies are available either as stand-alone or combination systems. Nominally, the immediately obvious scenarios are

- Addition of WAM to the baselines listed, or;
- Replacement of the baseline by WAM (i.e. WAM sole means).

A more exhaustive consideration of these scenarios confirms this simple view and is set out in Appendix 1 to the current Annex.

The most demanding scenario is WAM sole means and that is the scenario which is developed further.

E.5.2 Use of Aircraft Transponders

A WAM sub-system providing surveillance will be expected to provide at least equivalent levels of reliability, availability and integrity to radar ground sensors.

The same applies to aircraft transponders as they are the same transponders used for an SSR/ADS-B environment. However, in cases where there are slight differences identified between SSR and ADS-B compared to WAM, they will be addressed in the safety assessment.

The flight crew should be able to check the aircraft identification information set on board and subsequently transmitted by the transponder.

Different transponders have differences in timing accuracy, but this is dependent on the make, model and maintenance rather than the mode the transponder is set to (A/C as opposed to S). Such differences will produce a small variance in achieved position accuracies that are entirely dependant upon the transponder equipage because of the varying round trip processing times from initial SSR interrogation to the broadcasting of the reply. This effect is usually constrained by regulators mandating international standards to which transponder equipped aircraft must adhere to in order to place accuracy limits uniformly across all aircraft flying in a given section of airspace.

The barometric altitude (Mode C) broadcast by the transponder depends upon the accuracy of the onboard instrumentation, whereas the geometric altitude determined by WAM sub-systems relies upon the accuracy and consistency of the timing within the system. Geometric altitude is not used operationally, and is therefore not considered within this safety assessment.

Where the pilot is unable to amend the aircraft identification, then ground-ground coordination procedures will ensure the error is communicated to all concerned parties.

In addition to using the aircraft ID, the IDENT (i.e. SPI) feature is also required by the proposed procedures. There is no change to existing transponder operation procedures as defined for SSR, including handling of SPI.

In regards to altitude information, WAM merely introduces a new transfer medium (or a new reception method of old transfer mediums) and not a new source of data, as such it is expected that verification of the barometric flight level provided by WAM will be the same as for current verification procedures for use of radar.

E.5.3 Technology Considerations – General

The WAM application shall provide controllers with the same facilities and control benefits[4] to those available from SSR radar with potentially better coverage and update rates. Consequently, the intention is that the principles of operation using radar information are maintained for WAM use.

[4] Although geometric vertical position can be calculated by the WAM sub-system, it is not thought that this would be used operationally. In the future, it may be used by the system as an integrity check of Mode C barometric altitude.

Nevertheless, to assess the safety of WAM sub-systems, different system architectures, as produced by different WAM providers, need to be taken into account. The main difference that needs to be addressed is the methodology used for time stamping reception of relevant signals broadcast by the aircraft's transponder.

E.5.3.1 Determining the Time Difference Of Arrival (TDOA)

Multilateration derives the position of a target by determining the TDOA of a given signal, broadcast by the target, at the various ground stations. Commonality in time reference used throughout the receiver chain is therefore required for the signals to be directly comparable.

The TDOA can be determined either by comparing the absolute time of arrival (TOA) of the signal at the various ground stations or by directly cross correlating the relative signal times.

The architecture dependent methods of processing the signal times are given in Table 7 below [20].

Cross correlation systems	TOA systems
1. A series of correlations are performed on the same signal received from *pairs* of sites. 2. Ambiguous or erroneous results obtained by using signal cross correlation are minimised by using algorithms to sort and categorise the time differences centrally to the system. 3. These systems are used when the signal has a well defined pulse edge, such as those generated in SSR signals.	1. The TOA of a signal local to the receiver is recorded. 2. The SSR codes contained within it are decoded 3. The TOA of signals from a given aircraft transmission are then correlated (or grouped) together *across the system* to calculate the TDOA of the signal at the various ground stations.

Table 7: The methods of processing signal times to determine the TDOA

For both systems TDOA algorithms calculate the coordinates of the target from the TDOA input (either from the time difference in arrival from pairs of stations or directly from absolute timings).

E.5.3.2 Synchronising the Receivers

Synchronisation is defined as the method by which the digitisation processes of the received signals at each site are tied together. Digitisation time stamps the signal, however its true time of arrival at a ground station is determined by allowing for the time it takes for signal to be digitised (which must be known). Two principal methods of synchronising the receivers exist using either a distributed or common clock system. These are outlined in Table 8 (Source: WAM: Report on EATMP TRS 131/04 Version 1.1, August 2005, Produced by EUROCONTROL by Roke Manor Research, HITT Traffic and the National Aerospace Laboratory of the Netherlands Section 3 [8]).

Common clock systems	**Accuracy**	**Baseline**	**Link Choice**	**Line of sight (mast required)**
	Medium	Medium	Microwave Fibre	Yes–high mast required No
A central processing site holds both the system clock and the bulk of the processing complexity. The RF signals are received at the ground stations and rebroadcast on a custom analogue signal (typically over a single hop microwave link or using a dedicated optical fibre) to the central processing site where digitisation, synchronisation and subsequent processing take place. Accurate knowledge of the long delay time between initial remote RF reception and central digitisation for every receiver station is required. The longer the delay the greater the inherent environmental inaccuracies in such a system (which vary as a fraction of the total). Therefore the central processing site has to be geographically situated at the centre of the system to minimise the distances involved however only low levels of power are needed at the remote receiver stations.				
Distributed Clock system				
The receiver down-converts, digitises, and measures the time of arrival of the signal before extracting the code contained within it. The TOA and message code is then transmitted to the processing site from each receiver over a digital data link where correlation and tracking of the target take place. Although a method for synchronising the remote clocks is required, no geographical constrains apply to the location of the central processing site.				
Reference transponder transmission passes through the receiver chain that a SSR transmission would pass along introducing a common delay that cancels out any local bias. Multiple transponders may be used providing every pair of sensors can be linked to every other pair by means of common references.	Medium	Medium	Any	Yes- high mast required
Standalone Global Navigation Satellite System (GNSS) providing a highly accurate external common timing reference, (if using a GPS disciplined oscillator at each site), the integrity of which depends on the integrity of the receiver at the remote and central processing ground stations.	Low-Medium	Any – global system.	Any	No
Common view GNSS Synchronised System Use GNSS satellites that are in full view of all receivers and calculated differential data produces a common relative timing between all signals to achieve sub-nanosecond accuracies. No GNSS receiver is required at the central processing site as the data has been captured at the sensors. This system facilitates the checking of its own integrity.	High	Any – when constellation in full view of all receivers.	Any	No

Table 8: Common and distributed clock systems

Defining ‘accuracy’ is complicated as it is often difficult to distinguish between short term noise, long term drift, and random/systematic errors. For the purposes of the table above the accuracy level is defined in terms of timing precision (the degree to which we can be assured of a given signal being received) as:

- Low; worse than 20ns;
- Medium: 2-20ns;
- High: better than 2ns.

The baseline is typically defined as the spacing between adjacent receiver stations.

Other issues may need to be considered when assessing the differences between the system architectures including those relating to the reliability and the interface. Some key notes in this respect include:

- The data used in a given WAM sub-system is assumed to be completely interoperable with its surrounding environment.
- The combination of common and distributed clock receivers into a combined single system is not considered due to the fundamental differences.
- The combination of different receivers in a distributed clock system, is potentially possible although is not considered as the reference time against which the TOAs are measured would need to be converted to one standard before a TDOA could be calculated.
- The combination of different distributed clock systems is feasible in principle, although differences in the digitisation time base used and accuracy offered could make this a difficult task in practice and so is not considered.

APPENDIX 1 to ANNEX E

DETAILED CONSIDERATION OF SCENARIOS

Conceivable Baseline Scenarios

In the matrix below, conceivable baseline scenarios are defined, based on credible options:

	PSR	SSR	ADS-B
Single layer only	PSR only	SSR only	ADS-B only
PSR	Dual layer PSR	PSR + SSR	PSR + ADS-B
SSR		Dual layer SSR	SSR + ADS-B
ADS-B			Dual layer ADS-B

Table 9: Identified baseline surveillance scenarios

Surveillance in core area Europe utilising only PSR is not considered credible; scenarios that involve this method of surveillance are therefore shaded out in blue in the first column of Table 9.

ADS-B represents one possible layer of surveillance; although there may be a requirement for redundancy in this layer, a dual ADS-B layer is not considered realistic; this scenario is therefore also shaded in blue in Table 9.

This leads to the following relevant baseline (current) environments:

- Single layer SSR;
- Dual layer SSR;
- SSR + PSR;
- ADS-B sole means;
- ADS-B + SSR;
- ADS-B + PSR.

Target Environments

Regarding potential target environments, WAM can be introduced as an additional surveillance layer or as a replacement of an existing layer. Taking into account that implementing WAM as an additional surveillance layer in an environment where there are already two surveillance layers available will not lead to safety-critical requirements, the following matrix presents the rationale behind applicable scenarios:

Current environment	Target environment
Replacement of existing surveillance layer by WAM	
Single layer SSR	WAM sole means as replacement of SSR
Dual SSR layer	SSR + WAM
PSR + SSR	PSR + WAM SSR + WAM
ADS-B sole means	Not considered: termination of available ADS-B function when expanding to WAM is not considered likely.
ADS-B + SSR	WAM + ADS-B WAM + SSR not considered as termination of ADS-B function when expanding to WAM is not considered likely.
ADS-B + PSR	WAM + ADS-B WAM + PSR not considered as termination of ADS-B function when expanding to WAM is not considered likely.
Addition of WAM surveillance layer	
Single layer SSR	WAM + SSR
Dual layer SSR	Not considered: a triple surveillance layer is not considered safety critical
SSR + PSR	Not considered: a triple surveillance layer is not considered safety critical
ADS-B sole means	WAM + ADS-B
ADS-B + SSR	Not considered: a triple surveillance layer is not considered safety critical
ADS-B + PSR	Not considered: a triple surveillance layer is not considered safety critical

Table 10: Potential future surveillance scenarios

Based on the matrix above, the following scenarios could be considered:

- WAM sole means as replacement for single SSR;
- WAM in combination with SSR; either with a single SSR or as a replacement to existing SSR or PSR in a dual layer environment.
- WAM in combination with PSR, as a replacement to SSR in a dual layer environment.
- WAM in combination with ADS-B: either with ADS-B only (no radars previously present), or as a replacement to existing SSR or PSR in a dual layer environment.

It should be noted that a single WAM layer can be implemented with significant levels of redundancy, in central processors, ground sensors and data link communications.

There is also a choice of a passive or active WAM sub-system, where active entails interrogation of the aircraft. Given that the assumption is that Mode A/C transponders are the baseline equipage, interrogation will be necessary to obtain identity and pressure altitude. Interrogator failures are therefore considered in each scenario. (Note that the interrogator function may not be within the WAM sub-system – the interrogator may be part of an SSR, if this can be shown to induce the required signals from the aircraft for WAM to meet safety and performance requirements).

In addition to the scenarios derived above, replacement of a single or dual layer of SSR by WAM + ADS-B is considered relevant. A ‘replacement’ surveillance layer is considered to cover the same area as the previous layer, an ‘addition’ is considered to meet or improve the surveillance coverage.

Therefore, the four relevant target environments are:

- **WAM SOLE MEANS** assumes WAM data is correlated by a surveillance data processor, and presented to the ATCo.
- **WAM & PSR** assumes WAM data is fused to PSR data, and a combined position symbol is presented to the ATCo.
- **WAM & SSR** assumes WAM data is fused to SSR data, and a combined position symbol is presented to the ATCo.
- **WAM & ADS-B** assumes WAM data is fused to ADS-B data, and a combined position symbol is presented to the ATCo.

The capabilities of the surveillance technologies under consideration are outlined in the table below.

Data type	Data transmitted by aircraft	PSR	SSR	ADS-B
2D position	(n/a)	X	X	X
Altitude	Mode C		X	X
Identity	Mode A		X	X
	24-bit address		X (Mode S only)	X
	Aircraft identification		X (Mode S only)	X
Flight/Aircraft information	Enhanced surveillance		X (Mode S only)	X

Table 11: Summary of technology capability

- The squitter contains information relating to the track history, ground speed, magnetic heading, indicated air speed, vertical rate and selected altitude and also provides information used in a climb and descent indicator.
- It is assumed that for the TMA and en-route airspace being examined, an interrogator is a default part of the architecture.
- Where a system is composed of two methods of surveillance that operate in parallel, (producing data that is fused together), the system has a layer of redundancy built into it. For example in the WAM & ADS-B surveillance system a failure in the WAM sub-system alone (resulting in loss of WAM based surveillance) may not degrade the overall level of surveillance (as shown by the table above). Evidently, the surveillance performance levels may change. WAM-SOLE MEANS does not provide this mitigation measure.
- When a failure in a dual system results in inconsistent data then it has become corrupted. If all targets under surveillance are affected by the same inconsistency to the same extent this may not present an immediate risk to safety.

Notes on scenarios

In the WAM + ADS-B scenario, it is envisaged that ADS-B will be used to communicate both the position of the aircraft and other data relating to it (such as the call sign and other aircraft derived data); ADS-B will not be just backing up WAM SOLE MEANS derived position but will actively provide additional data to augment its surveillance capability. This leads to two streams of data (position and other information) provided as input to the tracker, from WAM and ADS-B.

It is recognised that Mode S has enhancements over Mode A/C, although in practice the two variants of SSR are used together for the same applications. Operational experience gained indicates that the differentiating features are not significant for the construction of a separate safety case. As such, they are treated as the more generic “Secondary Surveillance Radar” in this OSED.

The make, model and manufacturer of the airborne and ground station equipment employed may influence the accuracy of the derived position for WAM; when undertaking the PSSA, care must be taken to represent a credible set of architectures and scenarios for each of these target environments (see section E.5.3.2 for examples of different architectures).

Scenario Justification

When examining each scenario, it is useful not only to understand the functional description, but also the expected objective behind its introduction.

The table below shows the expected objectives (benefits) for the four target scenarios. The table has been colour coded to categorise the benefits:

- Dark grey: benefits **common** between target environments
- Light grey: **different benefits** between various different target environments.

Current Environment	Scenario	Safety benefits	Capacity/efficiency benefits	Cost-effectiveness benefits
	Target environment is WAM sole means			
Single layer SSR	Replacement of an SSR layer	Potential benefits due to higher update rates and extended coverage.	Possible benefit of variable magnitude *	Potentially cost-effective system, based on required coverage area. *Lower maintenance due to **no** moving parts*
	Target environment is WAM + SSR			
	Addition to SSR single layer	Redundancy of surveillance coverage.	Not necessarily (dependent on ***coverage area and standard improvement*** [5]) – relies upon the traffic level/route structure complexity)	No benefit
Dual layer SSR	Replacement of SSR layer	Potential benefits due to higher update rates and extended redundancy coverage		Potentially cost-effective system, based on required coverage area *Lower maintenance due to **fewer** moving parts.*
SSR + PSR	Replacement of PSR layer	Redundancy of coverage for functions other than position determination.	More aircraft information down linked to surveillance system (e.g. intent) may facilitate greater efficiency in the use of the airspace (in line with arguments made for EHS in core area Europe)	
	Target environment is WAM + PSR			
	Replacement of an SSR layer	Potential benefits due to higher update rates and extended redundancy coverage. ***Independent of transponder.***	Possible benefit of variable magnitude *	Potentially cost-effective system, based on required coverage area. *Lower maintenance due to **fewer** moving parts.*
	Target environment is WAM + ADS-B			
ADS-B Sole means	Addition to ADS-B sole means	Redundancy of surveillance coverage.	Improvement if different receivers are used to provide independent validation of position and increase quality of position.	Redundancy and improved quality at relatively low cost.
SSR + ADS-B	Replacement of SSR layer	Potential benefits due to higher update rates and extended redundancy coverage	No benefit	Potential cost effective system based on required coverage area. *Same ground stations (which require **no** moving parts and so require lower maintenance) can be used to provide both surveillance layers if system has adequate redundancy.*
PSR + ADS-B	Replacement of PSR layer	Redundancy of coverage for functions other than position determination.	More aircraft information down linked to surveillance system (e.g. intent) may facilitate greater efficiency in the use of the airspace(in line with arguments made for EHS in core area Europe)	

Table 12: Expected benefits for WAM scenarios

[5] The benefits depend upon the impact of extended squitter introduction (and possibly mode S capability if the previous SSR radar sub-system was limited to mode A/C) will depend on the usefulness of the additional information down linked vs. any additional frequency congestion.

F Assumptions and Conditions

F.1 Introduction

For convenience, and as a quick reference, this Annex gathers together all assumptions of any sort: operational assumptions, hazard related assumptions, environmental conditions, environmental mitigation means and PSSA assumptions. The tables also indicate where else in the document these various assumptions are explained.

F.2 Operational Assumptions and Environment Conditions

This table lists the Assumptions made in the Safety Assessment, and includes the Operational Assumptions and Environmental Conditions identified as a precursor to the safety assessment. Note that these assumptions must be validated in the Local Safety Case, and may become Safety Requirements.

ID	Assumptions	Section	Where explained
ASSUMP01	The ATC separation service is assumed to generate the most severe requirements on the system and human.	OSED & safety argument	3.2.1
ASSUMP02	The source of the surveillance data should not impact on the operational application in question (assuming it meets the required performances). The roles of the pilot and controller thus remain unchanged.	OSED & FHA	3.2.1 E2.2
ASSUMP03	It is assumed that the capabilities arising from Mode A/C surveillance are the minimum level of surveillance capability available to the controller. [note that the technical analysis in the example PSSA in Annex L assumes 90% Mode S, 10% Mode A/C – measured figures for the local environment should be used in the local Safety Case]	OSED	3.2.1 E.2.2 E.3
ASSUMP04	Any equipment failure or service degradation (including for individual aircraft) must be recognised in the same time frame as for radar equipment failures today, such that reversion to the appropriate fallback mode can be achieved safely.	OSED	3.2.2 E.2.2
ASSUMP05	Ground-ground interoperability requirements are unchanged	OSED	4.2
ASSUMP06	Any changes to ATCO procedures are assumed to be implemented within a specified coverage volume (see also ASSUMP17 below)	OSED	3.2.2 E.2.2

ASSUMP07	Transponder equipage will be mandatory in the target environment where transponders are mandatory today for SSR surveillance.	OSED	E.3
ASSUMP08	For en-route, the maximum instantaneous count of aircraft in the sector is 20 for TMA, the value is 15 aircraft. Average duration of a flight is 20 minutes for en-route (0.33 hours) and 10 minutes for TMA (0.167 hours). On average 45 aircraft are managed per hour in the en-route while over the same period 40 are managed in the TMA. This makes 1 Air Traffic Service Unit (ATSU) hour equal to approximately 7 flight hours in the TMA and 15 flight hours en-route.	OSED	3.3 E.4
ASSUMP09	The data used in a WAM sub-system is assumed to be interoperable with the surrounding ATM system.	OSED	E.3
ASSUMP10	Direct R/T is available in the airspace	OSED	E.4
ASSUMP11	Flight strips are maintained for all aircraft at all times to ensure that all the information usually displayed on the screen is retained by the controller for all aircraft. A fallback system provides a basic static list of aircraft data should something else fail; this only helps in the short timeframe after a hazard occurs (after which the list becomes useless as it is out of date).	OSED	E.4
ASSUMP12	Controllers will always retain some level of 'mental' picture regardless of the amount of information lost as a result of flight strips being retained and used as required. The increased use of such strips will however increase controller workload.	OSED	E.4
ASSUMP13	The controller is applying the minimum separation standard applicable for the airspace (e.g. 5NM en-route, 3NM in TMA)	OSED	E.4
ASSUMP14	The performance of WAM-derived surveillance data is assumed to be equal to (or better than) SSR radar	OSED	3.3 E.3
ASSUMP15	The aircraft mix is assumed to be the same as in a high density SSR environment (when considering transponder-mandatory requirements)	OSED	3.3 E.3
ASSUMP16	The implementer has validated each operational assumption	OSED	N.4.4
ASSUMP17	The WAM coverage map has been defined and the WAM sub-system has been validated against it.	OSED	4.3
ASSUMP18	It is assumed that the ground ATC system has filtering functions, such that if the data is outside the required performances (e.g. in terms of the latency requirements), and is detected as being such, it is not displayed and is therefore treated as lost.	OSED	Table 17 H.3.2

ASSUMP19	The WAM sub-system is capable of differentiating replies from aircraft with duplicated Mode A/S codes (including those that are closely spaced).	OSED	4.3
ASSUMP20	The probability of correct message decode is sufficient to meet the update rate requirements. (15-20% message decode probability is expected to be required for a system without WAM sensor redundancy.)	OSED	4.3

Table 13: Key assumptions used in this safety assessment

F.3 Functional Hazard Analysis – background "assumptions" used in assessment

This table contains a list of the background "assumptions" used to clarify the Functional Hazard Analysis (in particular, the controller assessment of hazard effects and severities). The entire table is repeated in Table 3: in section 5.3 in the main body of this assessment. More detailed explanation is given in the section referenced in the column "Where explained". They include the External Mitigation Means identified within the FHA.

ID	Assumptions	Section	Where explained
FHA01	There is an assumption that the worst credible effect for combinations of the data elements occurs when ALL data elements are affected	FHA	H.3.1
FHA02	If the controller detects the corruption, it is treated as loss (since the controller will not use the data).	FHA	Table 17 H.3.2
FHA03	The ground system includes some form of track extrapolation over a short time period (assumed to be 30 seconds, or approximately 3 updates, in the Fault Tree Analysis). Therefore the ground system knows that it has no new data and can alert the ATCO (for example by displaying the extrapolated position using different symbology). This enables the ATCO to prepare for the possible loss of displayed data after, typically, 3 extrapolated updates, i.e. 30 seconds.	FHA	Table 17 H.3.2 H.4.2.2
FHA04	It is assumed that the controller will detect lost data on the CWP 999 in 1000 times (i.e. there is a 0.1% chance that the loss of the data element will remain undetected long enough to cause a safety-related effect).	FHA	H.4.2.3 H.4.3
FHA05	It is assumed that, in the undetected case, the hazard lasts long enough for the worst credible effect to occur.	FHA	H.4.2.3 H.5.2

FHA06	It is assumed that the loss of call sign would mean it is replaced by the Mode A code (i.e. assumptions on the system are made in the fault tree analysis that Code-Call sign Correlation is available, and that standard reversion techniques are used). If Mode A code is lost, it is assumed that flight strips are maintained.	FHA	I.4 (severity classificati on tables)
FHA07	It is assumed (based on track structure, airspace complexity and traffic density) that for 1% of the time, aircraft will be in close enough proximity such that a separation-related effect will occur	FHA	H.5.2
FHA08	It is assumed that fusion is present in the ground data processor, such that the delivery of dual tracks for one aircraft to the controller will not occur.	FHA	H.3.2
FHA09 (EMM1)	It is assumed that the experience and ability of controllers is sufficient to enable them to identify that the failure has occurred.	FHA	H.3.2 Table 17
FHA10 (EMM2)	It is assumed that procedural control can be established by controllers in the event of loss of data for one aircraft. The procedures are available (PANS-ATM, ANSP Manuals of ATC), training is given to the controllers in the use of procedural control, and the aircraft can successfully apply procedural control operations (R/T is available to make voice position reports, and flight crew procedures exist (PANS-OPS)).	FHA	H.3.2 Table 17
FHA11 (EMM3)	It is assumed that the experience and ability of flight crew is sufficient to enable them to identify that something is not nominal.	FHA	H.3.2 Table 17
FHA12 (EMM4)	It is assumed that sector transfer procedures ensure that when an aircraft enters a sector, they contact the controller via R/T.	FHA	H.3.2 Table 17
FHA13 (EMM5)	It is assumed that procedural control when altitude data is missing is safe (through controller training, experience etc).	FHA	H.3.2 Table 17
FHA14	It is assumed that the controller is able safely to revert to procedural separation (for the affected aircraft) in the case of a continuous loss of all data for one aircraft (this also applies to individual data element loss).	OSED	3.2.2
FHA15	It is assumed that the controller is not able to safely revert to procedural separation in the case of a continuous loss of all data for all aircraft (in the high density environment). However, in the case of loss of altitude data for all aircraft, it is assumed that controller may safely revert to procedural separation.	OSED	3.2.2

Table 14: Functional Hazard Analysis – background assumptions

F.4 Example PSSA technical and operational specific conditions

This table highlights the technical and operational specific conditions which needed to be assumed to allow the example PSSA to be carried out. They should not be taken as formal "assumptions" (as in section F.1 above), but as example conditions that may become safety requirements in the Local Safety Case, subject to validation.

This table is a synthesis of the unique PSSA conditions identified in section L.2, Table 30.

ID	Conditions	Section	Where explained
PSSA01	It is assumed the WAM sub-system has been successfully implemented and meets operational requirements when it is operating correctly. In other words, the system has the required operational coverage with the necessary performance validated throughout the operational area (e.g. by flight tests).	PSSA	Table 30
PSSA02	Any other surveillance sub-systems are correctly specified and implemented properly (e.g. no holes in coverage). See also ASSUMP06 and ASSUMP17.	PSSA	Table 30
PSSA03	If the WAM interrogator suffers a detected failure, it is assumed the WAM sub-system shuts down (since it could not guarantee to detect Mode A/C aircraft).	PSSA	Table 30
PSSA04	Conversion to/from local WAM co-ordinates to the tracker co-ordinates is assumed to be implemented correctly.	PSSA	Table 30
PSSA05	A minimal sub-system architecture is assumed (i.e. one that comprises of the fewest possible number of components to meet basic operational requirements). This assumption implies that the failure of, e.g., any WAM sensor or sensor to CP data link will cause surveillance information relating to a target to be lost. It is assumed that only the minimum number of ground sensors required to meet the operational coverage are present.	PSSA	Table 30
PSSA06	It is assumed traffic includes commercial and GA aircraft entering controlled airspace or requiring a separation service. Of them 90% are assumed to be Mode S equipped.	PSSA	Table 30

PSSA07	It is assumed that no system track monitor is present that raises an alarm if one or more tracks or data items should 'disappear' or show inconsistent data (such as a large jump in position). This reflects expert opinion on the assumptions that can be made for a typical surveillance sub-system.	PSSA	Table 31
PSSA08	It is assumed the tracker can accommodate a changed Mode A code during flight whilst keeping the correct aircraft identity. If the technical address (Mode A or 24-bit address) changes in an unpredictable way the tracker will raise an alert to the controller (e.g. by starting a new track with the new Mode A code and by coasting the old one).	PSSA	Table 31
PSSA09	It is assumed the tracker can process targets with duplicate Mode A or S codes in the same airspace (as long as the targets are distinguishable by the tracker). This is assumed to occur once every 100 ATSU hours.	PSSA	Table 31
PSSA10	It is assumed that an elliptical ranging function is present and is used to achieve the required position determination performance together with the TDOA method (how this is achieved by the elliptical ranging and the TDOA methods will vary depending on implementation). See Figure 17 below.	PSSA	Table 31
PSSA11	It is assumed that there exists a function to correlate flight plans with surveillance targets.	PSSA	Table 31
PSSA12	It is assumed a separate flight strip processing system is present and that it can continue to operate even if the tracker fails.	PSSA	Table 31
PSSA13	It is assumed that the WAM sub-system has a reference transponder that provides a health check function (i.e. checks that its transmissions can be received by the system) and/or time synchronisation function to the system at the sensors.	PSSA	Table 31
PSSA14	It is assumed the probability of a failure occurring is distributed equally over all elements that can cause this failure (e.g. the probability of a failure on board an aircraft is equally likely for all aircraft in the airspace [the principal of equal a priori]).	PSSA	Table 32
PSSA15	The probability of a component failure with time is an exponential decay function: Pr(once or more) = 1 – exp(-t/MTBF) Where the MTBF is the Mean Time Between Failures and t is time. (this assumes independent failures)	PSSA	Table 32

PSSA16	When calculating failure rates, it is assumed aircraft do not have a redundant transponder or antenna sub-system. Whilst many aircraft in fact do, it is known that failures of the transponder/antenna sub-system can remain undetected by the aircrew with the consequence that the redundant sub-system is not activated. Therefore no benefit is taken for the redundant sub-systems.	PSSA	Table 32
PSSA17	It is assumed that the MTBF used are constant with time (i.e. improved failure rates in the future are not considered).	PSSA	Table 32
PSSA18	Unavailability is formally defined as: $Q = 1 – (MTBF/(MTBF+MTTR))$ Where MTTR is the Mean Time To Repair of the component. All unavailabilities used in the fault trees are calculated for an operational hour of the Air Traffic Service Unit (ATSU).	PSSA	Table 32
PSSA19	It is assumed that a component is considered as failing if it is unavailable for 30 seconds or more (equivalent to 3 update periods on the CWP or the length of time an extrapolation function in the tracker might last for).	PSSA	Table 32
PSSA20	It is assumed the airborne transponder or antenna failure probability is 1E-4 per flight hour [17]. The MTTR is assumed to be the transit time in the sector (i.e. once the failure has occurred it continues for the duration of the flight in the sector but is fixed before the aircraft returns). This is a worst case since it assumes the failure occurs soon after or before entry to the sector.	PSSA	Table 33
PSSA21	Assumed to have the same failure probability as one airborne transponder (1E-4 per flight hour).	PSSA	Table 33
PSSA22	It is assumed that an airborne transponder failure from RF pollution is 100 times less likely than other possible transponder failures.	PSSA	Table 33
PSSA23	For transponders that lie within the surveillance coverage it is assumed that one every 1000 ATSU hours does not meet the ICAO specification.	PSSA	Table 33
PSSA24	It is assumed that the probability of the aircrew entering an incorrect mode A code is 1E-3 per entry. It is assumed that the Mode A code is set once per flight hour on average [18,17].	PSSA	Table 33

PSSA25	Incorrect decoding of a message may be due to overlapping messages, caused by multipath or FRUIT overload for example. [19] gives approximately 5% decoding probability for a single extended squitter at a 60 mile range in very high density airspace. In low density airspace this probability increases to an average of 15%. It is assumed that the generic surveillance environment is of medium density, so an average of these two figures is taken to give an average decoding probability of 10%. [Note that this requirement has been added to by safety recommendation Rec1, which increases the probability of decode to 15%].	PSSA	Table 33
PSSA26	It is assumed that the WAM interrogator can repeat an interrogation in 0.5s if no correctly decoded position is available from the previous interrogation.	PSSA	Table 33
PSSA27	It is assumed that for 10% of the flight duration [16] the aircraft are close enough to cause very closely spaced Mode A replies.	PSSA	Table 33
PSSA28	It is assumed that the probability of there being a duplicated 24 bit address present in the surveillance airspace is 1E-4 per flight [16].	PSSA	Table 33
PSSA29	Drawing upon operational experience based upon the Austro Control system the MTBF for the WAM interrogator was estimated to be 25000 ATSU hours (approximately three years). The MTTR is assumed to be 1 ATSU hour.	PSSA	Table 33
PSSA30	It is assumed that the failure probability and MTTR for each sensor is the same as that for the ground system interrogator.	PSSA	Table 33
PSSA31	Operational experience has shown the failure probability to be in the region of 1E-3 to 1E-4 per ATSU hour. A mid-way value of 5E-4 has been assumed. MTTR is assumed to be 1 ATSU hour.	PSSA	Table 33
PSSA32	It is assumed that other static ground system components, such as the tracker, SDP alarm, CWP and WAM central processor have a failure rate of 1E-5 per ATSU hour. The MTTR is assumed to be one ATSU hour.	PSSA	Table 33
PSSA33	It is assumed that the WAM timing sub-system has a failure rate of MTBF 1E-5 and MTTR of 1 hour.	PSSA	Table 33

Table 15: Example PSSA technical and operational specific conditions

G Approach to Identifying Safety Requirements (Failure Case)

G.1 EUROCONTROL Safety Assessment Methodology process (SAM)

The approach used to identify and justify the safety requirements, described in the safety argument under the failure case (abnormal operations) scenario, is based on the EUROCONTROL Safety Assessment Methodology (SAM) [3].

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.

This EUROCONTROL SAM process consists of three major steps as illustrated in Figure 9 [7]:

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

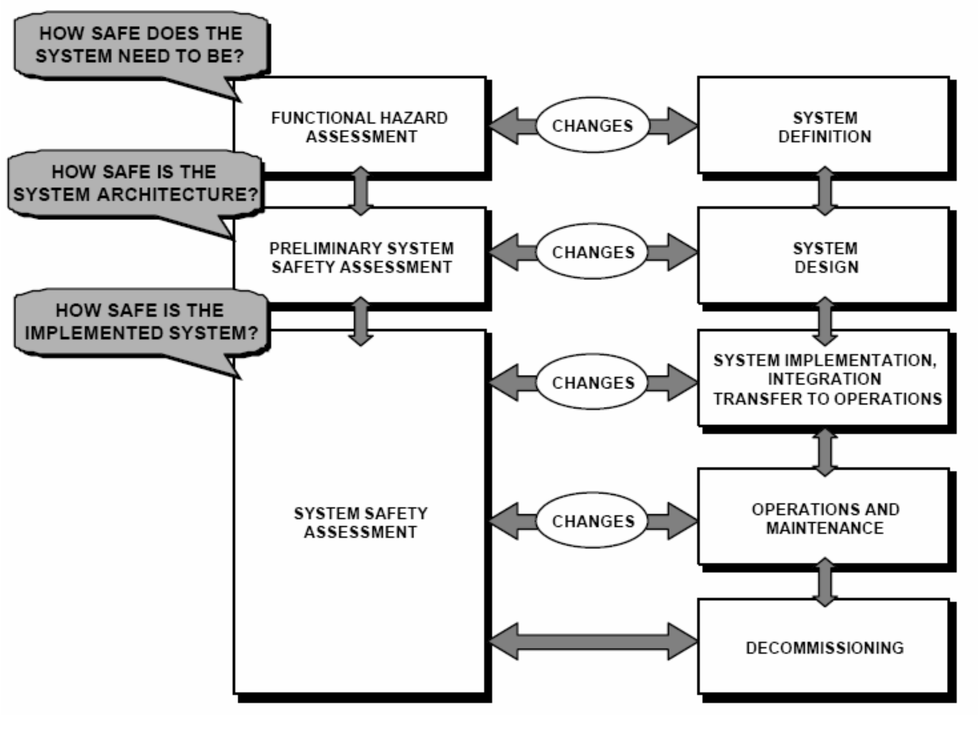

HOW SAFE DOES THE SYSTEM NEED TO BE?
FUNCTIONAL HAZARD ASSESSMENT
CHANGES
SYSTEM DEFINITION
HOW SAFE IS THE SYSTEM ARCHITECTURE?
PRELIMINARY SYSTEM SAFETY ASSESSMENT
CHANGES
SYSTEM DESIGN
HOW SAFE IS THE IMPLEMENTED SYSTEM?
CHANGES
SYSTEM IMPLEMENTATION, INTEGRATION TRANSFER TO OPERATIONS
SYSTEM SAFETY ASSESSMENT
CHANGES
OPERATIONS AND MAINTENANCE
DECOMMISSIONING

Figure 9: EUROCONTROL Safety Assessment Methodology

G.2 FHA

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

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.

The FHA for this project is described in this Annex H.

G.3 PSSA

The objective of performing a PSSA is to define, based on the safety objectives, a set of safety requirements[6] on the ATM system components so that they can reasonably be expected to achieve the Safety Objectives specified in the FHA. In this case, the ATM system components are those necessary to provide the data required to fulfil the ATC separation service under investigation. These components are detailed in the functional models, contained in Annex K.

The PSSA process apportions Safety Objectives into Safety Requirements allocated to the ATM surveillance sub-system elements.

This safety case developed a "bottom-up" model of the system, based on achievable failure rates, in order to develop the fault trees. This pragmatic approach ensured that no unachievable requirements were unnecessarily placed on existing equipment (e.g. trackers, transponders etc). However, where a higher requirement was thought necessary to meet the safety objective, this has been highlighted in the study.

The PSSA (or Fault Tree Analysis) for this project is described in Annex L.

G.4 SSA

The SSA is not performed in this Generic Safety Assessment.

G.5 "Bow-Tie" Model

This SAM process may be illustrated graphically in the "Bow-Tie" model, shown in Figure 10 below. Note that although this is similar to the full Bow-Tie model, the process did not include an iteration from the Fault Trees back to the Event Trees (in understanding whether a particular external mitigation will be effective), and is therefore not the full model.

[6] 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.

The process begins with the definition of the OSED, containing the application and environment description.

The FHA runs from the centre of the diagram to the right, as follows:

- Identify Potential Hazards: What could go wrong with the data at the boundary of the system (i.e. on the Controller Working Position) [A]
- Identify Potential Operational Effects: What is the consequence of the hazard and does it affect the safety of aircraft operations, given the presence of External Mitigation Means? [B]
- Assess Severity of the Hazardous Effects: How bad would those effects be, given the presence of External Mitigation Means? [C]
- Specify Safety Objectives: How often can we accept the hazard to occur? [D]

Note that each step also takes account of the Environmental Conditions (ECs), within which the application takes place. ECs do not always reduce the effects of a hazard (for example, high traffic density may increase the likelihood or severity of the effect).

It is also necessary to ensure that the specification of the safety objectives (and safety requirements arising from external mitigation means) is complete, coherent and consistent. Thus the FHA is verified and validated through an evaluation activity.

Following the setting of Safety Objectives (the result of the FHA process), the failures in the system (functional model) that could have resulted in each credible hazard are assessed. This is the PSSA process. The combinations of faults (i.e. basic causes) are used to calculate the overall achievable safety level in the Fault Trees. If this safety level does not meet the relevant Safety Objective, Internal Mitigation Means (IMMs) may need to be applied (for example, procedural mitigations, redundancy or fault detection).

The Safety Requirement per component of the system, the External Mitigation Means, and the Internal Mitigation Means are all captured as Safety Requirements. Where necessary, Environmental Conditions may also be written as Safety Requirements (for example, if the safety case depends upon the traffic density being less than a certain value).

The following acronyms are used in the diagram:

EMM	External Mitigation Means
FHA	Functional Hazard Assessment
IMM	Internal Mitigation Means
OE	Operational Effect

OSED	Operational Services and Environment Description
PSSA	Preliminary System Safety Assessment
Sev. *X*	Severity Classification (X=1, 2, 3, 4, 5)
SO	Safety Objective
ST	Safety Target (according to Target Level of Safety per severity of effect)

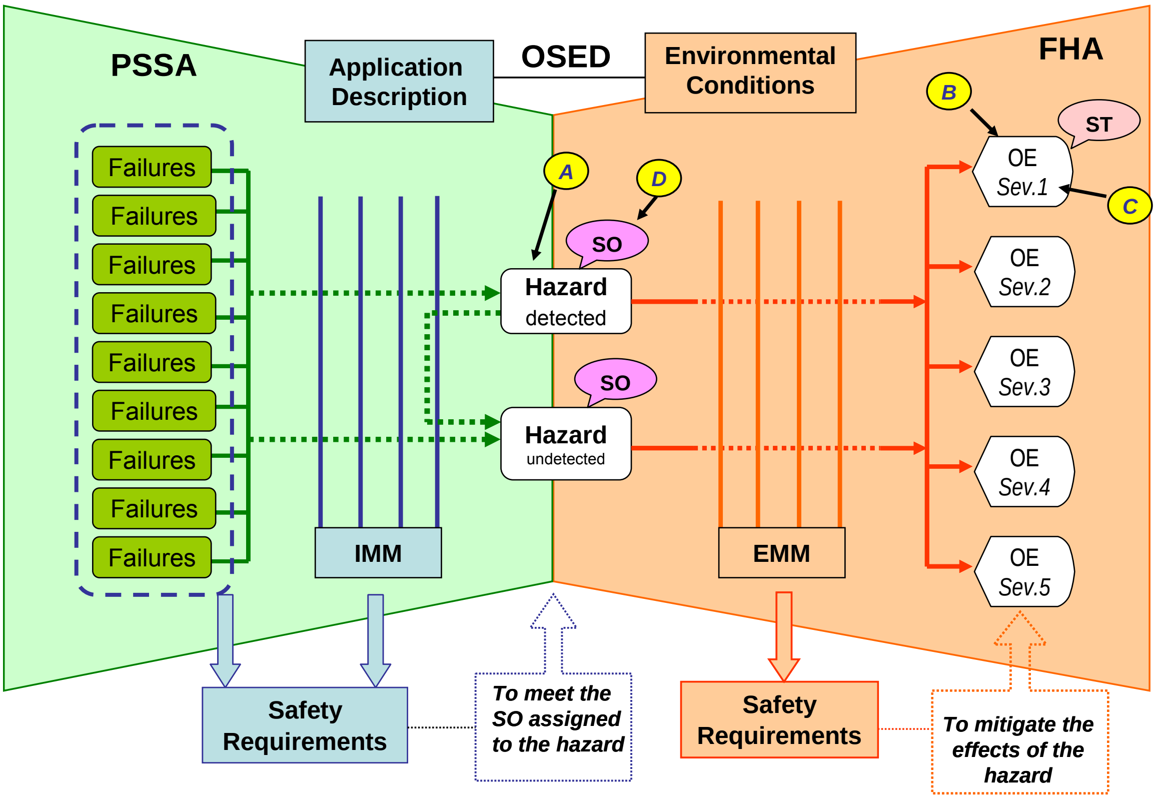


Figure 10: "Bow-Tie" Diagram (Figure 20 from ED-126)

H Generic Functional Hazard Assessment (FHA)

H.1 General

This annex contains the Functional Hazard Assessment (FHA) for the provision of an ATC service in en-route and TMA Airspace (focusing on the separation task).

It is intended to be independent of the source of the surveillance data used to provide the service – i.e. a core set of data is defined, which can feasibly be derived from a number of technology elements such as SSR, ADS-B, or Multilateration.

H.2 Target Levels of Safety and Risk Classification Schemes

H.2.1 Severity Classification Scheme

The Severity Classification Schemes contained in Annex J provide the basis for determining the severity of an effect for a particular hazard. These schemes are taken from ESARR 4 [5] and the EUROCONTROL Safety Assessment Methodology [3] respectively.

H.2.2 Risk Classification Scheme

A Risk Classification Scheme aims at setting the maximum contribution of an ATM system to accidents and incidents.

The purpose of the Risk Classification Scheme is therefore to set safety targets for the occurrence of each severity of hazard (based on its effects). The Safety Target specifies the overall maximum frequency of occurrence of any type of hazard having a given Severity Class whatever the ATM cause.

Thus a Severity 1 effect will be set a certain target probability of occurrence (safety target), with a Severity 2 effect setting a less severe target probability of occurrence (as the consequences of the hazard are judged to be less severe).

The Risk Classification Scheme (RCS) is defined for this Generic Safety Case using ED-125 [6]. ED-125 recommends a process for specifying a RCS, and deriving Safety Objectives in ATM, in compliance with ESARR 4 [5].

ED-125 specifies the use of an ECAC Regulator Safety Target as the starting point for the scheme. For Severity 1 effects, this is set by ESARR 4. For Severity 2, 3 and 4 effects, Safety Targets are set by ED-125 through consideration of data and expert judgement. Severity 5 hazards have no safety effect, and are therefore not considered.

A regulatory ambition factor (AF) is used in this safety case for Severity 1 effects, reflecting the fact that introducing a safety margin increases the confidence that the Safety Target will be actually met, as the target value is higher than the absolute requirement. This is useful given the uncertainty in operational application (due to the low amount of data available on Severity 1 incidents/accidents). ED-125 defines the minimum National Regulator Ambition Factor for Severity Class 1 as 1.55.

ED-125 also recommends that a minimum ambition factor of 10 should be applied to severities 2, 3 and 4 by the local ANSP. So as to set a representative Safety Target that would be used by an ANSP, this factor has been included in Table 16 below.[7]

Safety Target	ECAC Regulator Safety Target (/ flight hour)	Ambition Factor	Safety target (/ flight hour)	Acceptable event frequency per ANSP[8] (approx)
ST1	1.55×10^{-8}	1.55	1×10^{-8}	One event every 200 years
ST2	1×10^{-5}	10	1×10^{-6}	One event every 2 years
ST3	1×10^{-4}	10	1×10^{-5}	One event every 2 months
ST4	1×10^{-2}	10	1×10^{-3}	One event every day
ST5	n/a	n/a	n/a	n/a

Table 16: Risk Classification Scheme

H.3 Identification of Potential Hazards

H.3.1 Data Elements

The data elements being examined are:

- 2D position
- Altitude (pressure)
- Identification (call sign) (note that the Mode A code or the ICAO 24-bit aircraft address are assumed to be correlated with the flight plan call sign as part of the tracker function: namely, the Code-Call sign Correlation Database. In the event of no correlation, the Mode A code may be displayed).
- Short intent / history
- ALL

[7] The ambition factor is used to make the distinction between tolerable risk (Regulator's view) and acceptable risk (ANSP's view). The ANSP has no margin of error if applying only the tolerable risk value. This is explained more fully in ED-125.

[8] Frequency calculated using approximate flight hours per ANSP per year of 500,000

Assumption FHA01: There is an assumption that the worst credible effect for combinations of the data elements occurs when ALL data elements are affected. Hence for combinations of data element failures, only the ALL parameters case is considered.

Figure 11 shows the data elements, as they appear on a typical Controller Working Position (including an electronic flight information strip, which would normally appear on a separate display).

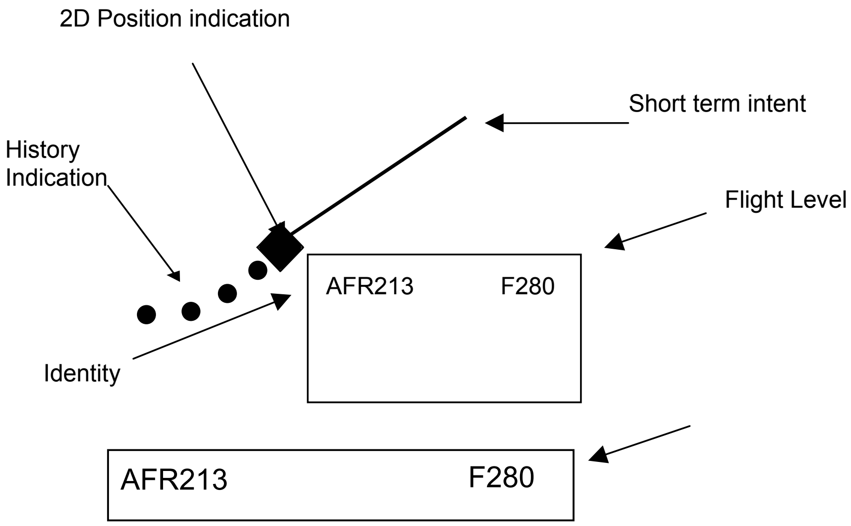


Figure 11: Track Label Augmented with Parameter Descriptions

H.3.2 Failure Modes (types of hazard)

In order to assess the hazards that may occur in the application with a degree of rigour, a series of failure modes are applied to the data elements identified above. These failure modes (types of hazard) are taken from guidelines for conducting an FHA in the EUROCONTROL SAM [3].

Note that hazards, and therefore failure modes, are assessed at the output of the system – i.e. at the Controller Working Position. Therefore, although the system may be carrying out filtering functions, only the result of these functions is assessed.

Within this hazard analysis, the actions of the controller do still impact the severities and effects; whether the hazard is detected or undetected by the controller is an important factor in the assessment of worst credible effect. However, the hazards themselves, being measured at the boundary of the system (i.e. the CWP), are independent of controller detection.

Table 17 shows the keywords, together with the justification of their treatment within this safety analysis.

Failure mode (hazard type)	Justification of treatment at operational level
Loss of data	Loss of data (at the CWP) results in the data disappearing from the screen (the track, label or flight information strip data, or all the above). Loss of data incorporates those occasions when the system filtering function removes the data due to it being outside the required performance parameters.
Misdirected data	i.e. data delivered to the wrong Controller Working Position. This situation is considered to be a subset of the loss of data (since the result at the operational controller's CWP is the same – no data), although note that different basic causes exist for misdirected data.
Corruption of data	Data corruption would result in an incorrect value for the data element being displayed on the CWP (the track, label or strip). If data is not updated (i.e. the screen freezes), the data is effectively out of date (i.e. corrupted). The controller is increasingly likely to detect corruption as the difference between the expected value and the corrupted value grows. Inconsistent, spurious and malicious data are treated as examples of data corruption. Note that delayed data, because it appears on the controllers display, is also treated as corrupted data. Assumption FHA02: if the controller detects the corruption, it is treated as loss (since the controller will not use the data).
Delayed data	i.e. data delivered after a longer period of time than operationally acceptable. In common with non-updated data, this can be regarded as a corruption of the data element. Note this is only to a certain point in time; the ground ATC system has filtering functions, such that if the data is outside the required performances (e.g. in this case, the latency requirements), it is not displayed and is therefore treated as lost. [ASSUMP18]
Spurious and malicious data	Spurious and malicious data may both be credible corruptions of the data, and can be treated as part of the "corrupted data" set.
Inconsistent data	For all other data elements than 2D position, it is assumed that one of the inconsistent values is lost, leading to a possible corruption of the displayed data element if an inaccurate value is shown. For 2D position, a further hazard occurs if a fusion algorithm is not present in the ground system. For the purposes of this generic safety

	case, it is assumed that fusion is present and dual tracks (i.e. the display of two plots for the same aircraft) is not a credible hazard [FHA08].

Table 17: All failure modes (hazard types) and justification of treatment

Therefore the Failure Modes can be consolidated into the following:

Failure Mode	Including:
Loss of Data	Misdirected Data, Delayed Data (over a certain threshold),
Corruption of Data (i.e. display of erroneous data)	Delayed Data (non-filtered), Inconsistent Data, Spurious and Malicious data

Table 18: Assessed failure modes

Loss or corruption of the data should be considered as separate hazards, as differing effects and probabilities may result in different Safety Objectives (particularly when undetected), with differing basic causes and fault trees.

H.3.3 Number of Aircraft Affected

In addition to these failure modes, hazards can be defined by the number of aircraft affected. Within this analysis, the cases of:

- one aircraft or
- all aircraft

have been considered [FHA14, FHA15]. Note that the “more than one” aircraft case is included in the consideration of hazards affecting “all aircraft” (as the worst cases will be similar). As we are sensor independent for this FHA, there are no qualifiers such as ‘All Mode S transponders’. The failures arising from solely Mode S transponders will impact the basic causes in the Fault Tree Analysis.

H.3.4 List of Possible Hazards

Using the types of hazard outlined above, we derive a list of possible hazards that may affect the surveillance sub-system, based on an analysis per data element. The list is shown in the Table 19 following (which is a slightly reorganised version of Table 2.

Note that controller detection is not yet considered in detail – however, the options for that particular hazard that were outlined in section 5.3.1 are repeated below. These are that:

- ➢ Undetected loss for many aircraft (for any parameters) is not considered credible.

- Detected corruption is treated the same as detected loss, as in both cases the controller will not use the data.

- Undetected corruption of all data items simultaneously is not considered credible.

Corruption of data is written in terms of the hazard it creates on the controller's CWP, which is the "display of erroneous data".

Hazards specific to the tracker are not assessed here and will need to be assessed in the local safety case. This assessment must cover such performance issues as availability, the track fusion function and the display of dual tracks.

Parameter	ID	Variant	Hazard – short description	Severity (worst credible case)
2D position or all parameters	H01	U1	Loss of 2D position (or of all parameters).	ER=3 TMA=2
		D1		4
		D-many		ER=3 TMA=2
	H02	U1	Display of erroneous 2D position (i.e. corruption of position)	ER=3 TMA=2
		U-many		ER=3 TMA=2
Pressure altitude	H03	U1	Loss of pressure altitude	5
		D1		4
		D-many		3
	H04	U1	Display of erroneous pressure altitude (i.e. corruption)	ER=3 TMA=2
		U-many		2
Aircraft ID / call sign	H05	U1	Loss of aircraft identity (Call sign)	5
		D1		4
		D-many		3
	H06	U1	Display of erroneous aircraft identity (Call sign) (i.e. corruption)	3
		U-many		2
Short intent	H07	All	Loss of, or display of erroneous, short intent	4

Table 19: List of possible hazards

H.4 Assessment of Potentially Hazardous Effects and Severities

H.4.1 Initial Assumptions

Having categorised the hazards likely to occur in the provision of surveillance to ATC to provide a separation service, the next step is to identify their consequences. The full results of this operational effects analysis are shown in the tables in Annex I, and provide traceability of the effects and severities chosen by operational experts.

Effects and their consequences depend on a number of environmental factors, captured as environmental conditions. Note that each of these conditions will need to be validated in the service providers' local environment.

The environmental conditions are necessary to enable the identified External Mitigation Means (summarised in Table 21). As mentioned in the OSED, a conservative assumption (ASSUMP06) was made in the context of this study that the use of procedural control was not applicable as a safe fallback mode in case of hazards affecting several (or all) aircraft (note that standard procedures such as radio contact on sector transfer still apply to the many aircraft case as an External Mitigation however).

The Environmental Conditions are defined in full in Table 6. A summary of these conditions is provided here:

- The capabilities arising from Mode A/C surveillance are the default level that can be assumed for the airborne domain (ASSUMP03)
- Traffic conditions for ENR and TMA are defined, with average number of aircraft managed per ATSU hour being 45 in en-route and 40 in the TMA (ASSUMP08)
- Direct R/T is available (ASSUMP10);
- Flight strips are maintained for all aircraft at all times (ASSUMP11);
- Controllers will retain some level of "mental" picture of the traffic (this cannot replace the CWP for all aircraft however) (ASSUMP12);
- The controller is applying the minimum separation standard applicable for the airspace (e.g. 5NM en-route, 3NM in TMA) (ASSUMP13).

H.4.2 Qualifiers for Effects of Hazard

H.4.2.1 Overview

For each type of hazard (failure mode), there is also a list of criteria which qualify the hazard (and affect the consequences arising):

- Exposure onset (sudden or progressive) and duration (short or continuous) – these are used to help set the worst credible effect; the assumption used for exposure onset and duration is shown for each hazard;
- Detected or undetected by controller.

During the analysis, where it may have been possible to claim that the event could be mitigated by the movement from one working position to another, it is considered that the worst credible effect is that all working positions can be affected by a failure. This is because a transponder failure on a particular aircraft will remain across all sectors that the aircraft passes through. Similarly, in the event of a complete failure of a Surveillance Data Processing sub-system within an Air Traffic Service Unit, all CWPs could be affected.

It should be noted that a controller working position is the segment of the system (people, procedures and equipment) which holds responsibility for the area of controlled airspace under discussion. This segment may include more than one radar screen and possibly more than one person in differing roles depending on the architecture and method of working deployed at a particular ATSU. The system architecture at this level is not included within this Functional Hazard Assessment, but may need to be taken into account in local safety assessments.

H.4.2.2 Exposure Onset and Duration

The following exposure criteria were derived from the EUROCONTROL SAM Severity Indicator Sets 2 and 3 [3] – shown in Annex J.2. This enables the effects on ATC (Severity Indicator Set 1) to be more precisely established, and hence the severity of the hazardous effect to be selected. These criteria are mainly used as modifiers for the detectable failure modes. However, they also have a role in determining the worst credible case for undetected failure modes – certain exposure times may be less credible than others, and therefore a distinction must be made.

Note that in each of these cases, an assumption has been made that the ground sub-system includes some form of track extrapolation over a short-time period (assumed to be 30 seconds, or approximately 3 updates, in the Fault Tree Analysis). Therefore, although a failure in the system may occur over a period of 40 seconds, it will only be displayed to the controller for 10 seconds (for detection) due to the extrapolation function. [FHA03]. Some trackers may output a different symbol during coasting and therefore present the controller with an earlier indication of coasting on the Controller Working Position. If this happens in a local implementation then the consequences of this hazard may be reduced.

By utilising these modifiers, detectable failures are considered in terms of the exposure of the system to the hazard. This is expressed in terms of the duration of the failure condition and the rapidity with which it develops (either sudden, such as the loss of position function, or progressive which is the loss of information that is increasingly necessary for the identification of a particular target). The exposure criteria included within this assessment are:

- Sudden, Short Duration
  This criterion equates to an event which reaches its maximum severity very quickly, but which does not persist for sufficient time to enable procedures for abnormal operation to be put into place. Such a situation could correspond to an aircraft transponder that provides the surveillance system with “out of date” information (i.e. falls outside the latency requirements for a short time). For the purpose of this document ‘short duration’ was taken to be 10 seconds on the Surveillance Display (corresponding to 2 x the required update rate for TMA).

- Progressive, Short Duration
  This criterion equates to an event which would reach its maximum severity

over a significant period of time. The failure does not persist for a sufficient period of time for the full severity to be reached.

- Sudden, Continuous
  This criterion equates to an event which reaches its maximum severity very quickly, and continues indefinitely. It is not possible for procedures for abnormal operations to take effect immediately and exposure to the failure continues until the procedures take effect.

- Progressive, Continuous
  This criterion equates to an event which reaches its maximum severity over a significant period of time. Sufficient time is available and functionality remains to enact abnormal operations procedures.

Intermittent failure was also considered and is included within the other exposure criteria. For example:

- Short duration failures, which occur on a regular basis, can be considered to be equivalent to the continuous failure.

- Infrequent, intermittent failures can be considered to have the same effects as the short duration equivalent.

H.4.2.3 Detected or Undetected Failure

In each case the failure mode is assumed to be either detectable or undetectable by the controller.

The probability of detection by the system (e.g. monitoring, alarms) is taken into account in the fault tree analysis (for example, as an identified internal mitigation means). Failures in data elements detected by the system appear in the “detected loss of data” hazards because, where it affects the controller (i.e. is detected by the controller), they will not use the data.

In many cases in operations, the loss of data is detected by the controller (e.g. a data element on a track label disappears), and therefore this is considered a ‘detected failure’. However where the value on the track label appears correct – it is caused by the display of erroneous data, such as slightly out of date data – the probability that the failure is undetected is much higher.

For the purposes of this analysis, an assumption (FHA04 Annex F) has been made that the controller will detect lost data 999 in 1000 times (i.e. there is a 0.1% chance that the data element will remain undetected long enough to cause a safety-related effect). Note that even when detected, a safety-related effect may result.

This assumption is based on the fact that there any many procedural checks in place to allow a controller to detect a possible hazard, for example during the sector-sector transfer (as an aircraft reports altitude and identity on first contact). The value also reflects a commonly accepted human error rate of 1E-3.

An undetected failure occurs when no part of the system or controller detects the loss or corruption of data. This means that the ground domain continues in operation without realising the data is lost or corrupted.

All failures are undetected initially by the controller but will, after a given time period, become detected (whether by system intervention e.g. alert or by controller scanning of the display, or when another source of information – e.g. provided by pilots or another controller – contradicts that displayed to the controller). The greatest risk lies during the undetected period, as no recovery action can take place. The longer the period, the greater the risk.

It is assumed in all cases that the undetected period lasts long enough for the worst credible effect to occur (FHA05, Annex F. This provides the worst case scenario. As mentioned previously, this is longer than the 30 second extrapolation capability of the ground tracker.

H.4.2.4 Recovery Mechanisms

The loss of a data element(s) does not necessarily mean the controller has lost control of the situation (because the mental picture is maintained and strips are still available).

However, in order for this generic safety assessment to be fully credible, conservative assumptions have been made. In particular, FHA14 and FHA15 (Annex F) in the Application Description state that a controller will be able to revert to procedural control in the case of a data hazard involving one aircraft, but not in the case of multiple (all) aircraft.

Note that the problem here is not with the controller’s ability to detect the hazard. It is the ability, once the hazard has happened, to safely manage the situation. This safety assessment has taken credit for the fact that controllers detect most hazards (99.9%). It does not take credit for possible procedural methods of separating aircraft (in the case of no surveillance data), as in the worst case, a sudden loss of data whilst operating a sector at maximum capacity may not allow the controller to accurately and safely apply procedural separations immediately.

It is the near-term effects that particularly concern this safety assessment. Any longer term mitigations (such as reduction of traffic levels entering the sector, or imposition of holding) would not apply to effects occurring soon after the hazard occurred.

Following the display of erroneous data, or loss of data, there will be an increase in controller workload to obtain the parameters lost, as required, using R/T.

In the event that an aircraft transponder capability fails completely (i.e. complete loss of WAM, ADS-B and SSR surveillance for one aircraft) there will be an abnormal situation. Other aircraft will require to be managed around the one which is not transponding. The non-transponding aircraft will be diverted from the airspace as soon as is tactically feasible to do so. It is likely that there will be an impact on the safety within the airspace.

In the event that the only means of recovering from a data element failure is the establishment of transponder equipped aircraft to procedural control, the following statements apply:

- All data requires manual acquisition using R/T.
- There will be high levels of controller workload in maintaining the airspace picture for that aircraft.
- There will be no ground-based safety nets available (none are taken into account during the safety analysis).
- Separation minima are increased significantly with respect to that aircraft.

H.4.3 Credible Cases

Three failure modes of 'detected loss (including detected display of erroneous data i.e. corruption)', 'undetected loss' and 'undetected display of erroneous data' have been identified.

Detected Loss/Corruption

Detected display of erroneous data (corruption) is equivalent (in consequence) to detected loss of information because it produces an unreliable surveillance picture that the controller can no longer 'trust'. When the corruption is detected (even for one aircraft) then confidence in the function would reduce.

If the corruption is consistent for all targets, this may not present an immediate degradation in the surveillance picture (e.g. all targets being simultaneously displaced 1NM north of real position).

Corruption of information for a single aircraft is credible and likely to have arisen from partial transponder failure.

Credible corruption for a group of aircraft in a particular area is likely due to degradation of performance of one or more ground stations, or in the common functions on the ground.

Undetected Loss

For 'undetected loss', the credible case only applies in certain cases – for example, the undetected loss of all position information for all aircraft is not credible, whereas the undetected loss of one aircraft's altitude may be more likely.

This failure mode includes the case of no acquisition of aircraft. For example, an aircraft entering the area of responsibility with its transponder off or functioning incorrectly. This is a credible case because the controller may not have previously identified the aircraft.

Note that this undetected loss applies in two cases:

- After track extrapolation (30 seconds assumed as per FHA03);
- In the event of an acquisition failure when an aircraft enters the sector of interest.

Undetected Display of Erroneous Data (i.e. Corruption)

A number of credible undetected corruptions in data exist, for example:

- Progressive position latency increases (aircraft looks like it is on the correct route, however its position x seconds ago is displayed);
- Aircraft enters sector with corrupted position (i.e. controller does not see the degradation, and assumes the initial position is correct);
- 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.

For this category of failure mode:

- Undetected display of erroneous data is one of the most dangerous situations.
- When the corruption is detected (even for one aircraft) then confidence in the function would reduce.
- Credibility depends upon the system architecture and the likelihood of the controller detecting the situation (depending upon workload etc.).
- Operational effect depends on the environment and the duration of non-detection – for the purposes of the safety case, the worst credible effect should be identified.

H.4.4 Hazard-Effect Severity Classification

Following the identification of hazards and their effects, the next step is to assess the level of severity of the effect, clearly identifying the worst credible case.

This is carried out using the Severity Classification Scheme contained in ESARR4 [5], and reproduced in Annex J. The EUROCONTROL ANS Safety Assessment Methodology Severity Indicators [2] (see Annex J.2) are also used to determine the likely severity for each effect and hazard.

Below, some factors are identified that could improve or worsen the consequences of failure and/or external event occurrence(s). They are classified according to three major headings: Effects on Air Navigation Services, Exposure and Recovery. Each is also related to the phase of flight (type of airspace – i.e.

TMA or en-route). This allows a robust process in identifying the worst credible consequence for each hazard, and allocating severities accordingly during the workshop.

Effects on Air Navigation Services

- **Safety of Provided Air Navigation Services.** Effects on the ability to provide or maintain safe Air Navigation Service(s).
- **Working Conditions.** Effects on the ATCos and Flight Crew ability to cope with the reduction in functional capability, especially, impacts on their workload.
- **Adverse Operational and Environmental Conditions.** Effects on the ability for ATCo and/or Flight Crew to cope with adverse operational and environmental conditions.

Exposure

- **Exposure time.** The amount of time the hazard exists.
- **Number of exposed aircraft.** Number of aircraft exposed to the hazards.
- **Adverse operational and environmental conditions.** The frequency with which adverse operational and environmental conditions are expected to be experienced.

Recovery

- **Credibility of Failure.** When appropriate, the assessment could also consider the possibility of detection of, and recovery from, failure(s).
- **Rate of development of the hazardous condition.** Rate of development of the hazardous condition (e.g., sudden, moderate, slow) compared to the average time required for recovering from unsafe conditions.
- **Contingency Measures.** In some cases, it may be also possible to consider the availability of alternative procedures, fall-back equipment and ability to apply contingency measures.

The hazards listed in Table 19 and their assessed consequences are detailed in Annex I. Table 20 below shows the high level classification for each data element. This is the same as Table 19, with the hazard onset and duration characteristics added in bold text.

Five failure modes are therefore identified for each data element. For each of the identified failure modes, the TMA and en-route cases were examined.

The rationale behind each severity classification is shown in Annex I. These are the result of a compilation of previous workshops (from Mode S and ADS-B functional hazard analyses), and two validation meetings held with operational personnel for the purpose of this generic surveillance FHA – in all cases also applying ESARR4 and SAM.

Param	ID	Variant	Hazard – short description	Severity (worst credible case)
2D position or All parameters	H01	U1	Loss of 2D position (or of all parameters). **Sudden only, short or continuous**	ER=3 TMA=2
		D1		4
		D-many		ER=3 TMA=2
	H02	U1 **Sudden or progressive**	Display of erroneous 2D position (i.e. corruption of position) **Continuous**	ER=3 TMA=2
		U-many **Progressive only**		ER=3 TMA=2
Pressure altitude	H03	U1	Loss of pressure altitude **Sudden only, short or continuous**	5
		D1		4
		D-many		3
	H04	U1 **Sudden or progressive**	Display of erroneous pressure altitude (i.e. corruption) **Continuous**	ER=3 TMA=2
		U-many **Progressive only**		2
Aircraft ID / call sign	H05	U1	Loss of aircraft identity (Call sign) **Sudden only, short or continuous**	5
		D1		4
		D-many		3
	H06	U1 **Sudden or progressive**	Display of erroneous aircraft identity (Call sign) (i.e. corruption) **Continuous**	3
		U-many **Progressive only**		2
Short Intent	H07	All	Loss of, or display of erroneous, short intent	4

Table 20: Hazard classification and severity per failure mode (See Annex I)

H.4.4.1 Specific severity allocation

The severity classifications presented in the table above have been derived from discussions with operational experts in Austrocontrol and Eurocontrol. If local conditions are significantly different then these values may be adjusted for a specific implementation.

In ESARR 4 terms [Annex A of Ref 1], a large reduction in separation (e.g. less than half the separation minima) with ATC and or crew able to recover the situation is nominally classed as severity 3. A conservative view regarded the worst credible case as being severity 2 in a complex TMA, because of the complex route structure together with more climbing and descending traffic. In this case an abrupt manoeuvre may be required to avoid collision with other aircraft.

Note that severity 1 typically signifies that if a hazard occurs and every barrier identified fails, an accident will result (subject to providence, and not taking account of safety nets). This situation was not regarded as applicable in the reassessment.

Whether we expressly identify the key barriers (e.g. controller detection, communications, route structure) or merely state that something is extremely unlikely (i.e. not credible) is a consequence of the way in which the assessment process is carried out. However, if possible (i.e. if time and effort allowed for the hazard assessment workshop and consolidation of its results is sufficient), explicit identification and quantification of the effect of barriers is preferred, as it provides better traceability. The approach taken in this study, in order to provide a worked example, attempts to provide such traceability in the assignment of Safety Objectives by quantitatively identifying the barriers appraised (for example, the impact of a regulated route structure and managed traffic density). It is important to realise that either approach should lead to the same Safety Objective.

In order to derive these worst credible effects (and severities), a series of mitigation means were identified in some cases to justify the allocation of a lower severity (i.e. the mitigation means lead to the judgement that higher severity consequences were not credible).

The identified External Mitigation Means are shown in Table 21. They are also collated in Annex F.

Mitigation Means References	Safety Requirement
FHA09 **(EMM1)**	Experience and ability of controllers is present, which enables them to identify that the failure has occurred.
FHA10 **(EMM2)**	Procedural control can be established by controllers in the event of loss of data for one aircraft. The procedures are available (PANS-ATM, ANSP Manuals of ATC), training is given to the controllers in the use of procedural control, and the aircraft can successfully apply procedural control operations (R/T is available to make voice position reports, and flight crew procedures exist (PANS-OPS)).
FHA11 **(EMM3)**	Experience and ability of flight crew is present, which enable them to identify that something is not nominal.
FHA12 **(EMM4)**	Sector transfer procedures ensure that when an aircraft enters a sector, they contact the controller via R/T.
FHA13 **(EMM5)**	It is assumed that procedural control when altitude data is missing is safe (through controller training, experience etc).

Table 21: Identified External Mitigation Means

H.5 Safety Objectives Derivation

H.5.1 Process Assumptions

In deriving the Safety Objectives, reference has been made to ED-125 [6] and the EUROCONTROL Safety Assessment Methodology [3]. For more information on the detailed process to be followed, refer to these documents.

The hazards have been classified with severities depending on detection, non-detection and whether the loss impacts single or multiple aircraft. This severity classification, by definition, has been assessed taking into account a subjective ‘worst credible effect’ viewpoint.

This ‘worst credible effect’ viewpoint assumes that the environmental characteristics, as defined in the OSED and in Table 6, are approximately at their ‘worst’ at the time of the failure. This does not assume that the operational effect usually or always occurs, merely that it can ‘credibly’ occur. Hence the severity classification assumes that the ATCo is managing a high level of aircraft, at distances corresponding to the applicable separation minima.

The next step is therefore to identify the probability of the worst credible effect occurring for each hazard. This is in line with the Semi-Quantitative Model in ED-125 [6]. This probability is known as the Pe value, and is unique for each Hazard – Effect pair in this model.

H.5.2 Assessing the Pe value

The probability of the worst credible effect happening as a result of a particular hazard has several factors contributing to it:

- Controller detection: whether the failure mode is detected or undetected by the controller;
- Procedural mitigations (already used to determine the worst credible effect, but may also be used to determine the approximate probability of that effect occurring);
- Airspace structure (deconflicted routes) leading to a lower probability that a separation-related event will occur;
- Airspace complexity and traffic density (evidently, the probability of an accident occurring as a result of a failure falls if there are only 2 aircraft in the airspace, as opposed to 20).

Firstly, taking the probability of controller detection; this only applies where detection by the controller will reduce the severity of the worst credible effect – if the severity for undetected and detected cases is the same, it does not apply.

An assumption was made that for all hazards, the probability of controller detection was 99.9% (FHA04, Annex F). *[Note to safety assessors – if thought useful, more detail could be added at this stage, and a breakdown of likely detection rates per hazard-effect pair could be made, since probability of detection depends on procedures in place (for example, reporting of altitude on first contact) and controller ability (human error rate).]*

Secondly, procedural mitigations may reduce the probability of a particular effect occurring. These procedural mitigations are identified as External Mitigation Means in Table 21. As they are unique to each scenario, and each hazard-effect pair, this analysis does not go into depth on the likelihood of a procedural mitigation reducing the probability of a consequence of a hazard in a particular scenario. However, a generic appreciation of the presence of procedural mitigations may give more confidence to the eventual result of the analysis (i.e. the conservative assumption taken means that we can have greater confidence that safety margins exist in operational reality).

Taking the last two factors together, there is a finite probability that given the airspace structure, complexity and traffic density, the identified worst credible effect will happen as a result of the hazard in the case of separation losses (does not apply to workload issues). Analysis on this probability (which relates to a collision risk model) was done in the context of ED-126 [15].

The results of a paper [13] produced for the Requirements Focus Group (an RTCA/EUROCAE joint group under SC-186/WG-51) gives show that, for the busy SE sectors of the UK (London), "*the likelihood of aircraft being separated by* *a lateral separation of up to 7.5 NM (i.e. 1½ times the separation minima) and within 500ft vertically is in the order of 0.2% of the time*".

A conservative assumption can be made on account of the fact of London having regulated track structures, and the fact that growth in traffic densities in the future may increase the value. Therefore, for the purposes of this safety analysis, a value of 1% was used (i.e. for 1% of the time, aircraft will be in close enough proximity such that a separation-related effect will occur, but not necessarily an accident) [FHA07].

An example event tree can be drawn to show the safety calculation that is happening here. The bold text shows the case where the barriers do not mitigate the effect. To demonstrate the principle, it is enough to show the use of two factors in the Pe calculation.

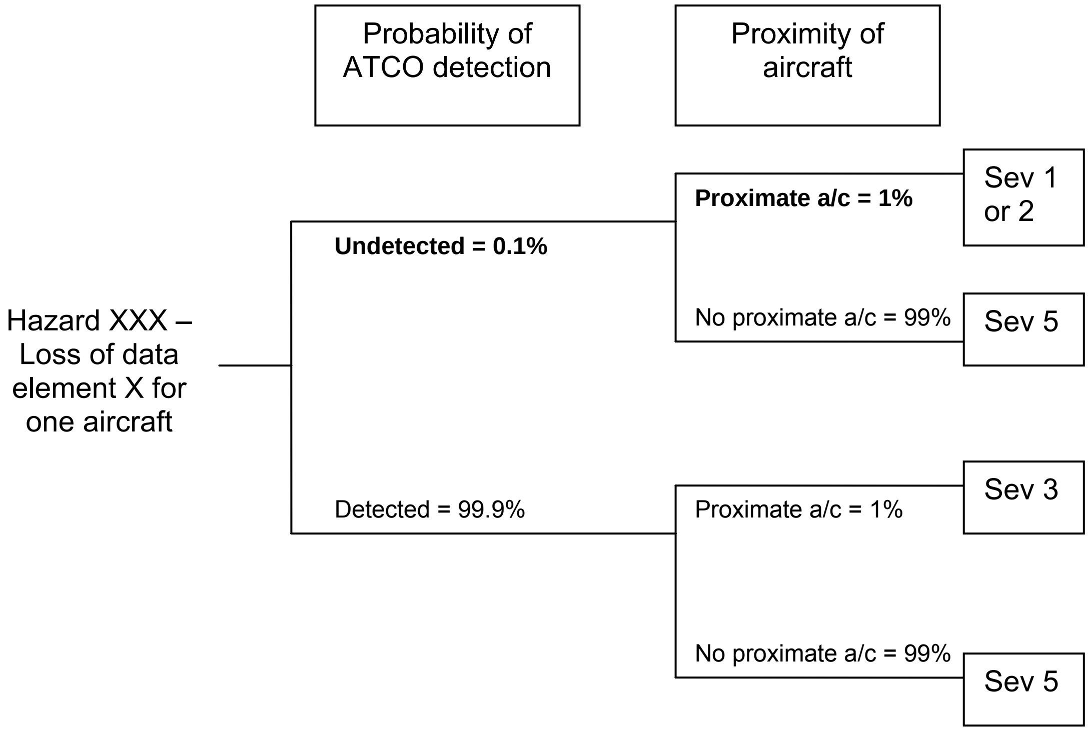


Figure 12: Example event tree

In the actual operational situation, even if the controller does not detect the loss of position and there is a proximate aircraft (the upper branch of the event tree shown), the situation does not lead inevitably to an accident. This is because the probability is low that, even if the aircraft are closer than the separation value to each other, the geometry is such that they are on a collision course. This provides a further significant barrier, which could be added to the Pe calculation if a numeric value could be assigned. However, as it is difficult to quantify, it has not been included in this example assessment.

H.5.3 Deriving the Safety Objective

In order to derive the safety objective, ED-125 postulates a formula as follows:

Safety Objective = STi / (Pe * N)

Where:

- STi is the safety target for a particular severity class i (see Risk Classification Scheme in H.2.2);
- Pe is the probability that a hazard can generate its worst credible effect, and;
- N is the part of the overall budget attributed to ATM that can be apportioned to this particular surveillance application and system.

According to ED-125, N is calculated by assuming a total number of ATM hazards, apportioning these hazards per worst credible effect (i.e. how many apply to each severity class), then dividing these per hazard.

The value N is necessary because, if the probability of an ATM-related accident can be no higher than $1x10^{-8}$, the surveillance application and system under investigation can only contribute to a proportion of that figure (as other, non-analysed, functions such as communications and navigation will also contribute to the final achieved probability).

ED-125 recommends that the total number of ATM hazards be considered to be 125 (based on 10-15 high level functions at the ATM service provision level, and approximately 10 hazards per function). If we assume that the hazards are apportioned equally between Severity Classes (a conservative assumption, given that experience tells us that most hazards lead to workload increase rather than collisions), this gives a value of N of 25 (i.e. 125 split 5 ways).

H.5.3.1 Example derivation for Hazard H01-U1

Hazard H01-U1 is “undetected loss of 2D position for one aircraft in the TMA”.

- The hazard has been found to have a worst credible effect of severity 2 for the undetected (by the controller) case (see Annex I for justification of this severity).
- The probability of the hazard, once it has occurred, leading to the worst credible effect is expressed by the Pe value. This is a combination of the probability of detection by the controller (i.e. in the majority of occurrences of the hazard, the controller will detect it, thus leading to the lower severity detected case), and the airspace complexity / traffic density mitigation.
- The probability of the hazard being undetected by the controller is set at 0.001. The probability of the consequence being of significance due to another aircraft being in the vicinity is assumed to be 0.01. These probabilities are assumed to be uncorrelated. Therefore this is stating that the loss of 2D position for one aircraft, if undetected by the controller, will lead to a severity 2 consequence (large reduction in safety margins) only 1 in

100000 times (1.0E-5), which is the product of the two independent probabilities.

- The Safety Target for the Severity Class in question (STi), as derived in the Risk Classification Scheme in Table 16, is now looked up – for the severity 2 case, this is 1.0E-6.
- These values are now all entered into the equation above, giving:
  - Safety Objective = 1.0E-6 / (1.0E-5 * 25) = 4.0E-3 / flight hour
- Note that because the Safety Objectives for this safety assessment need to be expressed in ATSU hours (since for ground-based surveillance a 'per sector' measurement makes more sense than a 'per flight' measurement), these values must then be translated into 'per ATSU hour' using the Environmental Conditions (ASSUMP08).The acceptable risk is expressed above as 'per flight hour', so if there are N flight hours in each ATSU hour (i.e. the average sector occupancy is N aircraft) then the equivalent acceptable risk per ATSU hour is increased by the factor N.
- The actual values used are that 1 ATSU hour in the TMA = 7 flight hours and that 1 ATSU hour in en-route = 15 flight hours. Therefore,
  - Safety Objective (TMA) = 4.0E-3 x 7 = 2.8E-2 per ATSU hour.

This derivation was carried out for all hazards and failure modes. The results are given below in Table 22.

H.5.3.2 Comments

- Note that the transition to operations may affect the probability of a hazard leading to a specific effect. This is due to a lack of experience of new operations. Due to the nature of this operation (surveillance for ATC), and the technology-independent nature of it as viewed at the CWP, there should be no transition to operations issues. Nevertheless it is recognised that in the introduction of a new sensor, the possibility of a certain hazard leading to an effect may be altered as the probability of the hazard changes.
- Example fault trees are developed in Annex L for all position related hazards and identification-related hazards.

H.5.3.3 Local Assessment variations

As noted in Volume 1, para 1.8, concerning the overall safety assessment process, safety objective values were worked out also as a more cautious assessment for hazards H01 (loss of 2D position or of all parameters) and H02 (display of erroneous 2D position). Table 22 below gives the results of the safety objective calculations. These alternative, more stringent, values (Table 23) are also taken account of in the fault tree discussion in Annex L. It is important to note that the example system architecture can be designed to meet even these more stringent safety objectives.

Hazard – short description	ID	Variant	Severity (worst credible case)	Probability of Effect (barriers)		Safety Objective (per ATSU hour)		Fault Tree ref
				Probability of being undetected by ATCO	Traffic complexity / density	ER	TMA	
Loss of 2D position (or of all parameters).	H01	U1	ER=3	0.001	0.01	6.0E-1		L.4.2
			TMA=2	0.001	0.01		2.8E-2	L.4.9
		D1	4		0.01	6.0E-2	2.8E-2	
		D-m	ER=3		0.01	6.0E-4		L.4.3
			TMA=2		0.01		2.8E-5	L.4.10
Display of erroneous 2D position (i.e. corruption of position)	H02	U1	ER=3	0.001	0.01	6.0E-1		L.4.4
			TMA=2	0.001	0.01		2.8E-2	
		U-m	ER=3	0.001	0.01	6.0E-1		L.4.5
			TMA=2	0.001	0.01		2.8E-2	
Loss of pressure altitude	H03	U1	5	0.001	0.01	NA	NA	
		D1	4		0.01	6.0E-2	2.8E-2	
		D-m	3		0.01	6.0E-4	2.8E-4	
Display of erroneous pressure altitude (i.e. corruption)	H04	U1	ER=3	0.001	0.01	6.0E-1		
			TMA=2	0.001	0.01		2.8E-2	
		U-m	2	0.001	0.01	6.0E-2	2.8E-2	
Loss of aircraft identity (Call sign)	H05	U1	5	0.001	0.01	NA	NA	
		D1	4		0.01	6.0E-2	2.8E-2	L.4.6
		D-m	3		0.01	6.0E-4	2.8E-4	
Display of erroneous aircraft identity (Call sign) (i.e. corruption)	H06	U1	3	0.001	0.01	6.0E-1	2.8E-1	L.4.7
		U-m	2	0.001	0.01	6.0E-2	2.8E-2	L.4.8
Loss of, or display of erroneous, short intent	H07	U	4	0.001	0.01	6.0E+1	2.8E+1	
		D	4		0.01	6.0E-2	2.8E-2	

Table 22: Deriving the Safety Objectives

Hazard – short description	ID	Variant	Severity (worst credible case)		Probability of Effect (barriers)		Safety Objective (per ATSU hour)		Fault Tree ref
			Revised assessment	Original assessment	Probability of being undetected by ATCO	Traffic complexity / density	ER	TMA	
Loss of 2D position (or of all parameters).	H01	U1	ER=3	1	0.001	0.01	6.0E-4		L.4.2
			TMA=2	1	0.001	0.01		2.8E-4	L.4.9
		D-m	ER=3	1		0.01	6.0E-7		L.4.3
			TMA=2	1		0.01		2.8E-7	L.4.10
Display of erroneous 2D position (i.e. corruption of position)	H02	U1	ER=3	1	0.001	0.01	6.0E-4		L.4.4
			TMA=2	1	0.001	0.01		2.8E-4	
		U-m	ER=3	1	0.001	0.01	6.0E-4		L.4.5
			TMA=2	1	0.001	0.01		2.8E-4	

Table 23: Deriving the Safety Objectives (more stringent alternative)

I Severity Classification Tables

I.1 Introduction

The following tables show the 'severity classification' for the loss or corruption of each surveillance parameter in en-route and TMA/approach airspace, according to the failure modes outlined in section H.4.4. It should be noted that this is an EXAMPLE, and implementers must conduct a Functional Hazard Analysis for their local environment and application.

The operational hazards identified at the CWP were the failure of the system to deliver surveillance information, and the possible corruption of such information (display of erroneous data). Hazards and safety objectives are defined for the following data items, identified in the OSED, which are displayed on the controller interface:

- 2D position,
- Mode C barometric altitude,
- aircraft identity (e.g. call sign and SPI)
- short intent / history and
- all parameters together.

Loss and corruption were treated as two different hazards, so initially there were 10 main hazards (2 for each of 5 parameter situations). However, loss and corruption hazards affecting “short intent” were treated together, and hazards for “all parameters” were considered to have almost identical effects as hazards for 2D position and assessed as having the same severity. This reduces the list to 7 main hazards.

Each parameter has nominally 8 failure mode variants as listed below. However, only 5 need separate consideration, for the reasons indicated.

- Loss, undetected, one aircraft.
- Loss, undetected, many aircraft. *Not credible.*
- Loss, detected, one aircraft.
- Loss, detected, many aircraft.
- Corruption, undetected, one aircraft.
- Corruption, undetected, many aircraft.
- Corruption, detected, one aircraft. *Treated as for loss as data not used.*
- Corruption, detected, many aircraft. *Treated as for loss as data not used.*

The detailed rationale is given in the tables below.

Note also, as mentioned earlier in this document, that the initial severity classification of position hazards was revised as a result of internal discussion. However, the initial more conservative assessment is retained in these tables by annotation in brackets.

I.2 Position Hazards

Ref.	Hazard	Exposure onset & duration type	Qualifier	Position Hazard Effect on ATC	Mitigation (H.4.4)	Severity ER	Severity TMA
H01 / U1	Loss of 2D position / Undetected	Sudden only (as progressive would be detected) / Short or continuous	One aircraft	For the undetected case, loss of 2D position would usually be detected by the controller in a short duration (leading to little to no safety impact). However, aircraft may be unknown to controller (e.g. entering the sector). *A particular hazard is aircraft entering the sector with the transponder off or functioning incorrectly.* Continuous loss (more than 10 seconds) applies here, as it is possible the controller will not notice the loss of position for an aircraft entering the sector (or with the track not being initiated for an aircraft on departure). It is less credible for aircraft already identified within the sector. Instructions to other aircraft could lead to incidents with the undetected aircraft. In the TMA, where manoeuvring and airspace complexity mean that more aircraft paths have the possibility of crossing, it may be credible to assume that the worst effect could be a collision (i.e. there is a finite probability). (This was reassessed.) The possibility of taking account of deconflicted routes in the airspace of interest was debated, particularly for the ENR case. It has not been captured in the severities, but should be further discussed in the "Probability of Effect" assessment leading to the safety objective. Note that no other mitigation means are applied here at this stage, as the controller has not detected the problem. There is a chance that the hazard will become detected as sector-sector transfer procedures currently in operation are designed to alert the controller to a new aircraft entering their sector. This is captured in the Safety Objective derivation. Mode S severity ENR=3, TMA=2. ADS-B-NRA severity ENR=1, TMA=1.		3 (Conservative assessment =1)	2 (Conservative assessment=1)
Note	Undetected loss of 2D position	Sudden or progressive. Short or continuous	More than one aircraft	The undetected loss of position of several aircraft (even at the boundary edge) was not considered to be credible (too unusual, and even if it happened, the controller would immediately detect the problem). The non-credibility of this failure mode applies to all other parameters also (i.e. undetected loss for several/all aircraft)		N/A	N/A

Ref.	Hazard	Exposure onset & duration type	Qualifier	**Position Hazard** **Effect on ATC**	Mitigation (H.4.4)	Severity ER	Severity TMA
H01 / D1	Detected loss of 2D position	Sudden only. / Continuous	One aircraft	The assumption is made that track extrapolation is operational in the ground sub-system, and therefore any failure in the transmitted information from the aircraft only becomes a failure on the controller's display after 30 seconds. If the failure lasts less than 10 seconds, then no effect on ATC. If the failure continues beyond 10 seconds, then the aircraft data would be lost to the system and the failure would become continuous loss. Controller treats the aircraft in similar manner to existing transponder failures, with aircraft proceeding to the next waypoint. There may be some increased controller workload due to the need for procedural separation to be applied for that aircraft, and in increased coordination with other sectors / adjacent ATSUs. Procedural separation methods for one aircraft were assumed to be safe, and lead to slight extra workload for the controller [EMM2]. Mode S severity ENR=4, TMA=4 ADS-B-NRA severity ENR=4, TMA=4	**EMM1 / EMM2 / EMM4**	4	4
H01 / D-many	Detected loss of 2D position	Sudden only / Continuous	More than one aircraft	If the failure lasts less than 10 seconds then no effect on ATC. If the failure continues beyond 10 seconds, then the aircraft data would be lost to the system and the failure would become continuous loss. Therefore, only continuous duration is assessed here. Ideally, the controller would notify all pilots of a problem, and request they report position updates, and perhaps maintain the current flight level until procedural control can be established (EC1). For airspace where crossing manoeuvres are being performed or where the traffic is likely to be in the process of changing levels there is an increased risk that separation minima may be infringed. It is then a question of the trust in procedural methods to maintain safety (see mitigations). The assumptions were made in the OSED [ASSUMP04, 05] that procedural separation applied in high density airspace for all aircraft suddenly would not be a safe recovery method. Therefore, although procedural control exists as a possible mitigation means, it was thought in the context of this safety case that the worst credible effect may be a collision between aircraft. (This was reassessed.) A mitigation does exist that aircraft are normally on deconflicted routes (i.e. airspace structure). This may reduce the probability of the SEV1 effect resulting from this hazard. Mode S severity ENR=2, TMA=2 ADS-B-NRA severity ENR=3, TMA=3		3 (Conservative assessment =1)	2 (Conservative assessment=1)

Ref.	**Hazard**	**Exposure onset & duration type**	**Qualifier**	**Position Hazard Effect on ATC**	**Mitigation (H.4.4)**	**Severity ER**	**Severity TMA**
H02 / U1	Undetected corruption of 2D position	Sudden or progressive / Continuous	One aircraft	A short exposure (<10 seconds) to a corrupted position, when undetected, would have little credible impact. Any impact rises in severity for the continuous case (> 10 seconds), and it is therefore this qualifier that is used. Aircraft may appear in a different location to their actual one – for this to be undetected, it is more likely that a progressive failure occurs (i.e. gradual corruption of the 2D position). Alternatively, the aircraft's 2D position may be corrupted as it enters a new sector (the sudden exposure case). The controller may issue instructions (clearances) based on incorrect locations, which could place the aircraft on conflicting paths. Again, in this case, the probability of detection of the hazard by the controller will be taken into account in determining the Safety Objective (rather than in determining the Worst Credible Effect of the undetected case). Mode S severity ENR=3, TMA=2 ADS-B-NRA severity ENR=1, TMA=1		3 (Conservative assessment =1)	2 (Conservative assessment=1)
H02 / U-many	Undetected corruption of 2D position	Progressive only / Continuous	More than one aircraft	Undetected corrupted position for more than one aircraft is considered to be non-credible for sudden changes, as the controller would detect the failure. Therefore, only the progressive case is considered. Aircraft may appear in different locations to their actual ones – there may be latency in the data (particularly a gradual build-up of latency). Alternatively, the relative positions of the aircraft may be correct, but there may be increased risk at boundaries of airspace, or close to terrain or other obstructions, where the incorrect absolute positions have a higher safety consequence. The probability of detection of the hazard by the controller will be taken into account in determining the Safety Objective (rather than in determining the Worst Credible Effect of the undetected case). Mode S severity ENR=2, TMA=2 ADS-B-NRA severity ENR=1, TMA=1		3 (Conservative assessment =1)	2 (Conservative assessment=1)

I.3 Pressure Altitude Hazards

Ref.	Hazard	Exposure onset & duration type	Qualifier	**Pressure Altitude Hazard** **Effect on ATC**	Mitigation (H.4.4)	Severity ER	Severity TMA
H03 / U1	Undetected	Sudden only (as progressive would be detected) Short only (as continuous would be detected)	One aircraft	For a period of less than 10 seconds, the loss of pressure altitude data has no safety impact. This differs from the equivalent "2D position" or "ALL" hazard cases, as the controller is aware that the aircraft is in the sector (as the position is still shown) – it is only altitude that is lost.		5	5
H03 / D1	Detected loss of altitude	Sudden only / Continuous (see effect on ATC)	One aircraft	Short duration loss of altitude, when detected, has no effect on ATC operations. Therefore, continuous exposure is considered. The Controller will treat the aircraft in a similar manner to other/existing transponder failures with the aircraft proceeding to next waypoint. There may be some increased controller workload due to the need for increased R/T activity and the need for increased co-ordination with other sectors/adjacent ATSUs. Mode S severity ENR=4, TMA=4	**EMM 1/ EMM 2/EMM 3/EMM 4**	4	4
H03 / D-many	Detected loss of altitude	Sudden only / Continuous	More than one aircraft	Notify all pilots of a problem and request that they maintain their current situation until procedural control can be established. It is assumed that procedural control with only altitude missing is safe (see EMM5) For airspace where crossing manoeuvres are being performed or where the traffic is likely to be in the process of changing levels there is an increased risk that separation minima may be infringed. Mode S severity ENR=3, TMA=3	**EMM 1/EMM 2/EMM 3/EMM 4/ EMM 5**	3	3
H04 / U1	Undetected corruption of altitude	Sudden or progressive Continuous	One aircraft	Aircraft altitude may be displayed incorrectly. Aircraft will not be at the intended flight level. Particularly a problem in the TMA, where climbing and descending traffic may increase the risk of separation minima being lost. A severity 1 accident was considered non-credible, due to reporting of altitude by aircraft (thus making the problem detectable by controller). Mode S severity ENR=3, TMA=2		3	2

Ref.	Hazard	Exposure onset & duration type	Qualifier	Pressure Altitude Hazard Effect on ATC	Mitigation (H.4.4)	Severity ER	Severity TMA
H04 / U-many	Undetected corruption of altitude	Progressive only / Continuous	More than one aircraft	Aircraft altitude may be displayed incorrectly. Aircraft will not be at the intended flight level. The undetected case may be unlikely (due to pilot reporting of altitude), but if it does occur, the severity will be high (2). Mode S severity ENR=2, TMA=2	**EMM 3**	2	2

I.4 Identification Hazards

Ref	Hazard	Exposure onset & duration type	Qualifier	Identification Hazard (call sign backed up by Mode A code) Effect on ATC	Mitigation (H.4.4)	Severity ER	Severity TMA
	All Loss Failure Modes	n/a	n/a	For all operational discussion of loss of identification, it was assumed that the display to the controller would still show position (e.g. if a primary plot was available, it would be displayed without a label). Flight strips would still be available. In the case of loss of identification also losing track, it is assumed that the worst case of ALL parameters being lost is applicable, and it is treated accordingly in that section (and in the relevant fault trees). Therefore, loss of identification in this section refers only to loss of the identification parameter, and not to loss of all parameters.		n/a	n/a
H05 / U1	Undetected loss of identification	Sudden only. Short only (as continuous would be detected)	One aircraft	Provided that the failure lasts less than 10 seconds, there will be no safety effect. Continuous is considered to be detected (and therefore not applicable here).		5	5
H05 / D1	Detected loss of identification	Sudden only / Continuous	One aircraft	Potential for recovery is higher than for 'all aircraft' due to the possibility that the aircraft identity can be derived by a variety of means (e.g. R/T) – if only transponder aircraft are affected, alternative means remain available. There may be slightly increased risk to aircraft involved in crossing or level change manoeuvres in this period.	**EMM 1**	4	4

Ref	Hazard	Exposure onset & duration type	Qualifier	**Identification Hazard** **(call sign backed up by Mode A code)** **Effect on ATC**	Mitigation (H.4.4)	Severity ER	Severity TMA
H05 / D-many	Detected loss of identification	Sudden only Continuous	More than one aircraft	Provided that the failure lasts less than 10 seconds, the potential for increased workload will be minimal. Therefore, only continuous failure is assessed. There may be increased risk to aircraft involved in crossing or level change manoeuvres in this period. It is assumed that the loss of call sign would mean it is replaced by the Mode A code (i.e. assumptions on the system are made in the fault tree analysis that Code-Call sign Correlation is available, and that standard reversion techniques are used) [FHA06]. There is a large increase in workload potentially resulting from moving from call sign based communications to 4096 codes for several aircraft. If the Mode A code is also lost (reverting in this case to PSR plots with no label), it is assumed that flight strips are maintained [FHA06], and therefore the effect is a high increase in controller workload, but not a severe loss of separation.	**EMM 1**	3	3
H06 / U1	Undetected corruption of identification	Sudden or progressive Continuous	One aircraft	One aircraft's corrupted call sign may mean an instruction is given to the wrong aircraft. A possible mitigation is the flight crew's awareness of the situation, and a detection of the problem, meaning that severe effects are not as credible.	**EMM 3**	3	3
H06 / U-many	Undetected corruption of identification	Sudden only / Continuous	More than one aircraft	The effect of swapped aircraft IDs is one of the most severe for this hazard. It may lead to incorrect clearances / instructions being given. Mitigation is provided by the flight crew's situational awareness (i.e. knowledge that an instruction is unlikely to be for them). This hazard may occur on the boundary of the sector, as aircraft enter the sector with a wrongly assigned call sign. It is not considered credible for the controller to not detect corruption in call signs over a period of time. Hence the duration is expected to be less than a minute, and would probably result in increased workload (possibly more severe in the TMA as tighter traffic may mean more risk of separation infringement).	**EMM 3 / EMM 4 /**	2	2

I.5 Aircraft Trend and History Hazards

Ref.	Hazard	Exposure onset and duration type	Qualifier	Aircraft Trend & History Hazard Effect on ATC	Mitigation (H.4.4)	Severity en-route	Severity TMA
	Detected loss of history Indication	All exposure types	All qualifiers	History Indication is provided by SDPS; therefore it is not a surveillance sensor problem. The absence of History Indication is caused by problems by the tracking function, which delivers plots instead of tracks for display.		5	5
H07 / U & H07 / D	Detected or undetected loss or corruption of Short Intent	All exposure types	One or more than one aircraft	No immediate impact upon safety as the ATCo retains knowledge of aircraft current position. May impose minimal increase in controller workload particularly in busy environments where knowledge of the short intent is useful. Inability to anticipate the short intent may decrease the capacity of the system.		4	4

I.6 "All parameters" Hazards

Ref.	Hazard	Exposure onset and duration type	Qualifier	ALL parameters hazard Effect on ATC	Mitigation (H.4.4)	Severity en-route	Severity TMA
	All parameters – loss or corruption – detected or undetected	N/A	N/A	"ALL parameters" hazards were considered to have the same effects as the 2D position hazards.		See 2D position hazards	See 2D position hazards

J Severity Classification Scheme

J.1 ESARR4 Severity Classification Scheme

Severity Class	**1** **[Most Severe]**	**2**	**3**	**4**	**5** **No safety effect** **[Least Severe]**
Effect on Operations	**Complete loss of safety margins**	**Large reduction in safety margins**	**Major reduction in safety margins**	**Slight reduction in safety margins**	**No effect on safety.**
Examples of effects on operations Include:	**Accidents, including:-** ❑ one or more catastrophic accidents, ❑ one or more mid-air collisions ❑ one or more collisions on the ground between two aircraft ❑ one or more Control Flight Into Terrain ❑ Total loss of flight control. No independent source of recovery mechanism, such as surveillance or ATC and/or flight crew procedures can reasonably be expected to prevent the accident(s).	**Serious incidents, including:-** ❑ (a) large reduction in separations (e.g., higher than half the separation minima), without crew or ATC fully controlling the situation or able to recover from the situation. ❑ one or more aircraft deviating from their intended clearance, and Abrupt collision or terrain avoidance manoeuvres are required to avoid an accident (or when an avoidance action would be appropriate).	**Major incidents.** ❑ (a) large (e.g., higher than half the separation minima) reduction in separations with crew or ATC controlling the situation and able to recover from the situation. ❑ (a) major (e.g., lower than half the separation minima) reduction in separation without crew or ATC fully controlling the situation, hence jeopardising the ability to recover from the situation (without the use of collision or terrain avoidance manoeuvres).	**Significant incidents**. ❑ No direct impact on safety but indirect impact on safety by increasing the workload of the air traffic controller or aircraft flight crew, or slightly degrading the functional capability of the enabling CNS system. ❑ (a) major (e.g., lower than half the separation minima) reduction in separations with crew or ATC controlling the situation and fully able to recover from the situation.	No hazardous condition i.e. in any direct or indirect impact to the operations**.**

Note: The worst credible effect in the environment of operations determines the severity class.

J.2 EATMP SAM Severity Indicators [3]

This table is taken from the EATMP SAM guidance material; specifically Appendix D of the FHA guidance material (v2.0).

Severity Class	**1** **[Most Severe]**	**2**	**3**	**4**	**5** **[Least Severe]**
Effects on Operations	**Complete Loss of Safety Margins**	**Large Reduction in Safety Margins**	**Major Reduction in Safety Margins**	**Slight Reduction in Safety Margins**	**No Safety Effect**
SEVERITY INDICATORS SET 1: EFFECTS ON AIR NAVIGATION SERVICE					
Effect on Air Navigation Service within the area of responsibility	Total inability to provide or maintain safe service	Serious inability to safe provide or maintain 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
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					
Exposure time	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 presence is such that no significant consequences are expected.	Too brief to have any safety-related effect
Number of aircraft exposed	All aircraft in the area of responsibility	All aircraft in several ATC Sectors	Aircraft within a small geographic area or an area of low traffic density	Single aircraft	No aircraft affected

Severity Class	1 [Most Severe]	2	3	4	5 [Least Severe]
Effects on Operations	**Complete Loss of Safety Margins**	**Large Reduction in Safety Margins**	**Major Reduction in Safety Margins**	**Slight Reduction in Safety Margins**	**No Safety Effect**
Likelihood to experience adverse operational and environmental conditions	Frequent to permanent presence of the considered adverse operational and environmental conditions	Relatively high likelihood to experience the considered adverse operational and environmental conditions	Slight likelihood to experience the considered adverse operational and environmental conditions	Low likelihood to experience the considered adverse operational and environmental conditions	Rare presence of the considered adverse operational and environmental conditions
SEVERITY INDICATORS SET 3: RECOVERY					
Annunciation, Detection and Diagnosis	Misleading indication. Hard to detect or diagnose. Diagnosis very likely to be incorrect	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	Faster	Similar	Slower	Much slower. Plenty of time available

K Example Functional Models

K.1 Introduction

This annex presents an example functional description of the surveillance sub-system scenarios.

The description comprises a functional model and a summary of the purpose of each element of the model for each scenario.

The purpose of presenting functional models is to help in the PSSA. The functional models allow experts to discuss possible failure modes and are therefore a useful tool in the development of fault trees.

This Annex focuses on the “WAM sole means” functional model, and it is this model used for the PSSA analysis in Annex L. Some illustrative alternative scenarios with other surveillance techniques are presented at the end of the annex. These alternative scenarios go beyond the main scope of this document.

The architectures shown here represent the system functions. No redundancy is shown although clearly functions may be duplicated in an implementation. These are minimal architectures, for which there is deliberately no redundancy in the functional model, so that system functional design sensitivities to failure are highlighted by the analysis within this Study. This approach is intended to assist ANSPs to understand where such design decisions are most important and have most effect on the safety and performance of the installed system.

K.2 Functional Architecture

K.2.1 Functional Model for WAM Sole Means

Figure 13 shows the functional model developed for this generic safety assessment.

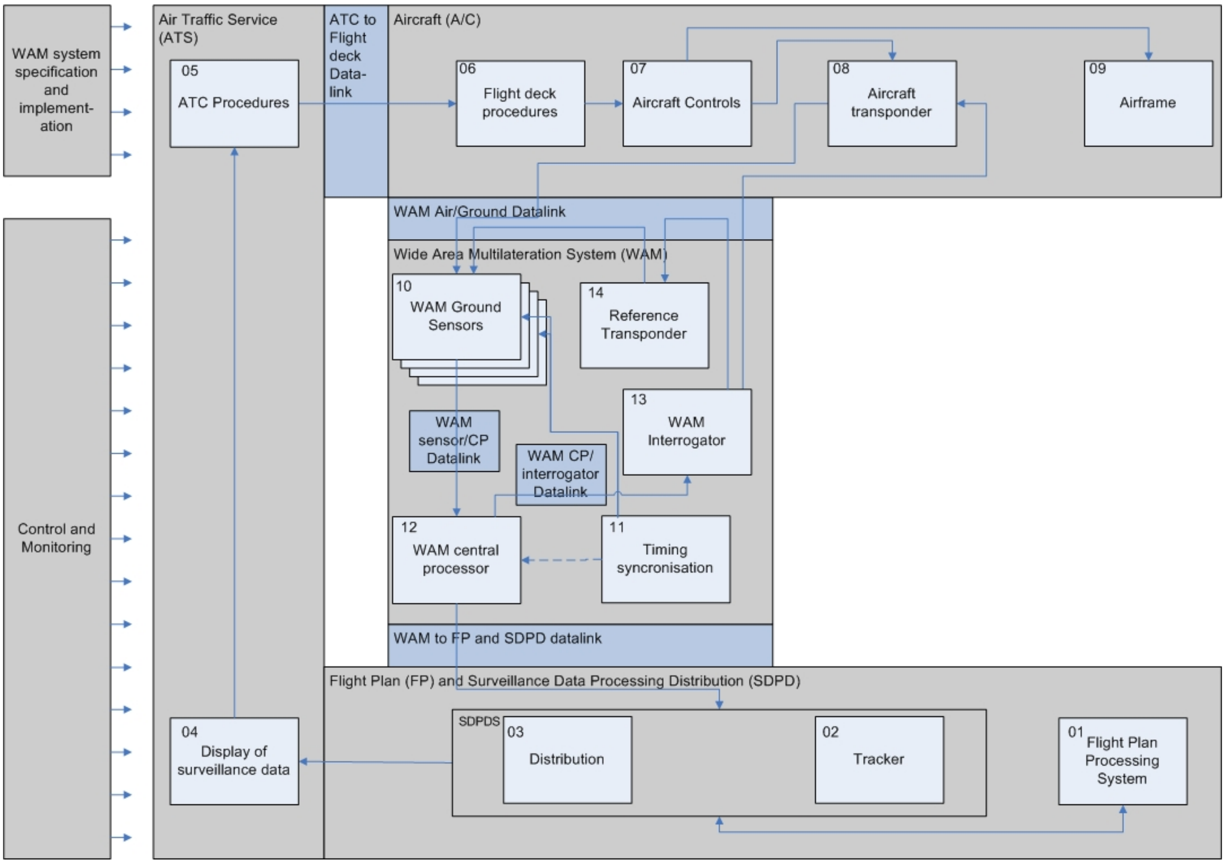

WAM system specification and implement-ation
Control and Monitoring
Air Traffic Service (ATS)
05 ATC Procedures
04 Display of surveillance data
ATC to Flight deck Data-link
Aircraft (A/C)
06 Flight deck procedures
07 Aircraft Controls
08 Aircraft transponder
09 Airframe
WAM Air/Ground Datalink
Wide Area Multilateration System (WAM)
10 WAM Ground Sensors
14 Reference Transponder
13 WAM Interrogator
WAM sensor/CP Datalink
WAM CP/ interrogator Datalink
12 WAM central processor
11 Timing syncronisation
WAM to FP and SDPD datalink
Flight Plan (FP) and Surveillance Data Processing Distribution (SDPD)
SDPDS
03 Distribution
02 Tracker
01 Flight Plan Processing System

Figure 13: Functional model of WAM sole means

K.2.2 System Blocks

The systems are divided up into component blocks, these include; Control and Monitoring, Air Traffic Service (ATS), Aircraft (A/C), Flight Plan (FP) and Surveillance Data Processing (SDP) and the surveillance scenarios themselves.

Component	Description
Wide Area Multilateration (WAM)	This includes all the WAM ground equipment.
(Various) data links	These are the communications data links between different functional blocks.
Control and Monitoring	Block represents the continual control and monitoring (heath check) of the system at all levels and includes both technical and human procedures.
Specification and Implementation	This is the process of specifying, designing, implementing and commissioning the WAM sub-system to ensure it offers continuity with other surveillance networks.
Air Traffic Service (ATS)	Dynamic control of the aircraft by a human based upon the information provided to him/her by the surveillance sub-system.
Aircraft (A/C)	Includes all airborne functions and operations.
Flight Plan (FP) and Surveillance Data Processing (SDP)	Specifies the 3-dimensional route which the aircraft is to follow when executing the flight plan by using knowledge of the predicted traffic level and current airspace structure.

Table 24: Describing component blocks in the system architecture

K.2.3 Functions

The following table provides a brief description of each of the Safety Functions shown above.

Function Ref	Function	Description
01	Flight Plan Processing System.	Provides the pre-flight planning and management functionality to the aircraft flight and then specifies the 3-dimensional route which the aircraft is to follow by using knowledge of the predicted traffic level and current airspace structure. This block includes the code call sign correlation database (CCCD) function which provides cross correlation between the aircraft **Mode A** code and the **aircraft identity (Call sign)** entered on the flight plan. Correlation is further discussed below.
02	Tracker	Correlates surveillance data from all sources available to it by creating and recording identified 3D target tracks associated with a filed flight plan.
03	Distribution	Distributes surveillance data from the tracker to the downstream systems.
04	Display of surveillance data	Provides the visual interface to enable to management of the situation by awareness of flight progress displayed by the **2D position**, **pressure altitude**, **aircraft identity** and **short-term intent** data items.
05	ATC Procedures	Gives clearances to the aircraft, monitors the progress of the flight against the expected trajectory and ensures safe separation of aircraft from other aircraft and terrain (when applicable).
06	Flight deck procedures	Accepts clearances and other instructions from ATC, manages and monitors both aircraft systems and the operational environment to ensure that the aircraft follows the required course to its destination.
07	Aircraft controls	Adjusts the aircraft’s attitude and/or velocity to achieve the desired position in the horizontal and vertical dimensions at the appropriate speed and rate of descent (includes both avionics and flight management systems).
08	Aircraft transponder	Receives interrogations and broadcasts replies to requests for information (mode A/C and mode S). Also broadcasts ‘squitters’ spontaneously.
09	Airframe	Represents the aircrafts response to the flight control function and external effects (weather and other meteorological conditions). the combination of which produces the actual position of the aircraft at a given point in time.
10	WAM ground Sensors	Receives signals broadcast by transponders. At least four are required to receive a message broadcast by an aircraft to determine its 3D position.
11	Timing synchronisation	Provides timing synchronisation through a clock system (be it distributed or common) which is used to determine the target position.
12	Central Processor Unit	Correlates transponder replies to produce position estimates and range measurements. It compares the results of multilateration and elliptical ranging. In addition, it controls the interrogator (rate and Mode-S or Mode-A/C) of the WAM sub-system. It keeps internal tracks for all aircraft and produces ‘plots’ for each target. It also timestamps the plots before forwarding them in ASTERIX format.

13	Interrogator	Issues interrogations to aircraft transponders to initiate replies.
14	Reference Transponder	Provides a heath check function for the WAM sub-system by ensuring that transponder replies that it issues are being received at all the required sensors and that the time synchronisation is correct. It may also form part of the timing synchronisation system.
Data link	ATC to Flight deck	Provides the ability for flight crew and ATC to exchange operationally necessary information by means of voice and/or data transmission.
Data link	WAM Air/Ground	RF Environment; Aircraft responding to interrogations from WAM sub-system in signals detected by sensors.
Data link	WAM to FP and SDPD	RF or microwave link from WAM CP to both Tracker SDPD and Code call sign CD.
Data link	WAM sensor to CP	High frequency (e.g. microwave) link from the sensors to the WAM CP.
Data link	WAM CP to interrogator	High frequency (e.g. microwave) link from the WAM CP to the WAM interrogator.

Table 25: Functional blocks for WAM sole means

The surveillance information presented at the controller working position is the result of the joint tracker and surveillance distribution functions, both of which are fed by the system surveillance sources. They are also cooperatively linked to the flight plan processing system as discussed in the following section.

K.2.4 Flight Plan Correlation

Correlation between the aircraft identification (either call sign or tail number, usually given in the flight plan) and a surveillance target is normally established using the Mode A identity code. Once the correlation is complete, the controller will normally only be presented with the aircraft identification.

If the aircraft identification is available directly from the aircraft, e.g. via Mode S, then this may be used for the initial correlation. In this case, the ground system compares the down linked identification with that in the filed flight plan. If they are the same then the correlation is made without any need for the Mode A code. This process already operates in a small number of centres.

However, in most cases the Mode A code is used for correlation. Here, the ATC-assigned code is compared with the down linked code from the aircraft. Once the initial correlation has been made, the down linked aircraft identification or the 24 bit address may be used for ongoing correlation and the Mode A code may be released. This is done by assigning a conspicuity code (e.g. 1000) to the aircraft.

It is worth noting that if correlation must be maintained using the Mode A code and this code is inadvertently lost, (e.g. by crew error) so too might the correlation and therefore the identity of the target.

The process of gaining and maintaining flight plan correlation using the Mode A code is outlined in the figure below.

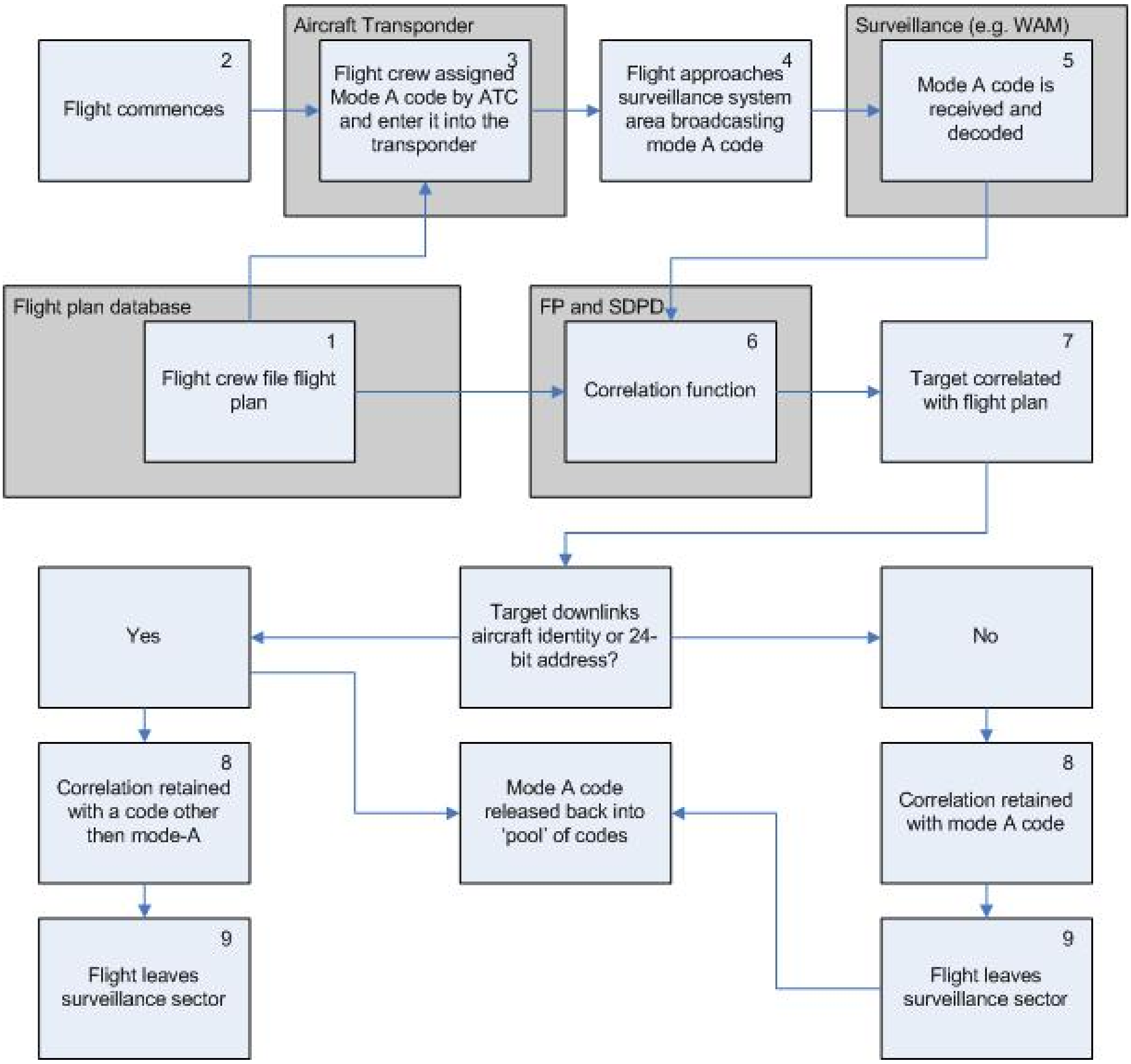

Aircraft Transponder
Surveillance (e.g. WAM)
2
Flight commences
3
Flight crew assigned Mode A code by ATC and enter it into the transponder
4
Flight approaches surveillance system area broadcasting mode A code
5
Mode A code is received and decoded
Flight plan database
1
Flight crew file flight plan
FP and SDPD
6
Correlation function
7
Target correlated with flight plan
Yes
Target downlinks aircraft identity or 24-bit address?
No
8
Correlation retained with a code other then mode-A
Mode A code released back into 'pool' of codes
8
Correlation retained with mode A code
9
Flight leaves surveillance sector
9
Flight leaves surveillance sector

Figure 14: Target and flight plan correlation using Mode A code

In Figure 14 the dark grey boxes represent the 'system blocks' of section K.2.2, while the light grey boxes represent processes or stages of flight.

Technically, a multilateration system will track the target using the Mode S address if it is available, and the Mode A code if not. The technical tracking of the target in the multilateration sub-system is not related to the correlation described here.

In addition to the methods described here the identity of a target may be established 'manually' by an ATCO request to the target via R/T. For the purposes of this document it is assumed that a functional level of flight plan to target correlation exists and is based on the Mode A code [FHA06], however this is an assumption that ANSPs will have to verify for their own system (see assumptions of Fault Tree Analysis in L.2).

K.2.5 Timing

This section provides a brief discussion on typical timing architectures in the different WAM sub-systems. The architectures are taken from reference 8. and are:

- Common Clock;
- Transponder Synchronisation;
- Standalone GNSS;
- Common view GNSS.

The first architecture has a single clock for the whole system. The last 3 architectures are examples of distributed architectures which use a local clock at each sensor. The local clocks are synchronised using GNSS or a reference transponder.

The following figures show the architecture taxonomy and the generic possible failure modes in each architecture.

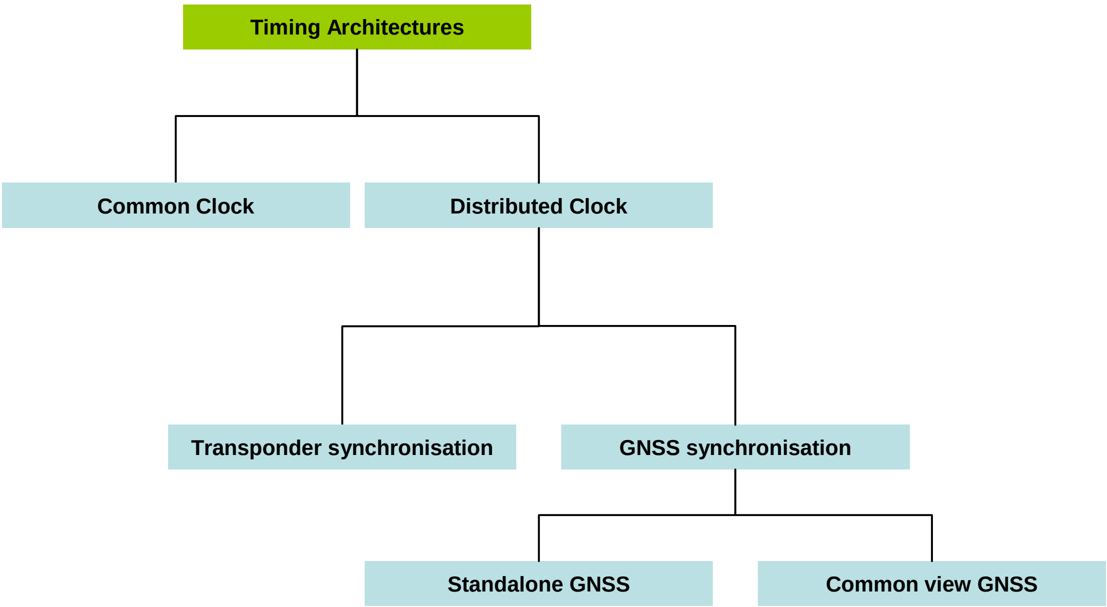


Figure 15: Timing architecture hierarchy

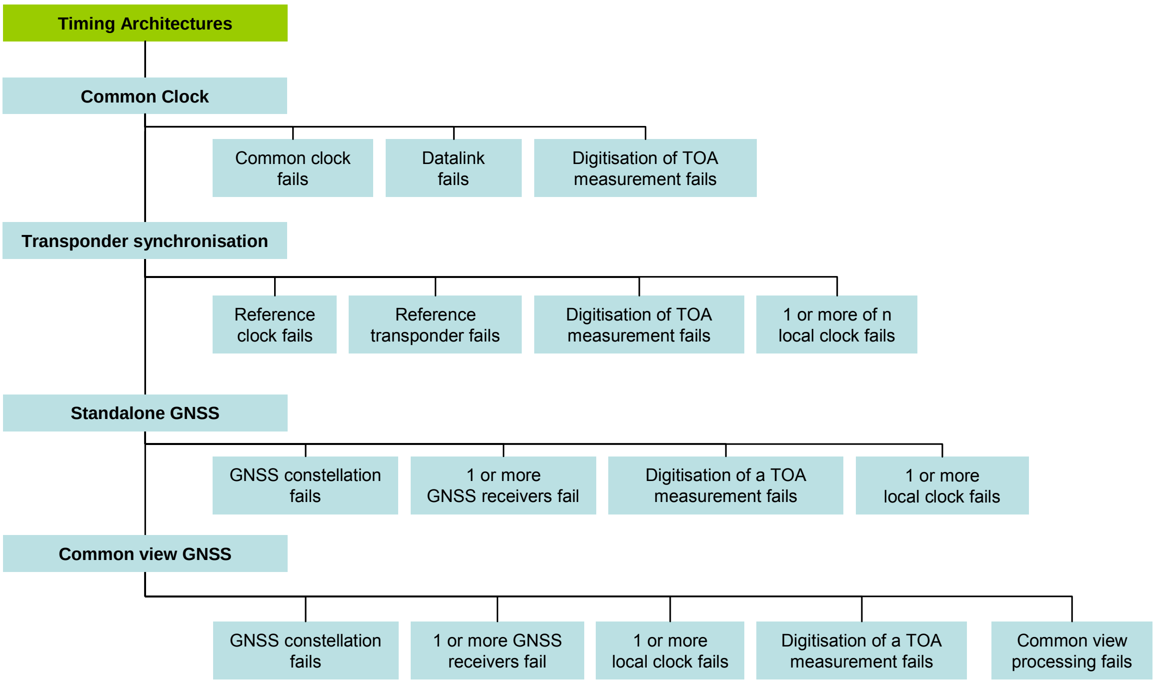

Timing Architectures
Common Clock
Common clock fails
Datalink fails
Digitisation of TOA measurement fails
Transponder synchronisation
Reference clock fails
Reference transponder fails
Digitisation of TOA measurement fails
1 or more of n local clock fails
Standalone GNSS
GNSS constellation fails
1 or more GNSS receivers fail
Digitisation of a TOA measurement fails
1 or more local clock fails
Common view GNSS
GNSS constellation fails
1 or more GNSS receivers fail
1 or more local clock fails
Digitisation of a TOA measurement fails
Common view processing fails

Figure 16: Timing architecture failure modes

Common clock architecture

In a common clock architecture, timing from a single clock is used throughout the system. The common time source is usually distributed to the WAM sensors to allow time stamping at each sensor.

The timing in a common clock system can fail if there is a fault originating within the single system clock itself or by incorrectly communicating its time to the other components of the system either through the data link itself or in the processing (digitising) of the signal. The clock and data link are single points of failure for the whole WAM sub-system,

In this and all architectures, the system can fail if the time of arrival (TOA) measurement fails in the sensor.

Transponder synchronisation architecture

In this system, local clocks are synchronised with by a reference transponder. The reference transponder has its own reference clock and must be in view of all the WAM sensors.

This architecture can fail due to failures in the reference transponder, the reference clock or the local clocks.

Standalone GNSS architecture

In this architecture, the local clocks are synchronised with GNSS time, as derived by a local GNSS receiver.

This system introduces two more possible sources of timing failure in addition to those associated with all distributed clock system. These new failures are GNSS constellation failure and GNSS receiver failure.

Note that a GNSS clock may also be used by other ATC systems as a timing source. This can make GNSS a common failure point for multiple ATC systems. This must be considered in any safety analysis of WAM and is added as a safety requirement (SR30).

Common View GNSS architecture

The architecture is similar to the standalone GNSS architecture, but requires each WAM sensor to derive time from the same GNSS satellites. This can only be achieved with satellites in the “common view” of the WAM sensors. It provides higher accuracy than standalone GNSS architectures.

This architecture broadly has the same failure modes as the standalone GNSS architecture. However, additional processing is required for common view processing which could introduce additional errors.

As for the standalone GNSS architecture, the safety analysis must consider if GNSS timing is used for multiple ATC systems.

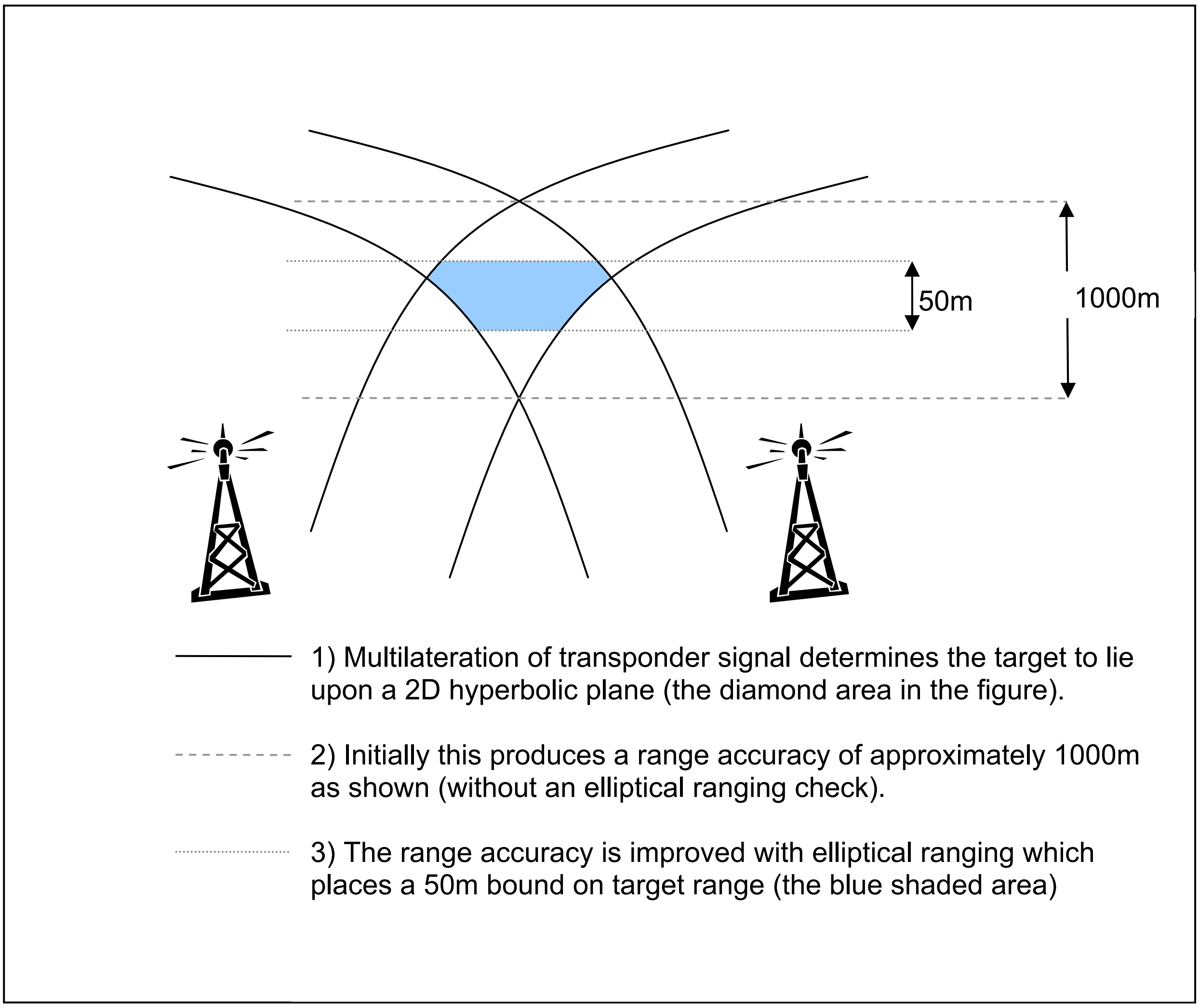
K.2.6 Elliptical Ranging

Elliptical ranging is commonly performed on targets identified by multilateration. It is designed to improve accuracy and to limit the effects of multipath, such as ‘ghost’ tracks:

- **Accuracy improvements** are possible because the multilateration accuracy will vary according to the relative geometry and position of the aircraft and ground sensors. Outside of the area of geometric footprint of the sensors, multilateration accuracy will quickly degrade, although in a complex manner [20] The elliptical range check can provide reasonable accuracy (e.g. 50 m) in a radial direction that reduces the uncertainty of the multilateration position in that direction.

- **Multipath** can be mitigated against because the interrogator/ transponder path should be subject to different multipath than the other sensors. Elliptical ranging can therefore be used to cross-check the multilateration-derived position estimate.

The accuracy improvement from elliptical ranging is illustrated below in Figure 17.



1) Multilateration of transponder signal determines the target to lie upon a 2D hyperbolic plane (the diamond area in the figure).

2) Initially this produces a range accuracy of approximately 1000m as shown (without an elliptical ranging check).

3) The range accuracy is improved with elliptical ranging which places a 50m bound on target range (the blue shaded area)

Figure 17: Example of improvement in WAM derived position accuracy from elliptical ranging

K.2.7 Alternative Scenarios

The following figures and tables illustrate the functional models that were developed for the WAM+ADS-B, WAM+SSR and WAM+PSR scenarios.

K.2.7.1 WAM + ADS-B

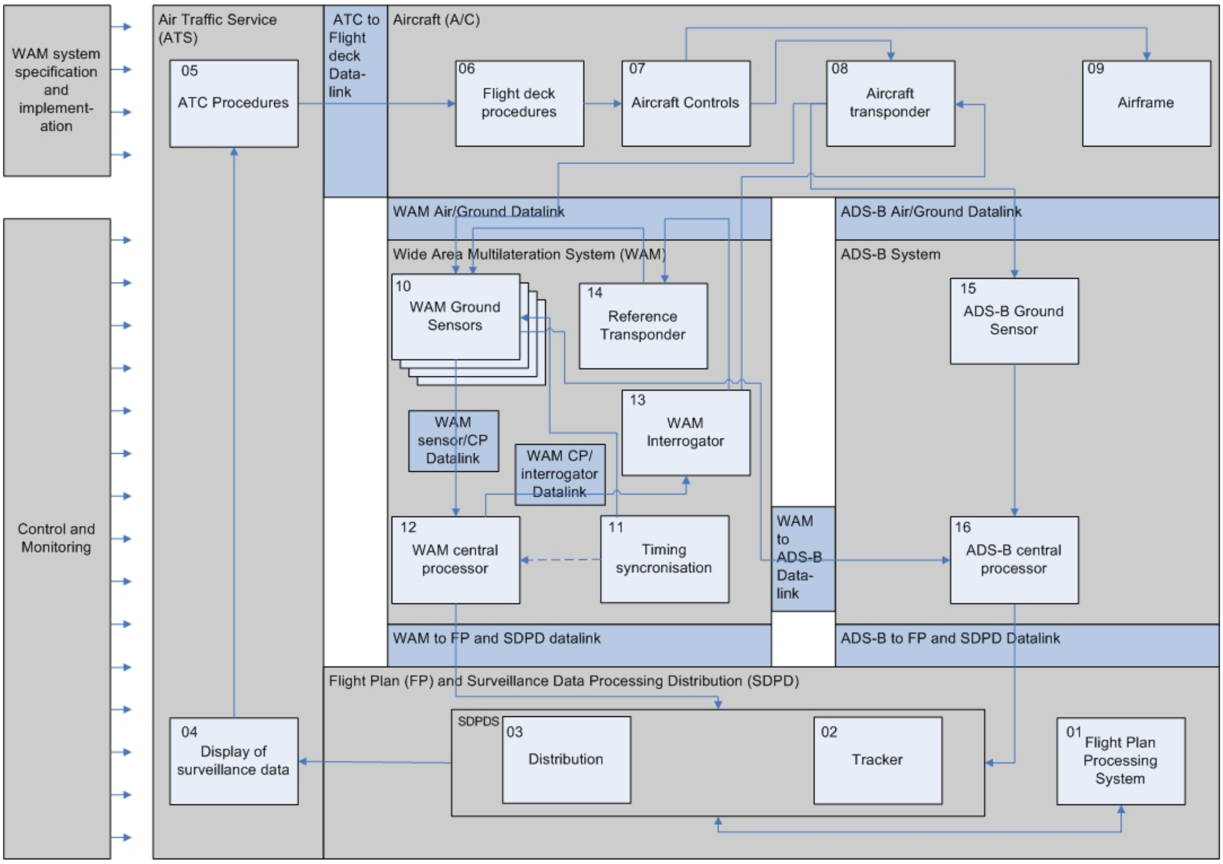

WAM system specification and implement-ation
Control and Monitoring
Air Traffic Service (ATS)
05 ATC Procedures
04 Display of surveillance data
ATC to Flight deck Data-link
Aircraft (A/C)
06 Flight deck procedures
07 Aircraft Controls
08 Aircraft transponder
09 Airframe
WAM Air/Ground Datalink
ADS-B Air/Ground Datalink
Wide Area Multilateration System (WAM)
ADS-B System
10 WAM Ground Sensors
14 Reference Transponder
15 ADS-B Ground Sensor
WAM sensor/CP Datalink
WAM CP/ interrogator Datalink
13 WAM Interrogator
12 WAM central processor
11 Timing syncronisation
WAM to ADS-B Data-link
16 ADS-B central processor
WAM to FP and SDPD datalink
ADS-B to FP and SDPD Datalink
Flight Plan (FP) and Surveillance Data Processing Distribution (SDPD)
SDPDS
03 Distribution
02 Tracker
01 Flight Plan Processing System

Figure 18: Functional model of WAM and ADS-B

A unique aspect of this architecture is the ADS-B central processor is provided with inputs by both the ADS-B and WAM ground sensors. Alternatively, WAM ground sensors may double up as ADS-B ground sensors, with additional functionality in the central Processor to extract the ADS-B data embedded in the received signal. This particular variant is not separately analysed.

Function Ref	Function	Description
15	ADS-B Ground Sensors	Receives the 1090MHz signal broadcast by the aircraft transponder.
16	ADS-B central processor	Decodes and de-garbles the message automatically broadcast by the aircraft. Correlates the replies from different ground stations to check for inconsistencies. Produces a single ‘plot’ for each target.
Data link	ADS-B Air/Ground	Automatic RF broadcasts from aircraft transponders detected by ADS-B sensor(s).
Data link	ADS-B to FP and SDPD	Data link from ADS-B processor CP to Tracker SDPD
Data link	WAM to ADS-B	RF or microwave link from WAM ground sensors detecting squitter to ADS-B processor

Table 26: Safety functions - WAM and ADS-B

K.2.7.2 WAM + SSR

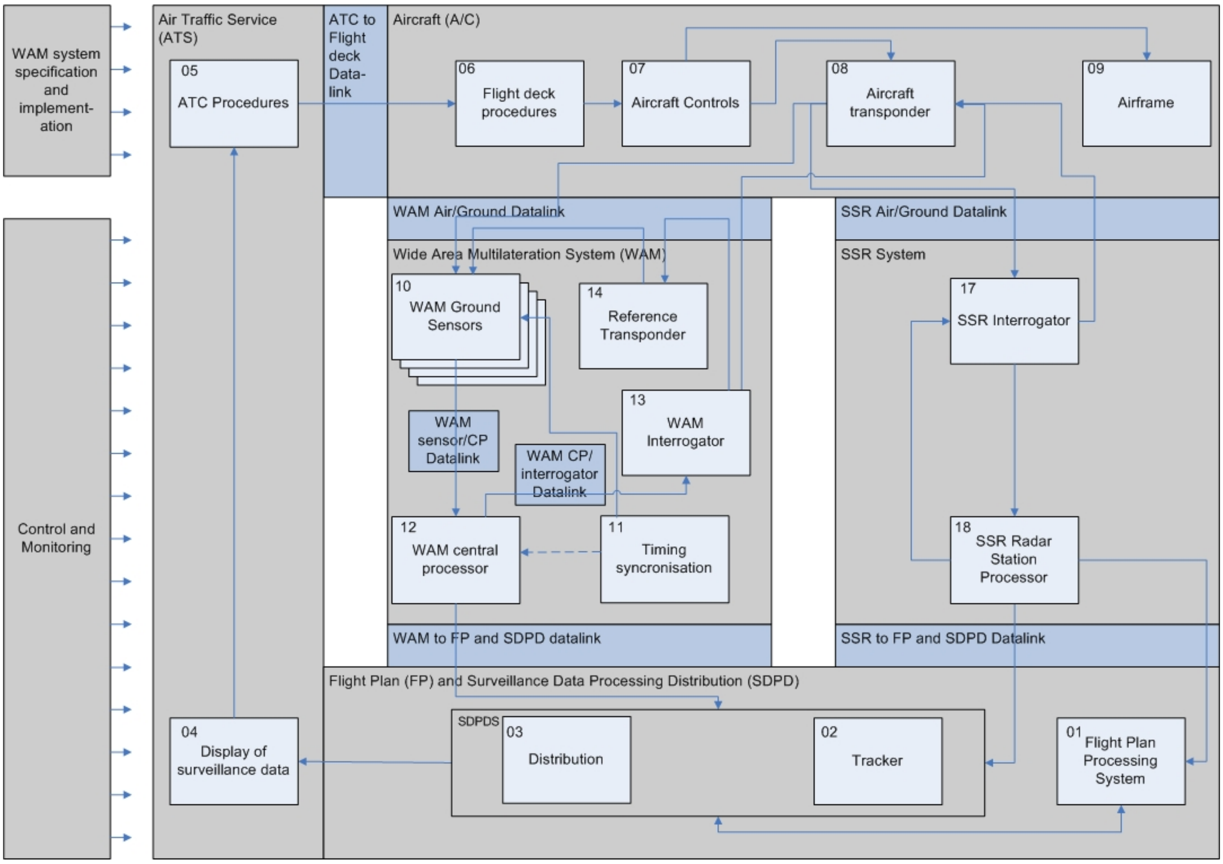

WAM system specification and implement-ation
Control and Monitoring
Air Traffic Service (ATS)
05 ATC Procedures
04 Display of surveillance data
ATC to Flight deck Data-link
Aircraft (A/C)
06 Flight deck procedures
07 Aircraft Controls
08 Aircraft transponder
09 Airframe
WAM Air/Ground Datalink
Wide Area Multilateration System (WAM)
10 WAM Ground Sensors
14 Reference Transponder
13 WAM Interrogator
WAM sensor/CP Datalink
WAM CP/ interrogator Datalink
12 WAM central processor
11 Timing syncronisation
WAM to FP and SDPD datalink
SSR Air/Ground Datalink
SSR System
17 SSR Interrogator
18 SSR Radar Station Processor
SSR to FP and SDPD Datalink
Flight Plan (FP) and Surveillance Data Processing Distribution (SDPD)
SDPDS
03 Distribution
02 Tracker
01 Flight Plan Processing System

Figure 19: Functional model and WAM and SSR

In this architecture the Code call sign receives inputs from both the WAM central processor and the Radar Station Processor. Both the WAM and SSR surveillance system independently interrogate the aircraft transponder and receive individual replies.

Function Ref	Function	Description
17	SSR Interrogator	Interrogates and receives information from the aircraft transponder (be it Modes A/C or Mode S) at 1030MHz and 1090MHz frequencies respectively.
18	Radar Station Processor	Decodes and de-garbles the message requested by the interrogator. Produces a described target at a given point in space.
Data link	SSR Air/Ground	Interrogates and receives RF replies from aircraft transponders.
Data link	SSR to FP and SDPD	Data link from SSR Radar Station Processor to both Tracker SDPD and Code Call sign CD.

Table 27: Safety functions - WAM and SSR

K.2.7.3 WAM + PSR

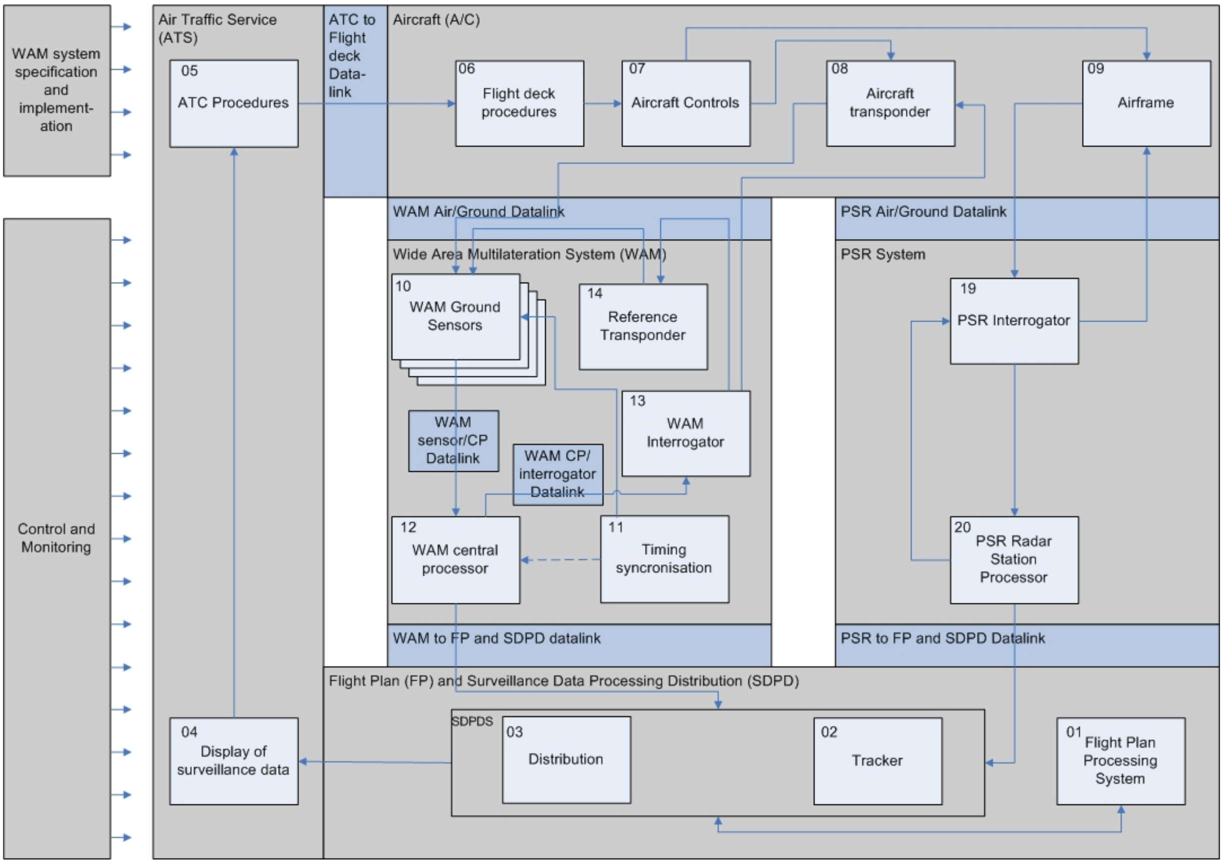

WAM system specification and implement-ation
Control and Monitoring
Air Traffic Service (ATS)
05 ATC Procedures
04 Display of surveillance data
ATC to Flight deck Data-link
Aircraft (A/C)
06 Flight deck procedures
07 Aircraft Controls
08 Aircraft transponder
09 Airframe
WAM Air/Ground Datalink
PSR Air/Ground Datalink
Wide Area Multilateration System (WAM)
10 WAM Ground Sensors
14 Reference Transponder
13 WAM Interrogator
WAM sensor/CP Datalink
WAM CP/ interrogator Datalink
12 WAM central processor
11 Timing syncronisation
PSR System
19 PSR Interrogator
20 PSR Radar Station Processor
WAM to FP and SDPD datalink
PSR to FP and SDPD Datalink
Flight Plan (FP) and Surveillance Data Processing Distribution (SDPD)
SDPDS
03 Distribution
02 Tracker
01 Flight Plan Processing System

Figure 20: Functional model of WAM and PSR

Here the PSR system transmits a pulse and receives the RF echo from the airframe of the aircraft. The surveillance data from the WAM and PSR system is fused at the tracker SDPD.

Function Ref	Function	Description
19	PSR Interrogator	Transmits a radio signal and receives echo information from the airframe.
20	Radar Station Processor	From round trip time and direction of the interrogation signal a 2D target is produced on a horizontal plane based on range and azimuth of the 'echo' produced from the aircraft skin.
Data link	PSR Air/Ground	Interrogates and receives RF echoes from airframe.
Data link	PSR to FP and SDPD	Data link from SSR Radar Station Processor to Tracker SDPD.

Table 28: Safety functions - WAM and PSR

L Example Preliminary System Safety Assessment (PSSA)

L.1 Introduction

The WAM safety assessment contained in this document does not set quantitative Safety Requirements. This is because any allocation of unavailability (Q-values) is dependent on the architecture being examined, and decisions made on trade-offs between system components. This study identifies the causes of hazards qualitatively, but does not prescribe the trade-off decisions (which are also a function of identified internal mitigation means).

It is recognised that merely providing a list of Basic Causes of hazards will not greatly aid implementers. Therefore, a worked example of a fault tree analysis has been developed, to show how realistic failure rates could be ascribed to elements of the system, fault trees built to analyse the achievement or otherwise of safety objectives, and internal mitigation means identified in response to areas where the safety objectives are not being achieved. Recommendations are made at the end of this section for possible internal mitigation means to be used during the implementation of a WAM sub-system.

The fault trees in this annex were created using version 11 of the ‘Fault Tree Plus’ software tool (produced by Isograph software) and are annotated in the accompanying text as appropriate.

This annex is structured as follows:

- Section L.1: as well as introducing the purpose of this annex, it briefly describes the output of Functional Hazard Assessment process and its relevance to this fault tree analysis. This section also mentions the main sources used in the construction of this annex.
- Section L.2 captures the conditions assumed in the construction of the fault trees. They relate the system functionality and its operating environment to the failure probabilities used in subsequent unavailability calculations (the values from which are used in the fault trees).
- Section L.3 derives illustrative unavailability values for system components that contribute towards the causation of the hazards analysed. These values are used in the Fault Trees.
- Section L.4 contains the fault trees and associated analysis for the hazards considered as most severe (i.e. more stringent safety objectives). The unavailability of the system is calculated in each tree and compared against its safety objective specified in the FHA for each hazard.

Annex M captures the safety recommendations resulting from the fault tree analysis, including any of the internal mitigation means identified as being necessary to meet safety objectives for all hazards.

Note that the Functional Models in Annex K have been used in the process of developing the fault trees. In a local safety case, the locally-developed Functional Models will be a useful resource for developing new fault trees.

L.1.1 Results of the FHA

The Functional Hazard Analysis derived safety objectives per hazard identified for the application in question (ATC separation-based service, see section H.4.4). The most stringent safety objectives are identified here, for further analysis in the Preliminary System Safety Assessment (PSSA).

In addition to all hazards concerning position information, the study also looked at some extra causes of faults for the Identification parameter (following concerns over understanding the failure modes), and built fault trees to see if the safety objective was satisfied.

As noted in para 1.8, the severity of position-related hazards was reassessed but the original, more stringent, assessments retained for comparison. The table below shows both original and reassessed hazards together with the derived safety objectives.

Hazard – short description	ID	Variant	Severity (worst credible case)	Safety Objective (per ATSU hour)	
				ER	TMA
Loss of 2D position (or of all parameters).	H01	U1	ER=3	6.0E-1	
			TMA=2		2.8E-2
		D1	4	6.0E-2	2.8E-2
		D-m	ER=3	6.0E-4	
			TMA=2		2.8E-5
Display of erroneous 2D position (i.e. corruption of position)	H02	U1	ER=3	6.0E-1	
			TMA=2		2.8E-2
		U-m	ER=3	6.0E-1	
			TMA=2		2.8E-2
Loss of pressure altitude	H03	U1	5	NA	NA
		D1	4	6.0E-2	2.8E-2
		D-m	3	6.0E-4	2.8E-4
Display of erroneous pressure altitude (i.e. corruption)	H04	U1	ER=3	6.0E-1	
			TMA=2		2.8E-2
		U-m	2	6.0E-2	2.8E-2
Loss of aircraft identity (Call sign)	H05	U1	5	NA	NA
		D1	4	6.0E-2	2.8E-2
		D-m	3	6.0E-4	2.8E-4
Display of erroneous aircraft identity (Call sign) (i.e. corruption)	H06	U1	3	6.0E-1	2.8E-1
		U-m	2	6.0E-2	2.8E-2
Loss of, or display of erroneous, short intent	H07	U	4	6.0E+1	2.8E+1
		D	4	6.0E-2	2.8E-2

Hazard – short description	ID	Variant	Severity (worst credible case)		Safety Objective (per ATSU hour)	
			Revised assessment	Original assessment	ER	TMA
Loss of 2D position (or of all parameters).	H01	U1	ER=3	1	6.0E-4	
			TMA=2	1		2.8E-4
		D-m	ER=3	1	6.0E-7	
			TMA=2	1		2.8E-7
Display of erroneous 2D position (i.e. corruption of position)	H02	U1	ER=3	1	6.0E-4	
			TMA=2	1		2.8E-4
		U-m	ER=3	1	6.0E-4	
			TMA=2	1		2.8E-4

Table 29: List of the hazards analysed in the FHA

L.1.2 Approach

Each fault tree is shown for the scenario where Multilateration is the sole-means of surveillance. The results of the tree are compared against the relevant safety objectives.

The impact of the alternative scenarios (shown in the functional models in Annex K) is considered qualitatively in section L.4.12. For each fault tree there are 3 alternative scenarios: WAM + SSR, WAM + PSR and WAM + ADS-B. The likely impact of each scenario is discussed, but new fault trees for each alternative scenario have not been developed.

If such alternative scenarios are envisaged in an actual implementation, then the appropriate FT should be constructed as part of the PSSA.

L.1.3 Annex Sources

For the example, in order to be reasonably representative, some quantitative values were obtained from Austrocontrol's experience.

L.2 Conditions

The following tables provide a brief description of the technical and operational assumptions used as an example in a typical analysis. In this assessment, they are called "specific conditions" to differentiate them from formal assumptions. It is expected that local ANSPs will review the PSSA conditions used in this document to check that they are consistent with their local case, before re-using them to allocate Safety Requirements in a quantitative manner.

These tables are also contained in Annex F, together with other assumptions, environmental conditions, mitigation means and other considerations that must be taken into account in the complete safety assessment.

The overall purpose of this subsection is to support calculation of illustrative unavailability values that are needed for the detailed (example) FTs in section L4. Each PSSA specific condition in the table is referenced to where it is used in these detailed calculations.

Ref	Section	Description
General		
PSSA01	L.3.1	It is assumed the WAM sub-system has been successfully implemented and meets operational requirements when it is operating correctly. In other words, the system has the required operational coverage with the necessary performance validated throughout the operational area (e.g. by flight tests).
PSSA02	L.3.1	Any other surveillance sub-systems are correctly specified and implemented properly (e.g. no holes in coverage). See [ASSUMP06] and [ASSUMP17].
PSSA03	L.3.1	If the WAM interrogator suffers a detected failure, it is assumed the WAM sub-system shuts down (since it could not guarantee to detect Mode A/C aircraft).
PSSA04	L.3.1	Conversion to/from local WAM co-ordinates to the tracker co-ordinates is assumed to be implemented correctly.
PSSA05	L.3.4.1	A minimal sub-system architecture is assumed (i.e. one that comprises of the fewest possible number of components to meet basic operational requirements). This assumption implies that the failure of, e.g., any WAM sensor or sensor to CP data link will cause surveillance information relating to a target to be lost. It is assumed that only the minimum number of ground sensors required to meet the operational coverage are present.
PSSA06	L.3.4.3	It is assumed traffic includes commercial and GA aircraft entering controlled airspace or requiring a separation service. Of them 90% are assumed to be Mode S equipped.

Table 30: PSSA - General conditions

Ref	Section	Description
System Functionality		
PSSA07	L.3.1	It is assumed that **no system track monitor is present** that raises an alarm if one or more tracks or data items should 'disappear' or show inconsistent data (such as a large jump in position). This reflects expert opinion on the assumptions that can be made for a typical surveillance sub-system.
PSSA08	L.3.2	It is assumed the tracker can accommodate a changed Mode A code during flight whilst keeping the correct aircraft identity. If the technical address (Mode A or 24-bit address) changes in an unpredictable way the tracker will raise an alert to the controller (e.g. by starting a new track with the new Mode A code and by coasting the old one).
PSSA09	L.3.4.2	It is assumed the tracker can process targets with duplicate Mode A or S codes in the same airspace (as long as the targets are distinguishable by the tracker). This is assumed to occur once every 100 ATSU hours.
PSSA10	L.3.1	It is assumed that an elliptical ranging function is present and is used to achieve the required position determination performance together with the TDOA method (how this is achieved by the elliptical ranging and the TDOA methods will vary depending on implementation). See Figure 17.
PSSA11	L.3.1	It is assumed that there exists a function to correlate flight plans with surveillance targets.
PSSA12	L.3.1	It is assumed a separate flight strip processing system is present and that it can continue to operate even if the tracker fails.
PSSA13	L.3.1	It is assumed that the WAM sub-system has a reference transponder that provides a health check function (i.e. checks that its transmissions can be received by the system) and/or time synchronisation function to the system at the sensors.

Table 31: PSSA - System functionality conditions

Ref	Section	Description
Unavailability Calculations		
PSSA14	L.3.1	It is assumed the probability of a failure occurring is distributed equally over all elements that can cause this failure (e.g. the probability of a failure on board an aircraft is equally likely for all aircraft in the airspace [the principal of *equal a priori*]).
PSSA15	L.3.1	The probability of a component failure with time is an exponential decay function: Pr(once or more) = 1 – exp(-t/MTBF) Where the MTBF is the Mean Time Between Failures and t is time. (this assumes independent failures)
PSSA16	L.3.1	When calculating failure rates, it is assumed aircraft do not have a redundant transponder or antenna sub-system. Whilst many aircraft in fact do, it is known that failures of the transponder/antenna sub-system can remain undetected by the aircrew with the consequence that the redundant sub-system is not activated. Therefore no benefit is taken for the redundant sub-systems.
PSSA17	L.3.1	It is assumed that the MTBF used are constant with time (i.e. improved failure rates in the future are not considered).
PSSA18	L.3.1	Unavailability is formally defined as: Q = 1 – (MTBF/(MTBF+MTTR)) Where MTTR is the Mean Time To Repair of the component. All unavailabilities used in the fault trees are calculated for an operational hour of the Air Traffic Service Unit (ATSU).
PSSA19	L.3.3.5	It is assumed that a component is considered as failing if it is unavailable for 30 seconds or more (equivalent to 3 update periods on the CWP or the length of time an extrapolation function in the tracker might last for).

Table 32: PSSA - Unavailability calculation assumptions

Ref	Section	Description
Failure Probabilities and MTBFs		
PSSA20	L.3.2 L.3.3.1	It is assumed the airborne transponder or antenna failure probability is 1E-4 per flight hour [17]. The MTTR is assumed to be the transit time in the sector (i.e. once the failure has occurred it continues for the duration of the flight in the sector but is fixed before the aircraft returns). This is a worst case since it assumes the failure occurs soon after or before entry to the sector.
PSSA21	Table 36	It is assumed that the WAM sub-system reference transponder has the same failure probability as one airborne transponder (1E-4 per flight hour).
PSSA22	L.3.3.2	It is assumed that an airborne transponder failure from RF pollution is 100 times less likely than other possible transponder failures.
PSSA23	L.3.3.3	For transponders that lie within the surveillance coverage it is assumed that one every 1000 ATSU hours does not meet the ICAO specification.
PSSA24	L.3.3.4	It is assumed that the probability of the aircrew entering an incorrect mode A code is 1E-3 per entry. It is assumed that the Mode A code is set once per flight hour on average [18,17].
PSSA25	L.3.3.5	Incorrect decoding of a message may be due to overlapping messages, caused by multipath or FRUIT overload for example. [19] gives approximately 5% decoding probability for a single extended squitter at a 60 mile range in very high density airspace. In low density airspace this probability increases to an average of 15%. It is assumed that the generic surveillance environment is of medium density, so an average of these two figures is taken to give an average decoding probability of 10%. [Note that this requirement has been added to by safety recommendation Rec1, which increases the probability of decode to 15%].
PSSA26	L.3.3.5	It is assumed that the WAM interrogator can repeat an interrogation in 0.5s if no correctly decoded position is available from the previous interrogation.
PSSA27	L.3.4.2	It is assumed that for 10% of the flight duration [16] the aircraft are close enough to cause very closely spaced Mode A replies.
PSSA28	L3.4.3	It is assumed that the probability of there being a duplicated 24 bit address present in the surveillance airspace is 1E-4 per flight [16].
PSSA29	L.3.5.1	Drawing upon operational experience based upon the Austro Control system the MTBF for the WAM interrogator was estimated to be 25000 ATSU hours (approximately three years). The MTTR is assumed to be 1 ATSU hour.

Ref	Name	Description
Failure Probabilities and MTBFs		
PSSA30	L.3.5.2	It is assumed that the failure probability and MTTR for each WAM sensor is the same as that for the ground system interrogator.
PSSA31	L.3.5.3 L.3.5.4	Operational experience has shown the failure probability of the WAM data link to be in the region of 1E-3 to 1E-4 per ATSU hour. A mid-way value of 5E-4 has been assumed. MTTR is assumed to be 1 ATSU hour.
PSSA32	L.3.5.6	It is assumed that other static ground system components, such as the tracker, SDP alarm, CWP and WAM central processor have a failure rate of 1E-5 per ATSU hour. The MTTR is assumed to be one ATSU hour.
PSSA33	L.3.5.5	It is assumed that the WAM timing sub-system has a failure rate of MTBF 1E-5 and MTTR of 1 hour.

Table 33: PSSA - failure probabilities and MTBF assumptions

L.3 Unavailability Derivation

L.3.1 Introduction

This section contains the derivation of illustrative unavailabilities (Q) used in the fault trees. These calculations are illustrative only and must not be used uncritically. They are offered to illustrate how parameters in the PSSA may be calculated from traffic statistics and known equipment failure rates, etc.

To calculate the unavailability, a number of core assumptions have been made about the successful implementation of the WAM sub-system:

- (PSSA01) It is assumed the WAM sub-system has been successfully implemented and meets operational requirements when it is operating correctly. In other words, the system has the required operational coverage with the necessary performance validated throughout the operational area (e.g. by flight tests).

- (PSSA02) Any other surveillance sub-systems are correctly specified and implemented properly (e.g. no holes in coverage).

- (PSSA03) If the WAM interrogator suffers a detected failure, it is assumed the WAM sub-system shuts down

- (PSSA04) Conversion to/from local WAM co-ordinates to the tracker co-ordinates is assumed to be implemented correctly.

A number of assumptions about the generic WAM implementation have also been made:

- (PSSA07) It is assumed that no system track monitor is present that raises an alarm if one or more tracks or data items should ‘disappear’ or show inconsistent data (such as a large jump in position).

- (PSSA10) It is assumed that an elliptical ranging function is present and is used to achieve the required position determination performance together with the TDOA method (how this is achieved by the elliptical ranging and the TDOA methods will vary depending on implementation).
- (PSSA11) It is assumed that there exists a function to correlate flight plans with surveillance targets.
- (PSSA12) It is assumed a separate flight strip processing system is present and that it can continue to operate even if the tracker fails.
- (PSSA13) It is assumed that the WAM sub-system has a reference transponder that provides a health check function (i.e. checks that its transmissions can be received by the system) and/or time synchronisation function to the system at the sensors.

Also, a number of mathematical assumptions are required to calculate the unavailability:

- (PSSA14) It is assumed the probability of a failure occurring is distributed equally over all elements that can cause this failure (e.g. the probability of a failure on board an aircraft is equally likely for all aircraft in the airspace [the principal of equal a priori]).
- (PSSA15) The probability of a component failure with time is an exponential decay function: Pr(once or more) = 1 – exp(-t/MTBF). Where the MTBF is the Mean Time Between Failures and t is time.
- (PSSA16) When calculating failure rates, it is assumed aircraft do not have a redundant transponder or antenna system. Whilst many aircraft in fact do, it is known that failures of the transponder/antenna sub-system can remain undetected by the aircrew with the consequence that the redundant sub-system is not activated. Therefore no benefit is taken for the redundant sub-systems.
- (PSSA17) It is assumed that the MTBF used are constant with time (i.e. improved failure rates in the future are not considered).
- (PSSA18) Unavailability is formally defined as follows:
  Q=1–(MTBF/(MTBF+MTTR)),
  where MTTR is the Mean Time To Repair of the component. All unavailabilities used in the fault trees are calculated for an operational hour of the Air Traffic Service Unit (ATSU).

Calculation of Q (unavailability)

The calculation of Q is based upon the assumption that the service provided by the component in question will become unavailable when the component fails, thus Q is indicative of the probability of a failure occurring. Unavailability is calculated from a known or assumed Mean Time Between Failure (MTBF) and a Mean Time To Repair (MTTR). The MTBF is the mean time interval during which the system or equipment performs its mission to within the requirements specified. The MTTR is the average time the component is unavailable for following failure and subsequent maintenance – this includes corrective/preventive maintenance that results in system unavailability. As the derived values are indicative only they have been given to an accuracy of 1 decimal place.

For the purposes of this study, all failure rates are calculated per hour of ATSU operation so the unavailability (“Q”) values derived give the non-availability for a given component or function per ATSU hour. The Q values can depend upon the type of airspace (TMA or en-route), the number of aircraft (1 or more than 1) or be common across an (assumed) system.

Unavailability is defined by ‘Q’ = 1 – (MTBF/(MTBF+MTTR))

L.3.2 Unavailability Derivation for Airborne Components

For airborne components, the MTTR is assumed (PSSA20) to be the transit time of the aircraft in the sector:

So $MTTR_{TMA}$ = 0.1 ATSU hours

and

$MTTR_{en\text{-}route}$ = 0.3 ATSU hours

A binomial expansion gives the probability distribution P of obtaining exactly n cases out of N Bernoulli trials in the formula:

$P(n|N) = (N!/n!(N-n)!)p^nq^{N-n}$.

Where:

- q = 1-p
- p is the probability of obtaining a given result in one trial
- N is the number of trials (i.e. the maximum number of aircraft simultaneously in the sector)
- p is the probability of failure (per flight hour).

From assumption [ASSUMP08], the maximum instantaneous count of traffic in the en-route and TMA airspace is

N_{TMA} = 15 aircraft and $N_{en\text{-}route}$ = 20 aircraft.

1) For one aircraft component failing

The probability of one case (event) occurring has n = 1 so

$P = (N!/(N-1)!)\ p\ (1-p)^{N-1}$

$P = Np(1-p)^{N-1}$

As $p \rightarrow 0$ then $(1-p)^{N-1} \rightarrow 1$. So for small p:

$P \approx Np$

Assuming probability of failure with time is an exponential decay function:

$P = 1 - \exp(-t/MTBF)$

Where the MTBF is the Mean Time Between Failures and t is time.

As $\exp(-x) = 1 - x + (x^2/2) - (x^3/6) + \ldots$

When x is small:

$\exp(-x) \approx 1 - x$

so:

$P \approx (t/MTBF)$

Defining the ATSU hour as being the unit of a trial makes t = 1 ATSU hour so:

$P \approx (1/MTBF)$, which can be re-written as:

$\underline{MTBF \approx 1/Np}$

for a single aircraft failure.

2) For more than one aircraft failing

The dominant probability in this case is the simultaneous failure of components on two aircraft, because the probability of occurrence for 3 or more is negligible by comparison since p is small in the formula $P = (N!/(N-1)!)\ p\ (1-p)^{N-1}$).

So using n = 2:

$MTBF = 1/P(\text{more than one aircraft component fails})$

$\approx 1/((N!/2!(N-2)!)p^2(1-p)^{N-2})$

L.3.3 Number of Aircraft Dependant Q Values

L.3.3.1 Aircraft Transponder Failure

The MTBF per transponder (including the antenna) is assumed to be 1E4 flight hours (PSSA20), using the formula presented in section L.3.2 gives:

<u>For one aircraft:</u>

Q_{TMA} = 2.6E-04

$Q_{\text{en-route}}$ = 6.7E-04

<u>For more than one aircraft:</u>

Q_{TMA} = 1.8E-07

$Q_{\text{en-route}}$ = 6.3E-07

L.3.3.2 Transponder Pollution

It is assumed (PSSA22) that a transponder failure from RF pollution is 100 times less likely than other transponder failures.

Failure of due to transponder RF pollution therefore has a probability of failure of 1E-6 which gives an unavailability of:

<u>For one aircraft:</u>

Q_{TMA} = 2.6E-06

$Q_{\text{en-route}}$ = 6.7E-06

<u>For more than one aircraft:</u>

Q_{TMA} = 1.8E-11

$Q_{\text{en-route}}$ = 6.3E-11

L.3.3.3 Transponder out of ICAO Specification

For transponders that lie within the surveillance coverage it is assumed (PSSA23) that one every 1000 ATSU hours does not meet the ICAO specification, giving a failure rate of 1E-3.

Failure due to transponder out of specification therefore has an unavailability of:

<u>For one aircraft:</u>

Q_{TMA} = 2.5E-3

$Q_{\text{en-route}}$ = 6.6E-3

<u>For more than one aircraft:</u>

Q_{TMA} = 1.8E-5

$Q_{\text{en-route}}$ = 6.2E-5

L.3.3.4 Mode A Code Entry Error by Pilot

It is assumed (PSSA24) that the probability of the aircrew entering an incorrect mode A code is 1E-3 per entry and that the Mode A code is set once per flight hour on average.

Therefore, failure due to incorrect Mode A code error has an unavailability of:

<u>For one aircraft:</u>

Q_{TMA} = 2.5E-3

$Q_{en\text{-}route}$ = 6.6E-3

<u>For more than one aircraft:</u>

Q_{TMA} = 1.8E-5

$Q_{en\text{-}route}$ = 6.2E-5

L.3.3.5 Incorrect Message Decode

It is assumed (PSSA25) that the probability of incorrect message decode is 10%. It is assumed (PSSA19) that a component (e.g. track) is considered failed if it is unavailable for 30s.

It is assumed (PSSA26) that a WAM interrogator can repeat an interrogation in 0.5s.

Therefore correct decoding of consecutive transponder replies has an unavailability of:

P(Outage) = P(60 consecutive replies are not received)

= 0.9^{60}

= 1.8E-3 per aircraft

I.e. 10% of replies are decoded incorrectly.

<u>For one aircraft</u>

Q_{TMA} = 4.6E-03

$Q_{en\text{-}route}$ = 1.2E-02

<u>For more than one aircraft:</u>

Q_{TMA} = 5.7E-5

$Q_{en\text{-}route}$ = 2.0E-4

L.3.4 Airspace Dependent Q Values

L.3.4.1 Multipath Effects

The probability of a failure due to multipath depends upon the number of sensors and aircraft within the coverage volume. It is assumed (ASSUMP08) that the maximum instantaneous count of traffic in the sector is 20 in the en-route and 15 in the TMA.

For TMA airspace, therefore:

$P(\text{single sensor experiences multipath})_{TMA} = 1.0E\text{-}5 \times 15$

$= 1.5E\text{-}4$

Assuming that the target is detected by a minimal system:

$P(\text{Multipath failure})_{TMA} =$

$N(\text{number of sensors}) \times p(\text{single sensor experiences multipath})_{TMA}$

$= 4 \times (1.5E\text{-}4)$

$= 6.0E\text{-}4$

$MTBF_{TMA} = 1/P$

$= 1.7E3$ ATSU hours

Assuming MTTR = 1 ATSU minute (0.017 ATSU hours) then:

$Q_{TMA} = 1.0E\text{-}5$.

For en-route airspace:

$p(\text{single sensor experiences multipath})_{en\text{-}route} = 1.0E\text{-}5 \times 20$

$= 2.0E\text{-}4$

It is assumed (PSSA05) that the target under surveillance is detected by a minimal system, i.e. one that is comprised of only 4 sensors. This means that a failure at one will cause data relating to the target to be lost:

$P(\text{Multipath failure})_{en\text{-}route} =$

$N(\text{number of sensors}) \times p(\text{single sensor experiences multipath})_{en\text{-}route}$

$= 4 \times (2.0E\text{-}4)$

$= 8.0E\text{-}4$

$MTBF_{en\text{-}route}$ = 1/P

= 1.3E+3 ATSU hours

Assuming (ASSUMP08) MTTR = 1 ATSU minute (0.017 ATSU hours) then:

$Q_{en\text{-}route}$ = 1.4E-5

L.3.4.2 Closely Spaced Mode A Replies

It is assumed (PSSA09) that a duplicated Mode A code occurs once every 100 ATSU hours in a full sector.

It is assumed (PSSA27) that for 10% of the flight duration the aircraft are close enough to cause very closely spaced Mode A replies.

For the TMA the MTTR = 0.17 ATSU hours (PSSA20 and ASSUMP08) so:

Q_{TMA} = 1.7E-4

For the en-route the MTTR = 0.33 ATSU hours (PSSA20 and ASSUMP08) so:

$Q_{en\text{-}route}$ = 3.3E-4

L.3.4.3 Duplicated 24 Bit Address

It is assumed that 90% of aircraft are Mode S equipped (assumption PSSA06) and for these aircraft the probability of a duplicated 24 bit address is 1E-4 per flight (assumption PSSA28). Therefore, the overall probability of its occurrence is:

0.9 x 1 E-4 = 9.0E-5 per flight.

From assumption (ASSUMP08) 45 flights are handled en-route per ATSU hour while in the TMA 40 flights are handled per hour.

So the failure probabilities are:

9E-5 x 40 = 3.6E-3 per ATSU hour in the TMA

9E-5 x 45 = 4.1E-3 per ATSU hour in the en-route.

This gives MTBFs of:

$MTBF_{TMA}$ = 2.7E+2 ATSU hours in the TMA

$MTBF_{en\text{-}route}$ = 2.4E+2 ATSU hours in the en-route

Using a MTTR equal to the average sector transit time (ASSUMP08) produces an unavailability of:

Q_{TMA} = 6.1E-4

$Q_{en\text{-}route}$ = 1.3E-3

L.3.5 System Wide Q Values

The unavailability of these ground system components is independent of the type of airspace they are monitoring, so all Q values are the same for TMA and en-route airspace.

L.3.5.1 WAM Interrogator (Transmitter Failure)

It is assumed (PSSA29) that the WAM interrogator MTBF is 25000 hours and the MTTR is 1 hour. Therefore, the unavailability is estimated to be:

Q = 4.0E-5

L.3.5.2 WAM Sensor (Receiver Failure)

It is assumed (PSSA30) that the probability of failure of a sensor is :

p = 1/25000 = 4.0E-5.

As the probability of failure of any sensor is approximately equal to:

$P \approx Np$

If no sensor redundancy exists (i.e. 4 sensor coverage):

P(failure to do WAM sensors)

= 4 x (4.0E-5)

= 1.6E-4

MTBF = 1/P

= 6.3E3 ATSU hours

This gives a WAM sensor unavailability of:

Q = 1.6E-4.

L.3.5.3 WAM Data link (from Sensor to CP)

The same logic applies for WAM sensors and assuming (PSSA31) that the data link MTBF is 5E-4 and MTTR is 1 hour:

P(failure due to data link)

= N(number of data links) x p(a single data link fails)

= 4 x (5.0E-4)

= 2.0E-3

MTBF = 1/P

= 500 ATSU hours

So WAM data link unavailability is:

Q = 2.2E-3.

L.3.5.4 WAM Data link (From CP Tracker)

It is assumed (PSSA31) that the data link MTBF is 5E-4 and MTTR is 1 hour. Therefore, the unavailability is estimated to be:

Q = 5.0E-4.

L.3.5.5 WAM Timing Sub-system

It is assumed (PSSA33) that the WAM timing sub-system has an MTBF of 1E-5 and MTTR of 1 hour, giving:

Q = 1.0E-5.

WAM timing sub-system architectures are discussed in Annex K.2.5.

Note that GNSS can be a single point of failure across multiple ATC systems. If GNSS is part of the WAM timing sub-system then this failure condition should be checked.

L.3.5.6 Non-WAM ground components

It is assumed (PSSA32) that the non-WAM static ground components (i.e. tracker and surveillance display) have MTBF of 1E-5 and MTTR of 1 hour, giving:

Q = 1.0E-5.

L.4 Fault Trees for Most Critical and Severe Hazards

This section gives an example fault tree, followed by the fault trees for the most critical hazards.

Each hazard is either detected of undetected by the controller. Note however that in the fault trees they are *all* undetected by the ATC system. In other words, every individual fault described here is undetected by the ATC system (whether or not it is detected by the controller). If it were detected, some kind of system alarm could be raised that would alert the controller.

The unavailability values in the fault trees shown below are for TMA airspace, except for Hazard H01-Dmany where both TMA and en-route trees are shown to illustrate the different numbers achieved. (Hazard H01-Dmany has been chosen because it is a large tree which must be revised to meet the safety objectives.)

In all cases, identical fault trees have been constructed for the en-route, (the Q values used in both cases are shown in the table accompanying the fault trees).

Following each fault tree is a comparison of the two top level unavailability values for the TMA and en-route airspace against their safety objectives as specified in the FHA.

L.4.1 Example Tree

Figure 21 shows a typical fault tree for a given hazard. A description of the top level hazard identified in the FHA is provided in the top box, together with a hazard reference (e.g. H01-Dmany). This top box also represents the top gate in the tree, in the example below this is an OR gate. Events in the tree have circles symbols. The unavailability (Q value) used is shown below the event it relates to, as is the Q value calculated at every gate in the tree. The trees presented are the results of an iterative analysis procedure which seeks to include only the credible (rather than conceivable) events that contribute towards a particular hazard.

In the following diagrams, Q should be interpreted in terms of ATSU hours, e.g. Q=1e-1 means an unavailability of 1 hour per 10 ATSU hours, (i.e. an availability of 9 hours per 10 ATSU hour).

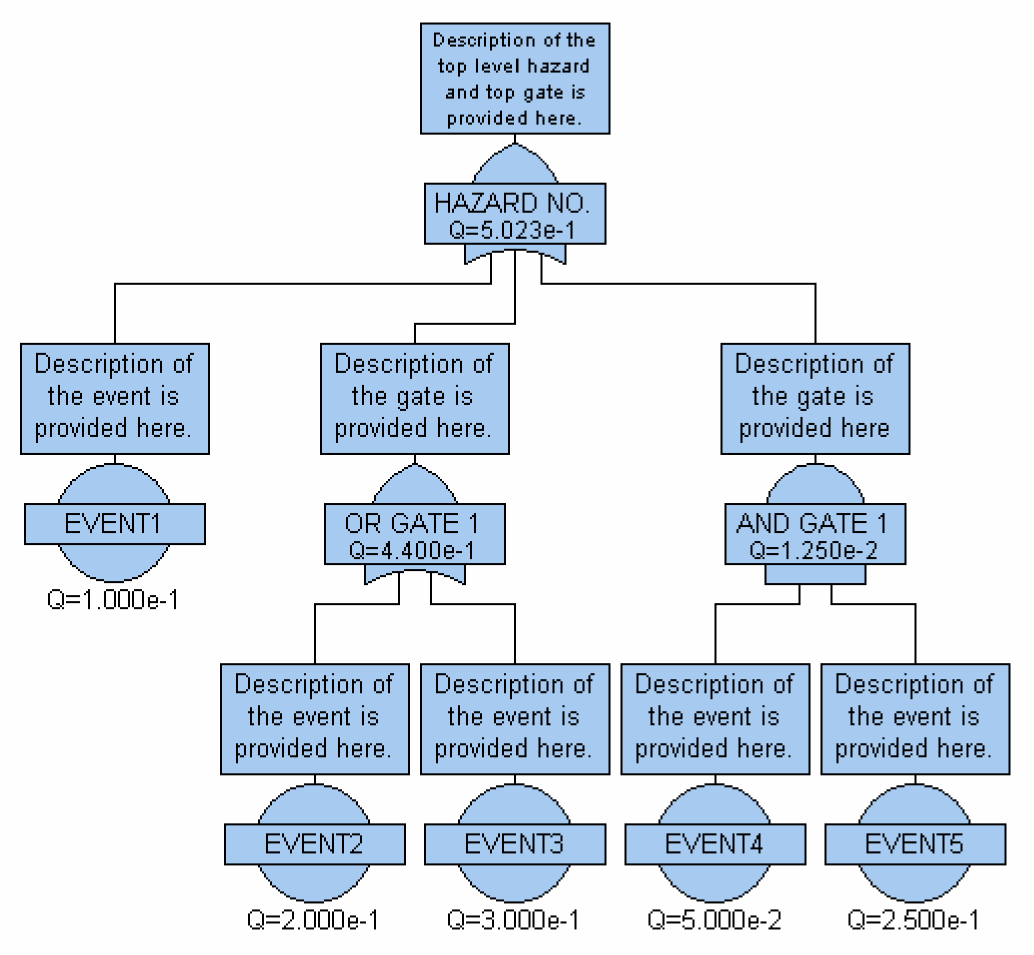

Description of the top level hazard and top gate is provided here.
HAZARD NO.
Q=5.023e-1
Description of the event is provided here.
EVENT1
Q=1.000e-1
Description of the gate is provided here.
OR GATE 1
Q=4.400e-1
Description of the gate is provided here
AND GATE 1
Q=1.250e-2
Description of the event is provided here.
EVENT2
Q=2.000e-1
Description of the event is provided here.
EVENT3
Q=3.000e-1
Description of the event is provided here.
EVENT4
Q=5.000e-2
Description of the event is provided here.
EVENT5
Q=2.500e-1

Figure 21: An example fault tree

A key to the symbols used in the tree is shown below

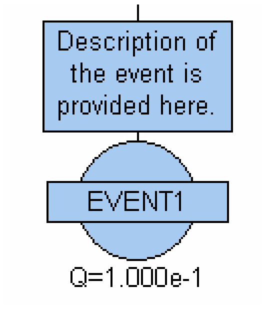
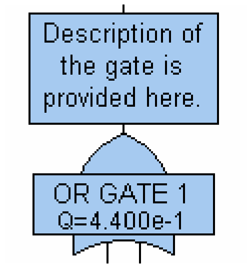
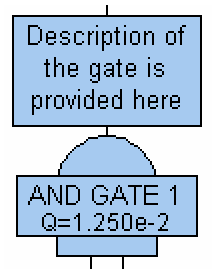
Symbol	Name	Description
 Description of the event is provided here. EVENT1 Q=1.000e-1	Event	The initial 'events' (or 'failures') that lead to the overall top level hazard are described within these symbols, together with a failure probability expressed as a "Q" value (see section L.3.1 for explanation). These values have been justified in this document by providing a cross-reference either to an appropriate external source or a derivation contained in section L.3.
 Description of the gate is provided here. OR GATE 1 Q=4.400e-1	OR gate	These produce Q values based on the condition that at least one of the events feeding into it occurs (thus it describes the total probability of one or more failure conditions occurring). For example when two Boolean (success or fail) events (1 and 2) feed into an OR gate with failure probabilities of P_1 and P_2 the probability calculated at the gate is equal to: P_{Gate}= P(Only event 1 occurs) + P(Only event 2 occurs) + P(Events 1 and 2 occur) $= (P_1x(1-P_2)) + (P_2x(1-P_1)) + P_1P_2$
 Description of the gate is provided here AND GATE 1 Q=1.250e-2	AND gate	These gates produce Q values based on the condition that both events occur simultaneously. The unavailability values produced are the result of a multiplicative operation on the events leading into the gate.

Table 34: Fault tree symbols used

L.4.2 Hazard H01-U1: Undetected Loss of 2D Position for One Aircraft

L.4.2.1 General

This hazard is interpreted to mean that the track and label is lost from the CWP for a single aircraft. However the flight strip information is still present for that aircraft.

L.4.2.2 WAM Sole Means Scenario

The figure below shows the fault tree for this hazard with probabilities calculated for the terminal area. Additional notes are provided in the accompanying table.

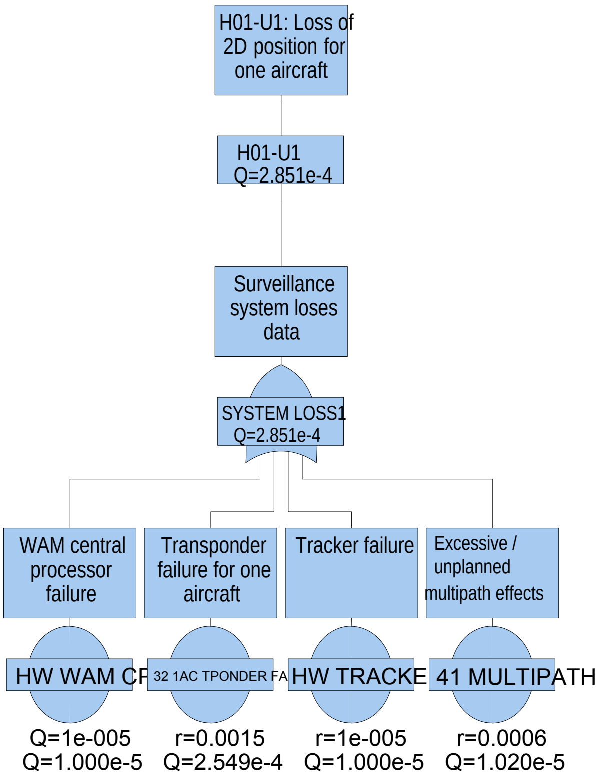

H01-U1: Loss of 2D position for one aircraft
H01-U1
Q=2.851e-4
Surveillance system loses data
SYSTEM LOSS1
Q=2.851e-4
WAM central processor failure
Transponder failure for one aircraft
Tracker failure
Excessive / unplanned multipath effects
HW WAM CF
32 1AC TPONDER FA
HW TRACKE
41 MULTIPATH
Q=1e-005
Q=1.000e-5
r=0.0015
Q=2.549e-4
r=1e-005
Q=1.000e-5
r=0.0006
Q=1.020e-5

Figure 22: Hazard H01-U1 (Undetected loss of 2D position for 1 aircraft)

Gate or Event		Failure
OR	SYSTEM LOSS	The aircraft track and label is not shown on the CWP.
	WAM CP FAILURE	Failure of WAM CP to process a track for one aircraft.
	1AC TPONDER FAILURE	Failure of one aircraft transponder due to equipment reasons.
	TRACKER FAILURE	Failure of the tracker.
	EXCESSIVE/UNPLANNED MULTIPATH	Multipath causes a corrupt position to be reported which is discarded after comparison with elliptical ranging check.
	ANTENNA MASKING	**Discarded.** Considered but discarded because it is short duration and so does not represent a viable failure for a continuous loss.
	OVER INTERROGATION	**Discarded.** Considered but discarded because it is not credible to cause an outage of significant duration.

Table 35: Additional notes for Hazard H01-U1

The results of the fault tree analysis are listed in the following table with a comparison of the Q value achieved against that specified as the safety objective.

Assessment	Airspace	Safety objective (per ATSU hour)	'Q' achieved (per ATSU hour)	Result
Revised assessment	En-route	6.0E-1	7.0E-4	Exceeded by 2 orders of magnitude
	Terminal	2.8E-2	2.9E-4	
Original assessment	En-route	6.0E-4	7.0E-4	Similar order of magnitude
	Terminal	2.8E-4	2.9E-4	

Table 36: Results for Hazard H01-U1 with initial fault tree

Since the safety objective is achieved with a margin of two orders of magnitude, we do not investigate additional mitigations to increase the availability. Therefore, no additional safety requirements are generated from this hazard.

Even for the more stringent original assessment, the safety objective is met.

L.4.3 Hazard H01-Dmany: Detected Loss of 2D Position for More than One Aircraft

L.4.3.1 General

This hazard is interpreted to mean that the track and label is not shown on the CWP for multiple aircraft. However, the flight strip information for those aircraft is still present.

L.4.3.2 WAM Sole Means Scenario

The figure below shows the fault trees for this hazard with probabilities calculated for both the terminal area and en-route. Additional notes are provided in the accompanying table.

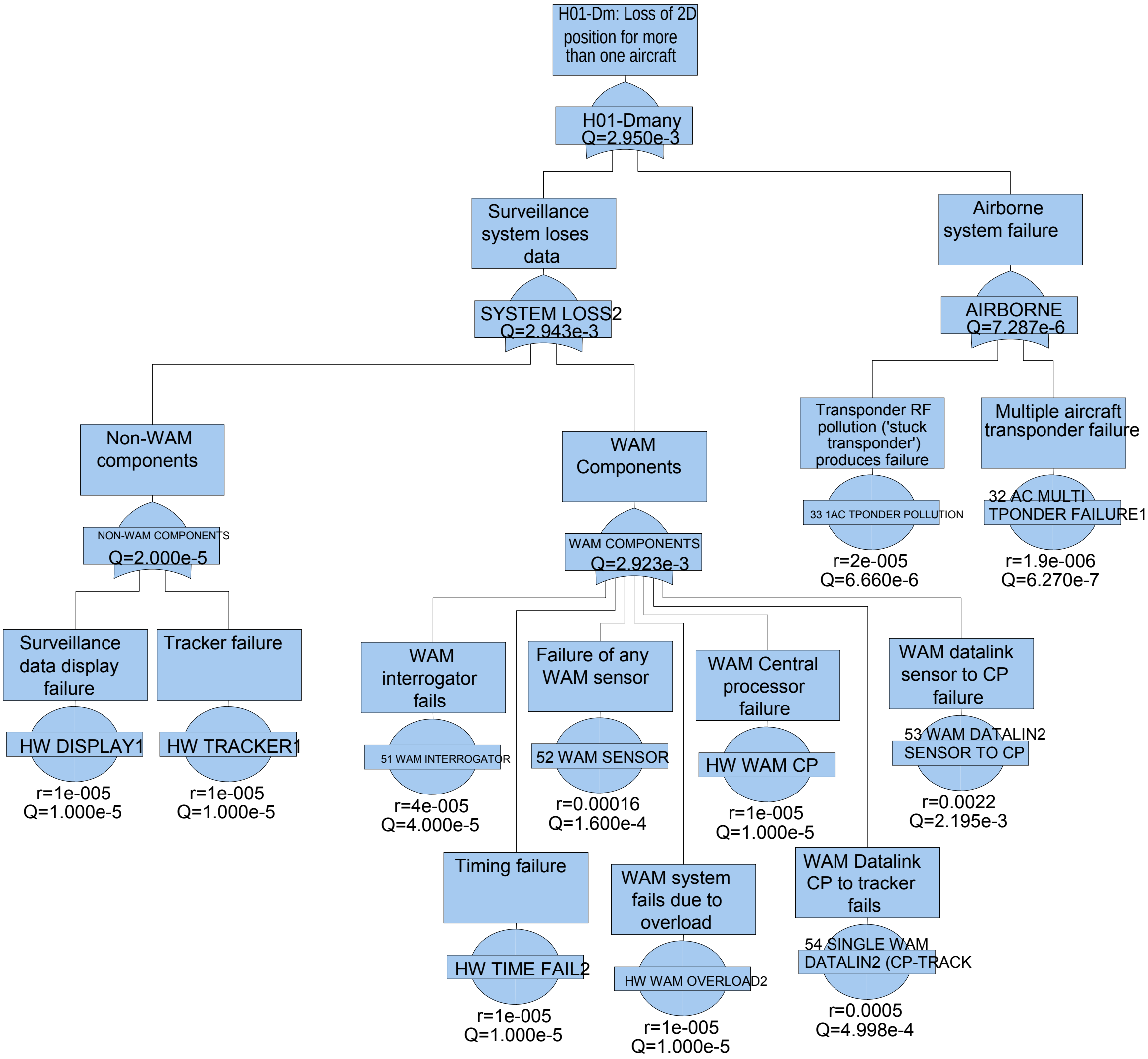


Figure 23: Hazard H01-Dmany (Detected loss of 2D position for multiple aircraft). En-route case (without redundancy)

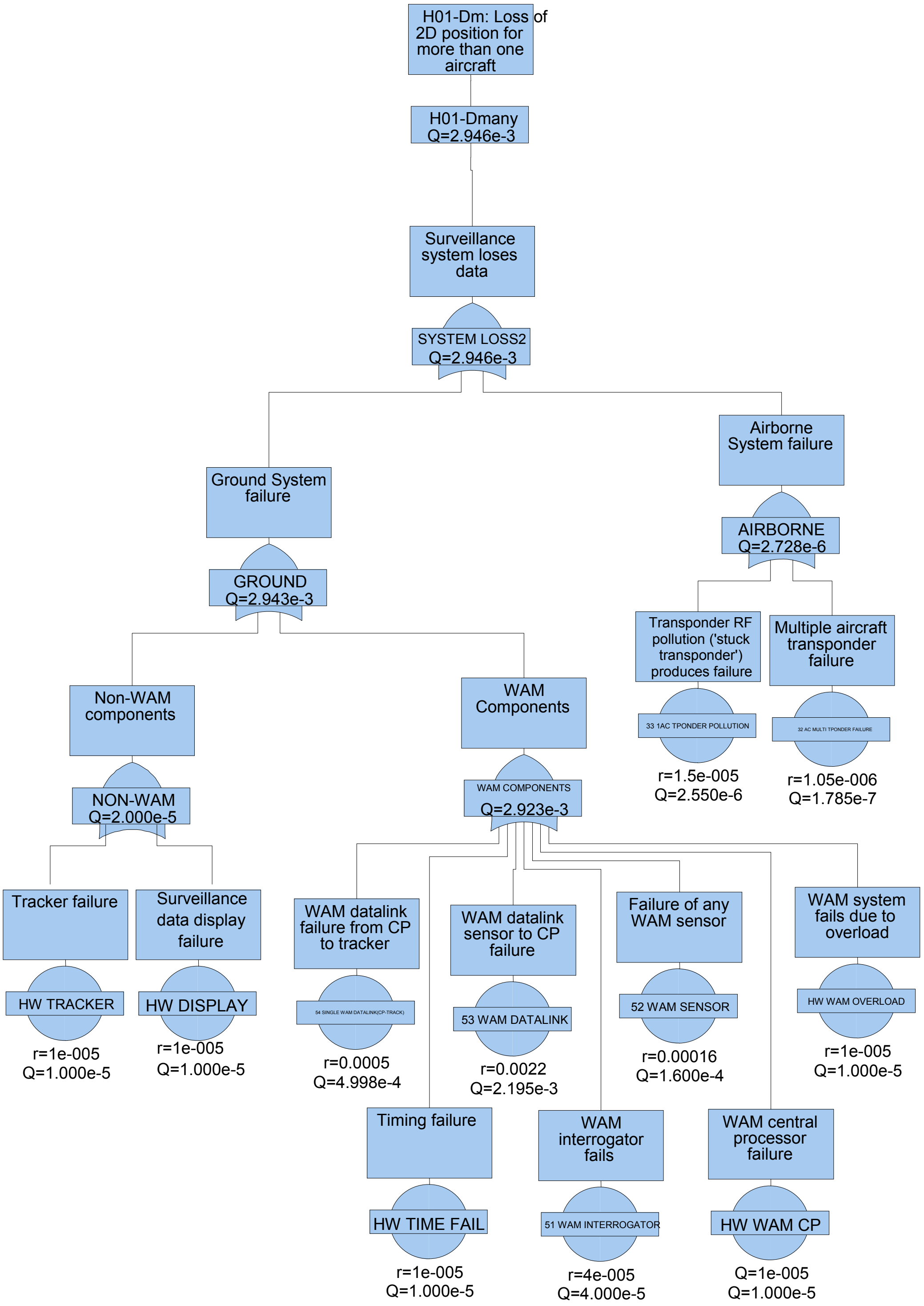


Figure 24: Hazard H01-Dmany (Detected loss of 2D position for multiple aircraft). TMA case (without redundancy)

The dominant faults in these trees arise from ground system failures. In particular, the loss of a single data link (from WAM sensors to CP) can cause the hazard since there is no redundancy in the initial tree. It can be seen from the figures that this fault has the highest ‘unavailability’.

Gate or Event		Failure
OR	SYSTEM LOSS	Multiple aircraft tracks and labels are not shown on the CWP.
OR	GROUND SYSTEM FAILURE	A failure of a ground system component
OR	NON-WAM COMPONENTS	
	TRACKER FAILURE	A failure in the system that produces tracks from the surveillance data for display on the CWP.
	SURVEILLANCE DISPLAY FAILURE	Display screen at the CWP.
OR	WAM COMPONENTS	
	WAM DATA LINK FROM CP TO TRACKER FAILURE	The single data link in the system between the WAM central processor and the tracker fails.
	TIMING FAILURE	The timing system failure includes the applied cross check of elliptical ranging.
	DATA LINK SENSOR TO CP FAILURE	A data link between the WAM central processor and one receiver fails.
	WAM INTERROGATOR FAILURE	Failure of WAM interrogator.
	WAM SENSOR FAILURE	Failure of a WAM sensor.
	WAM CP FAILURE	Failure of WAM central processor.
	WAM SUB-SYSTEM OVERLOAD	WAM sub-system gleans more information than it can process.
OR	AIRBORNE SYSTEM	A failure of an airborne system component
	AC MULTIPLE TPONDER FAILURE	Multiple aircraft in sector sustain simultaneous transponder failure.
	TPONDER RF POLLUTION	RF pollution/interference prevents multiple transponders from operating.

Table 37: Additional notes for Hazard H01-Dmany

The results of the fault tree analysis are listed in the following table with a comparison of the Q value achieved against that specified as the safety objective.

Assessment	**Airspace**	**Safety objective (per ATSU hour)**	**'Q' achieved (per ATSU hour)**	**Result**
Revised assessment	En-route	6.0E-4	3.00E-3	Achieved availability is (much) lower order of magnitude than required
	Terminal	2.8E-5	3.00E-3	
Original assessment	En-route	6.0E-7	3.00E-3	
	Terminal	2.8E-7	3.00E-3	

Table 38: Results for Hazard H01-Dmany

As can be seen from the table, the achieved availability does not meet the required safety objective.

A review of alternative mitigation possibilities are now required. These alternative mitigations, because they are needed to ensure that the safety objective is met, become derived safety requirements and are shown in Annex M. The reference in Annex M is shown as [SRxx].

A mitigation is added [SR28] that all ground components are duplicated so they become redundant. (This requirement can be achieved in different ways. For example, the tracker may provide a 'direct data feed' that bypasses normal tracker processing. This may be sufficient as long as the direct feed is independent of the main failure modes of the tracker.)

Note that different methods could have been used to meet the safety objective. For example, availability of individual components could have been increased. We have used component duplication as an illustration of the process.

In addition, a further mitigation is added [SR29] that the data link sensor to CP is triplicated, so that it has extra redundancy. (Again an alternative SR might achieve the same effect, for example using data links with higher availability. We have simply chosen SR29 to illustrate the process in this study.)

The revised fault tree (for terminal airspace) is shown below with the additional safety requirements implemented.

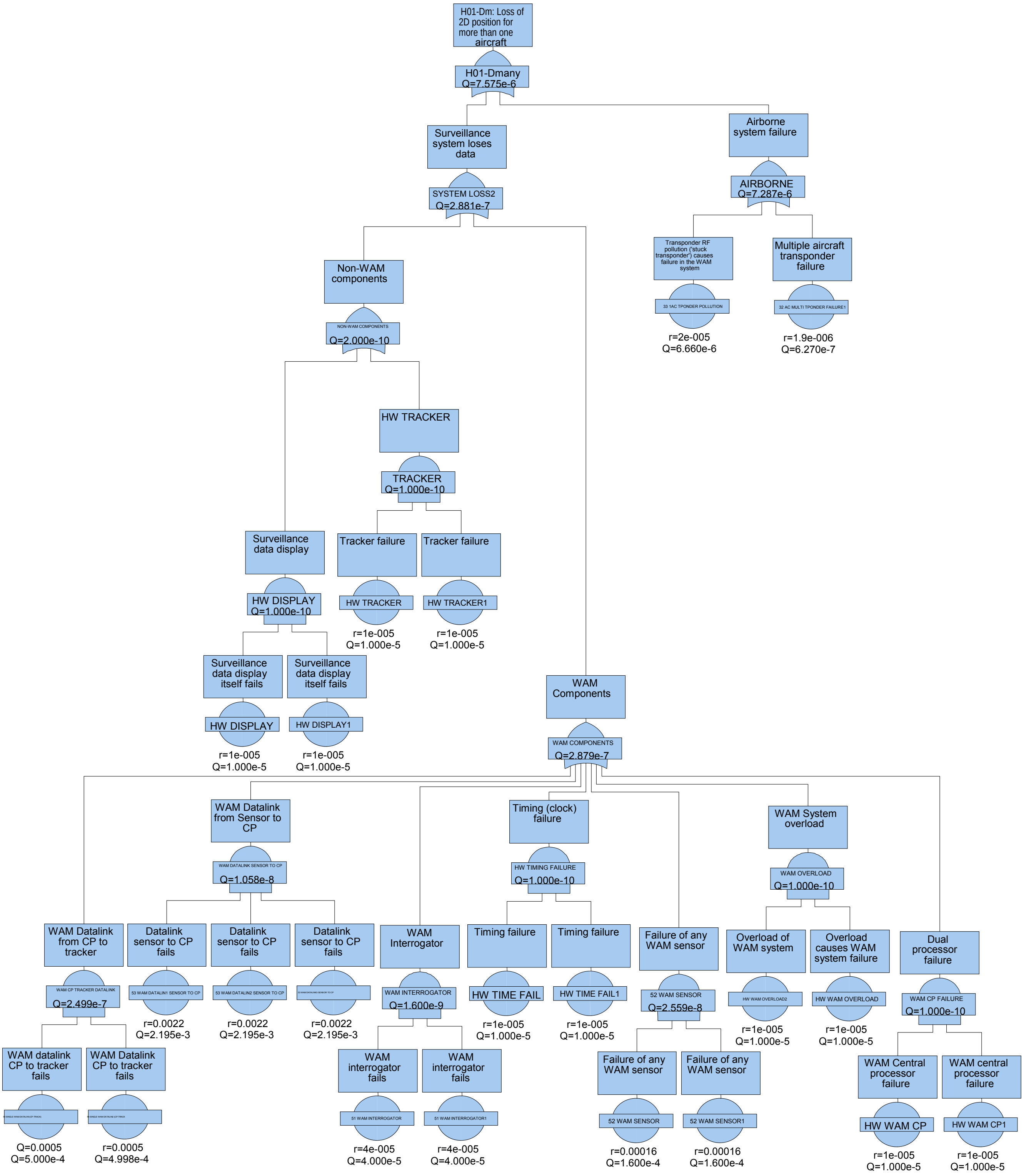


Figure 25: Hazard H01-Dmany (Detected loss of 2D position for multiple aircraft). En-route case. Revised with redundancy.

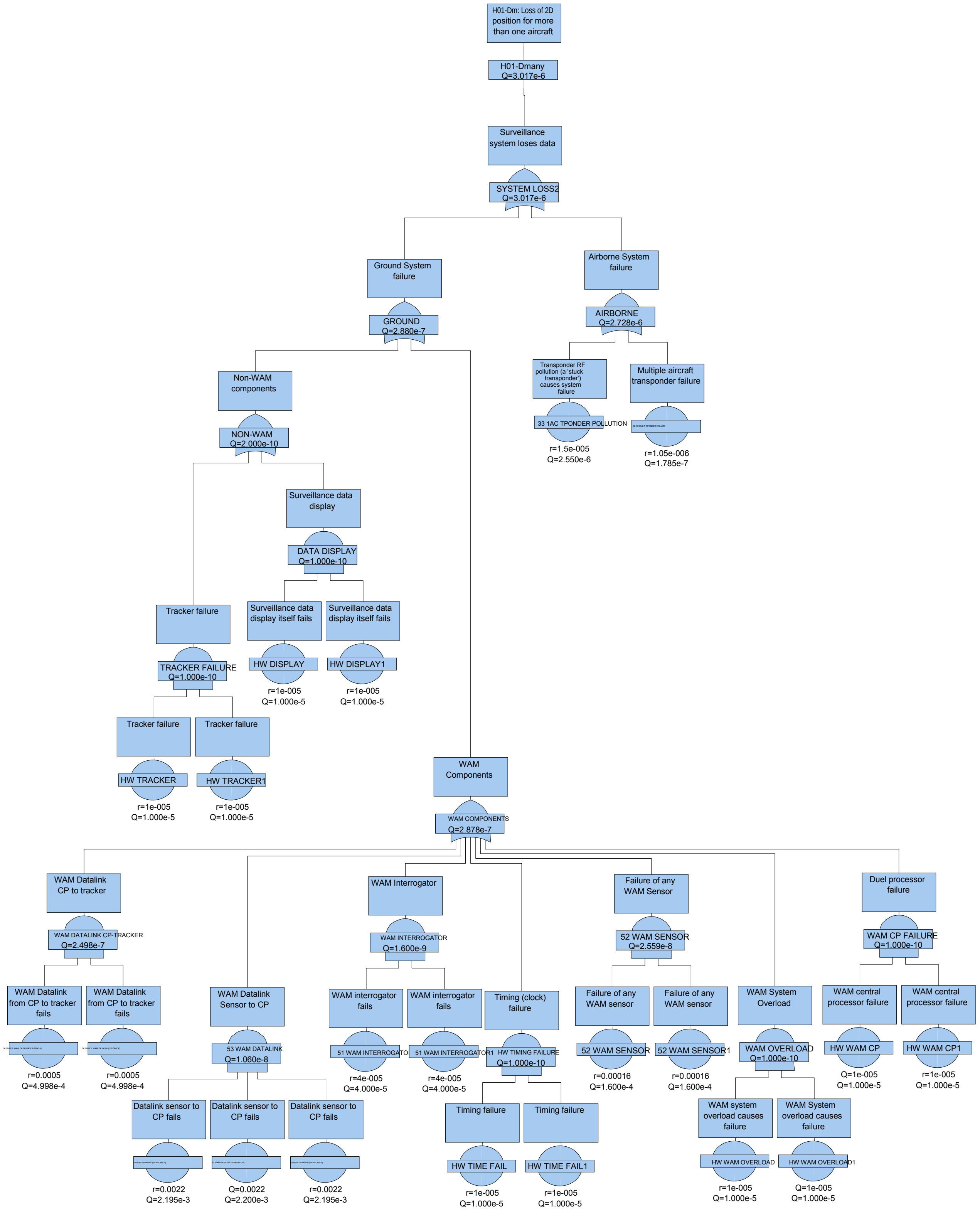

H01-Dm: Loss of 2D position for more than one aircraft
H01-Dmany Q=3.017e-6
Surveillance system loses data
SYSTEM LOSS2 Q=3.017e-6
Ground System failure
GROUND Q=2.880e-7
Airborne System failure
AIRBORNE Q=2.728e-6
Transponder RF pollution (a 'stuck transponder') causes system failure
33 1AC TPONDER POLLUTION
r=1.5e-005 Q=2.550e-6
Multiple aircraft transponder failure
32 AC MULTI TPONDER FAILURE
r=1.05e-006 Q=1.785e-7
Non-WAM components
NON-WAM Q=2.000e-10
Surveillance data display
DATA DISPLAY Q=1.000e-10
Surveillance data display itself fails
HW DISPLAY
r=1e-005 Q=1.000e-5
Surveillance data display itself fails
HW DISPLAY1
r=1e-005 Q=1.000e-5
Tracker failure
TRACKER FAILURE Q=1.000e-10
Tracker failure
HW TRACKER
r=1e-005 Q=1.000e-5
Tracker failure
HW TRACKER1
r=1e-005 Q=1.000e-5
WAM Components
WAM COMPONENTS Q=2.878e-7
WAM Datalink CP to tracker
WAM DATALINK CP-TRACKER Q=2.498e-7
WAM Datalink from CP to tracker fails
54 SINGLE WAM DATALINK(CP-TRACK)
r=0.0005 Q=4.998e-4
WAM Datalink from CP to tracker fails
54 SINGLE WAM DATALIN1(CP-TRACK)
r=0.0005 Q=4.998e-4
WAM Datalink Sensor to CP
53 WAM DATALINK Q=1.060e-8
Datalink sensor to CP fails
53 WAM DATALIN1 (SENSOR-CP)
r=0.0022 Q=2.195e-3
Datalink sensor to CP fails
53 WAM DATALIN2 (SENSOR-CP)
Q=0.0022 Q=2.200e-3
Datalink sensor to CP fails
53 WAM DATALIN3 (SENSOR-CP)
r=0.0022 Q=2.195e-3
WAM Interrogator
WAM INTERROGATOR Q=1.600e-9
WAM interrogator fails
51 WAM INTERROGATO
r=4e-005 Q=4.000e-5
WAM interrogator fails
51 WAM INTERROGATOR1
r=4e-005 Q=4.000e-5
Timing (clock) failure
HW TIMING FAILURE Q=1.000e-10
Timing failure
HW TIME FAIL
r=1e-005 Q=1.000e-5
Timing failure
HW TIME FAIL1
r=1e-005 Q=1.000e-5
Failure of any WAM Sensor
52 WAM SENSOR Q=2.559e-8
Failure of any WAM sensor
52 WAM SENSOR
r=0.00016 Q=1.600e-4
Failure of any WAM sensor
52 WAM SENSOR1
r=0.00016 Q=1.600e-4
WAM System Overload
WAM OVERLOAD Q=1.000e-10
WAM system overload causes failure
HW WAM OVERLOAD
r=1e-005 Q=1.000e-5
WAM System overload causes failure
HW WAM OVERLOAD1
Q=1e-005 Q=1.000e-5
Duel processor failure
WAM CP FAILURE Q=1.000e-10
WAM central processor failure
HW WAM CP
Q=1e-005 Q=1.000e-5
WAM central processor failure
HW WAM CP1
r=1e-005 Q=1.000e-5

Figure 26: Hazard H01-Dmany (Detected loss of 2D position for multiple aircraft). TMA case. Revised with redundancy.

The updated results for Hazard H01-Dmany are shown below. As can be seen from the table below the result is now within an order of magnitude of the safety objective.

Assessment	Airspace	Safety objective (per ATSU hour)	'Q' achieved (per ATSU hour)	Result
Revised assessment	En-route	6.0E-4	7.6E-6	Exceeded by 1 order of magnitude
	Terminal	2.8E-5	3.0E-6	
Original assessment	En-route	6.0E-7	7.6E-6	Similar order of magnitude
	Terminal	2.8E-7	3.0E-6	

Table 39: Updated results for Hazard H01-Dmany

It is also noticeable that the ground system availability now exceeds the airborne system availability. This is because of the limited availability of the airborne transponder and again illustrates the transponder as a “weak link” in the safety assessment.

L.4.4 Hazard H02-U1: Undetected Display of Erroneous 2D Position for One Aircraft

L.4.4.1 General

This failure occurs when an aircraft is displayed in the wrong place on the CWP.

L.4.4.2 WAM Sole Means Scenario

The figure below shows the fault tree for this hazard with probabilities calculated for the terminal area, additional notes are provided in the accompanying table. This hazard represents a display of erroneous 2D position for one aircraft.

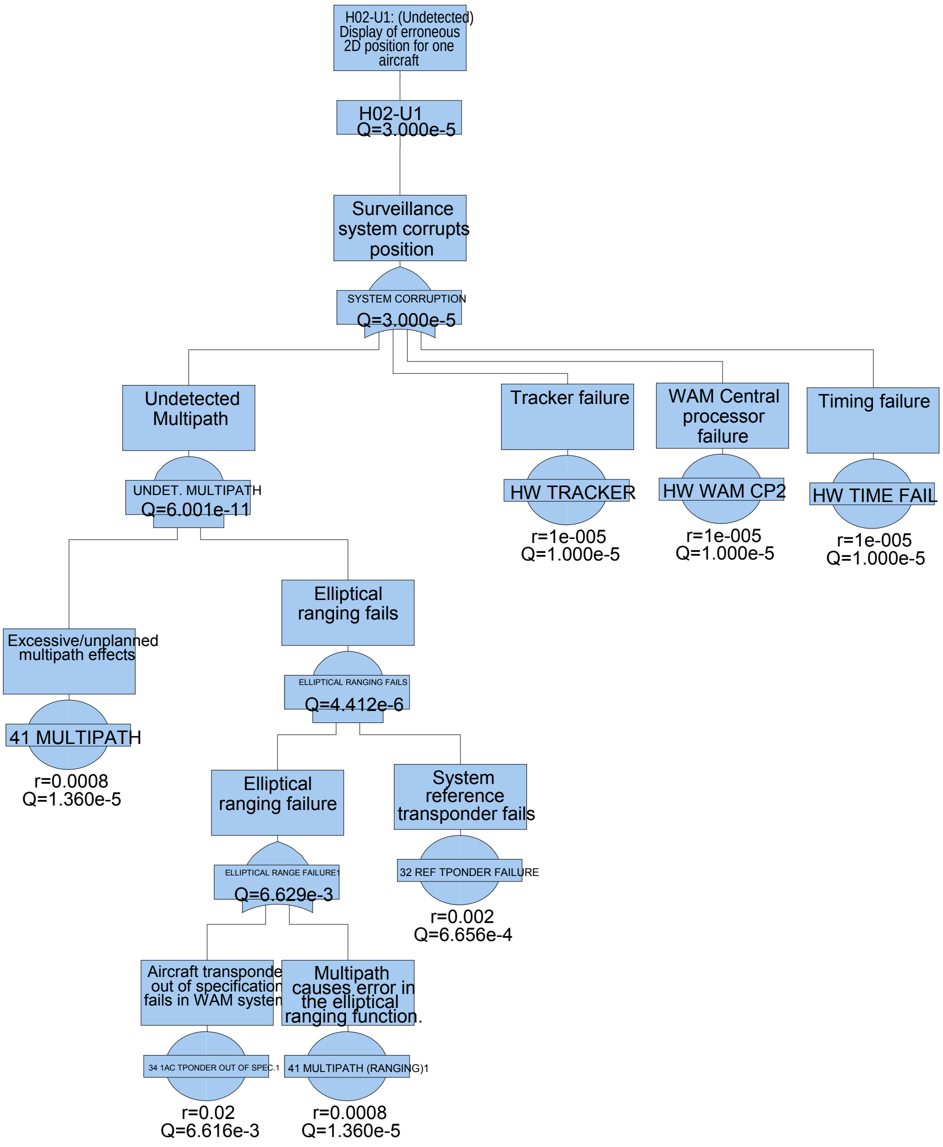

H02-U1: (Undetected) Display of erroneous 2D position for one aircraft
H02-U1
Q=3.000e-5
Surveillance system corrupts position
SYSTEM CORRUPTION
Q=3.000e-5
Undetected Multipath
UNDET. MULTIPATH
Q=6.001e-11
Tracker failure
HW TRACKER
r=1e-005
Q=1.000e-5
WAM Central processor failure
HW WAM CP2
r=1e-005
Q=1.000e-5
Timing failure
HW TIME FAIL
r=1e-005
Q=1.000e-5
Excessive/unplanned multipath effects
41 MULTIPATH
r=0.0008
Q=1.360e-5
Elliptical ranging fails
ELLIPTICAL RANGING FAILS
Q=4.412e-6
Elliptical ranging failure
ELLIPTICAL RANGE FAILURE1
Q=6.629e-3
System reference transponder fails
32 REF TPONDER FAILURE
r=0.002
Q=6.656e-4
Aircraft transponder out of specification fails in WAM system
34 1AC TPONDER OUT OF SPEC.1
r=0.02
Q=6.616e-3
Multipath causes error in the elliptical ranging function.
41 MULTIPATH (RANGING)1
r=0.0008
Q=1.360e-5

Figure 27: Hazard H02-U1 (Undetected display of erroneous 2D position for one aircraft) in the TMA.

Gate or Event		Failure
OR	SYSTEM CORRUPTION	Surveillance system corrupts the 2D position of one aircraft.
	TRACKER FAILURE	Failure of the tracker.
	WAM CP FAILURE	Failure of the WAM Central processor.
	TIMING FAILURE	A failure in the timing synchronisation system.
AND	ELLIPTICAL RANGING FAILS	Elliptical ranging fails
	REF TPONDER	Reference Transponder fails. (Probability as per PSSA 21).
AND	UNDET. MULTIPATH.	Multipath errors that are undetected by elliptical ranging check because it has also failed.
	EXCESSIVE/UNPLANNED MULTIPATH	Multipath at sensor causes corrupt position estimation.
OR	ELLIPTICAL RANGING FALURE	A failure of elliptical ranging function.
	AC TRANSPONDER OUT OF SPEC	Aircraft transponder is out of specification
	MULTIPATH (ELLIPTICAL RANGING) FAILURE	Multipath causes error in elliptical ranging function.

Table 40: Additional notes for Hazard H02-U1

The results of the fault tree analysis are listed in the following table with a comparison of the Q value achieved against that specified as the safety objective.

Assessment	Airspace	Safety objective (per ATSU hour)	'Q' achieved (per ATSU hour)	Result
Revised assessment	En-route	6.0E-1	3.0E-5	Achieved availability exceeds safety objective by more than order of magnitude
	Terminal	2.8E-2	3.0E-5	
Original assessment	En-route	6.0E-4	3.0E-5	Achieved availability exceeds safety objective by about order of magnitude
	Terminal	2.8E-4	3.0E-5	

Table 41: Results for Hazard H02-U1 with initial fault tree

The safety objective is achieved with a margin in all cases.

L.4.5 Hazard H02-Umany: (Undetected) Display of Erroneous 2D Position for More Than One Aircraft

L.4.5.1 General

This hazard is the display of erroneous 2D position for many aircraft (corruption).

L.4.5.2 WAM Sole Means Scenario

The figure below shows the fault tree for this hazard with probabilities calculated for the terminal area, additional notes are provided in the accompanying table.

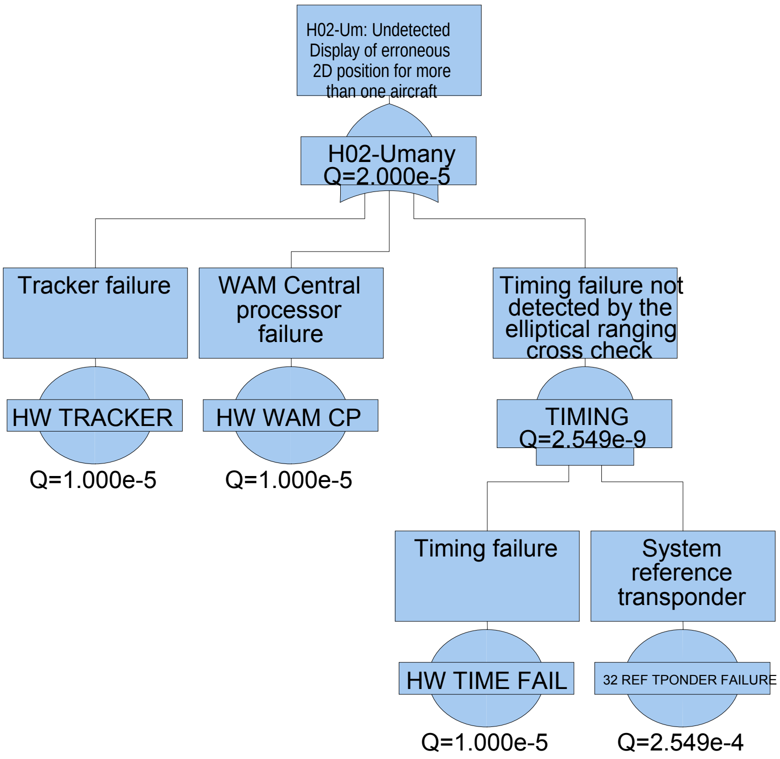

H02-Um: Undetected Display of erroneous 2D position for more than one aircraft
H02-Umany
Q=2.000e-5
Tracker failure
WAM Central processor failure
Timing failure not detected by the elliptical ranging cross check
HW TRACKER
HW WAM CP
TIMING
Q=2.549e-9
Q=1.000e-5
Q=1.000e-5
Timing failure
System reference transponder
HW TIME FAIL
32 REF TPONDER FAILURE
Q=1.000e-5
Q=2.549e-4

Figure 28: Hazard H02-Umany (Undetected display of erroneous 2D position for many aircraft)

Gate or Event		Failure
	TRACKER FAILURE	A failure in the system that produces tracks from the surveillance data for display on the CWP.
	WAM CP FAILURE	Failure of the WAM Central processor.
AND	TIMING FAILURE	Undetected timing failure at WAM sensors, simultaneously to a failure of the elliptical ranging function as caused by a reference transponder failure.
	TIME. FAILURE	Failure in the timing synchronisation system.
	REFERENCE TPONDER FAILURE	Reference transponder fails

Table 42: Additional notes for Hazard H02-Umany

The results of the fault tree analysis are listed in the following table.

Assessment	Airspace	Safety objective (per ATSU hour)	'Q' achieved (per ATSU hour)	Result
Revised assessment	En-route	6.0E-1	2.0E-5	Achieved availability exceeds safety objective by more than order of magnitude
	Terminal	2.8E-2	2.0E-5	
Original assessment	En-route	6.0E-4	2.0E-5	Achieved availability exceeds safety objective by about order of magnitude
	Terminal	2.8E-4	2.0E-5	

Table 43: Results for Hazard H02-Umany

The table shows that the safety objective is met with a margin..

L.4.6 Hazard H05-D1: Detected Loss of Identity for One Aircraft

L.4.6.1 General

This hazard implies the surveillance system loses the aircraft identity but not the position. For example, we assume that a primary track may remain on the CWP but without a label. The flight strip is assumed unaffected. In this example, we assume this could occur in one of two ways:

- A software failure in the tracker.
- The 24-bit address or Mode A code changes during flight. The WAM sub-system would produce an output track for the new address and drop the old one.

L.4.6.2 WAM Sole Means Scenario

The figure below shows the fault tree for this hazard.

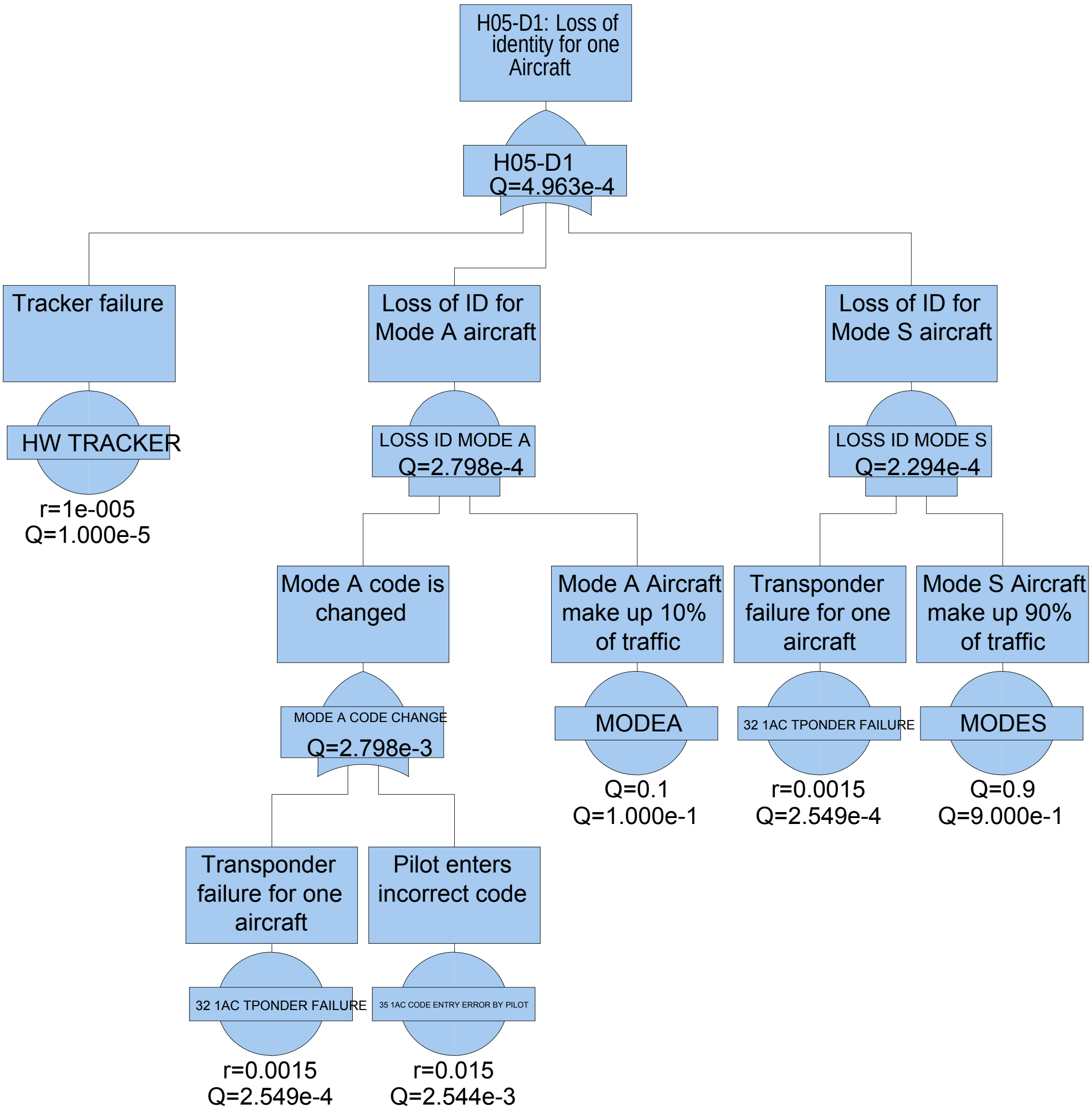

H05-D1: Loss of identity for one Aircraft
H05-D1
Q=4.963e-4
Tracker failure
HW TRACKER
r=1e-005
Q=1.000e-5
Loss of ID for Mode A aircraft
LOSS ID MODE A
Q=2.798e-4
Loss of ID for Mode S aircraft
LOSS ID MODE S
Q=2.294e-4
Mode A code is changed
MODE A CODE CHANGE
Q=2.798e-3
Mode A Aircraft make up 10% of traffic
MODEA
Q=0.1
Q=1.000e-1
Transponder failure for one aircraft
32 1AC TPONDER FAILURE
r=0.0015
Q=2.549e-4
Mode S Aircraft make up 90% of traffic
MODES
Q=0.9
Q=9.000e-1
Transponder failure for one aircraft
32 1AC TPONDER FAILURE
r=0.0015
Q=2.549e-4
Pilot enters incorrect code
35 1AC CODE ENTRY ERROR BY PILOT
r=0.015
Q=2.544e-3

Figure 29: Hazard H05-D1 (Detected loss of identity for one aircraft)

Gate or Event		Failure
	TRACKER FAILURE	A failure in the tracker.
AND	LOSS ID MODE A	The surveillance system loses identity of a Mode A equipped aircraft.
	MODE A	10% of the traffic is Mode A equipped.
OR	MODE A CODE CHANGE	Mode A code incorrectly changed in flight
	1AC TPONDER FAILURE	The aircraft transponder fails to output a correct Mode A code for any reason.
	CODE ENTRY ERROR BY PILOT	Pilot enters incorrect Mode A code during flight.
AND	LOSS ID MODE S	Loss of ID from Mode S equipped aircraft
	MODES	90% of the traffic is Mode S equipped
	1AC TPONDER FAILURE	The aircraft transponder fails to outputs incorrect 24 bit address
	WAM CP	**Discarded** The failure of the WAM central processor to correctly process on aircraft's Mode A code considered and discarded; it was not thought that a decoding problem only affecting the Mode A code was credible.
	MODE A DECODE	**Discarded** The failure of the mode A code being incorrectly decoded was considered and discarded. This problem must persist for multiple aircraft transmissions for this failure to occur; it was not thought that a decoding problem only affecting the Mode A code was credible.
	OVER INTERROGATION	**Discarded.** This was considered and discarded because it is not credible that over interrogation would only affect the Mode A code.
	TPONDER PULL	**Discarded.** This was considered and discarded because it is not credible that transponder pollution would only affect the Mode A code.
	AC ANTENNA FAILURE	**Discarded.** This was considered and discarded because it is not credible that an antenna failure would only affect the Mode A code.

Table 44: Additional notes for Hazard H05-D1

The results of the fault tree analysis are listed in the following table with a comparison of the Q value achieved against that specified as the safety objective.

Airspace	Safety objective (per ATSU hour)	'Q' achieved (per ATSU hour)	Result
En-route	6.0E-2	1.3E-3	Achieved availability exceeds order of magnitude of safety objective
Terminal	2.8E-2	5.0E-4	

Table 45: Results for Hazard H05-D1

The results show that the safety objectives are met.

L.4.7 Hazard H06-U1: (Undetected) Display of Erroneous Identity for One Aircraft

L.4.7.1 General

This hazard occurs if the identity of one aircraft is corrupted. It can occur if the technical address (24-bit address or Mode A code) either:

- changes to the address of another aircraft in the vicinity (in which case the surveillance system could confuse the aircraft identities and the controller could not be expected to reliably detect the event), or:
- changes to a different address (outside the immediate vicinity of the aircraft, a failure that would be more reliably noted by the controller).

L.4.7.2 WAM Sole Means Scenario

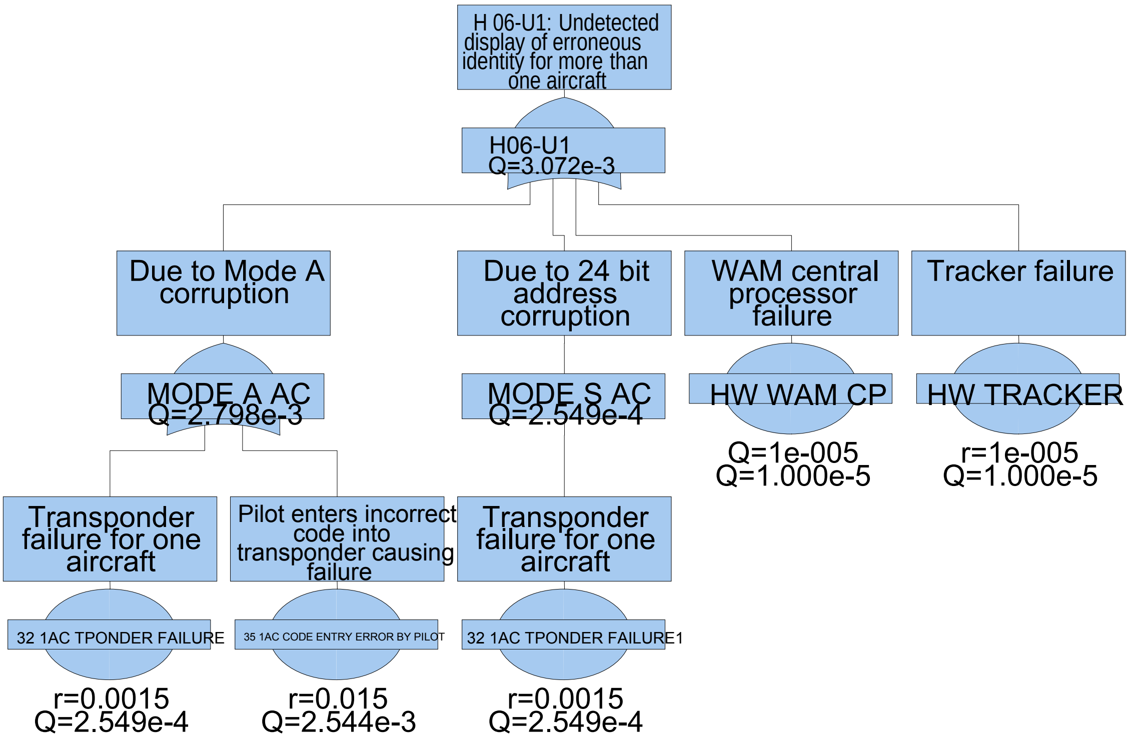

H 06-U1: Undetected display of erroneous identity for more than one aircraft
H06-U1
Q=3.072e-3
Due to Mode A corruption
Due to 24 bit address corruption
WAM central processor failure
Tracker failure
MODE A AC
Q=2.798e-3
MODE S AC
Q=2.549e-4
HW WAM CP
Q=1e-005
Q=1.000e-5
HW TRACKER
r=1e-005
Q=1.000e-5
Transponder failure for one aircraft
Pilot enters incorrect code into transponder causing failure
Transponder failure for one aircraft
32 1AC TPONDER FAILURE
35 1AC CODE ENTRY ERROR BY PILOT
32 1AC TPONDER FAILURE1
r=0.0015
Q=2.549e-4
r=0.015
Q=2.544e-3
r=0.0015
Q=2.549e-4

Figure 30: Hazard H06-U1 (Detected display of erroneous identity for one aircraft). For TMA airspace.

Gate or Event		Failure
	WAM CP FAILURE	Failure of the WAM CP.
	TRACKER FAILURE	Failure of the tracker.
OR	MODE A CORRUPTION	
	AC MODE A TPONDER FAILURE	The aircraft transponder fails to output a correct Mode A code for any equipment reason. (See section L.3.3.1.
	INCORRECT MODE A CODE ENTRY BY PILOT	Pilot enters incorrect Mode A code during flight, (by comparison Mode S code cannot be changed during flight). See section L.3.3.4 for unavailability derivation.
	24 BIT TPONDER FAILURE	Change of 24 bit address due to a transponder failure and no alarm given.

Table 46: Additional notes for Hazard H06-U1

The results of the fault tree analysis are shown below compared to the safety objectives.

Airspace	**Safety objective (per ATSU hour)**	**'Q' achieved (per ATSU hour)**	**Result**
En-route	6.0E-1	8.0E-3	Achieved availability exceeds order of magnitude of safety objective
Terminal	2.8E-1	3.0E-3	

Table 47: Results for Hazard H06-U1

The table shows that the safety objectives are met for this hazard.

L.4.8 Hazard H06-Umany: Undetected Display of Erroneous Identity for more than One Aircraft

L.4.8.1 General

This hazard is the display of erroneous identity for many aircraft (corruption). It can occur if the technical address (24-bit address or Mode A code) of multiple aircraft simultaneously either:

- changes to the address of another aircraft in the vicinity (in which case the surveillance system could confuse the aircraft identities and the controller could not be expected to reliably detect the event), or:
- changes to a different address (outside the immediate vicinity of the aircraft, a failure that would be more reliably noted by the controller).

These factors have been taken into account for the single aircraft case in the Fault tree analysis of Hazard 11. The probability of occurrence for the more than one aircraft case is dominated by the probability for the identity of two aircraft being simultaneously displayed erroneously (see section L.3.2). It follows that this probability can be represented on a fault tree by two outputs of Hazard 11 (the analysis for the single aircraft case) linked by an AND gate (because two individual failures must occur simultaneously for this Hazard 12 case).

In addition to the probability of corruption occurring for many aircraft other events that could produce a display of erroneous identity include a failure in the tracker or WAM central processor.

L.4.8.2 WAM Sole Means Scenario

The figure below shows the fault tree for this hazard with probabilities calculated for the terminal area, additional notes are provided in the accompanying table.

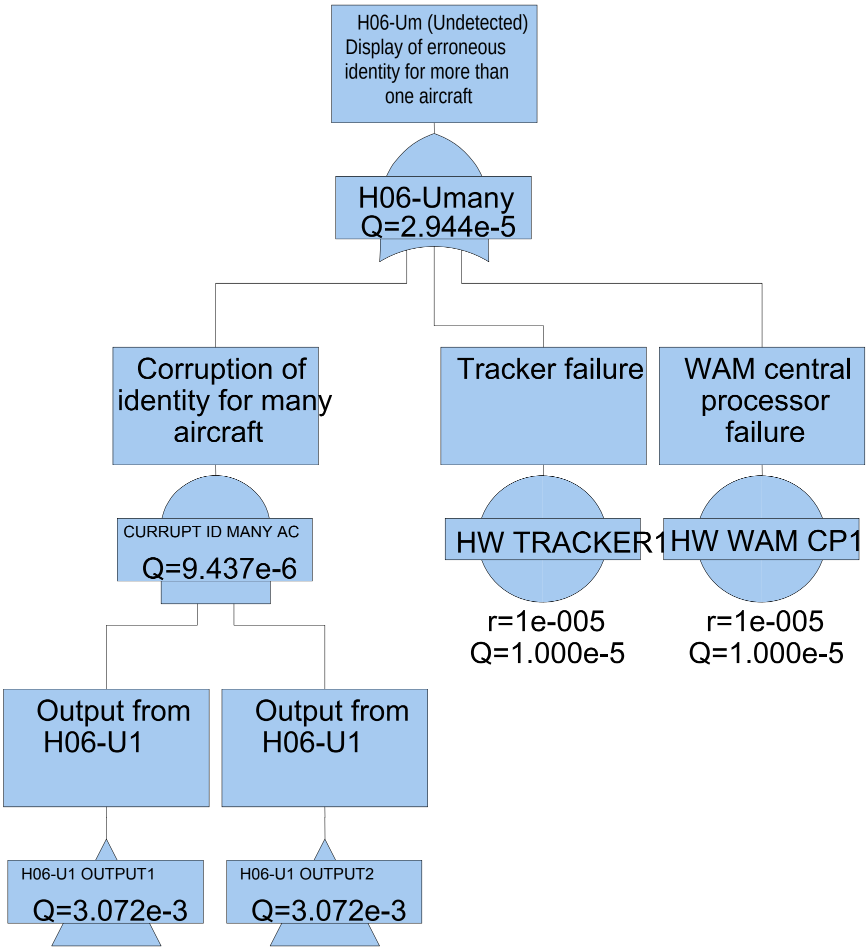


Figure 31: Hazard H06-Umany (Undetected display of erroneous identity for more than one aircraft). For TMA airspace.

Gate or Event		Failure
	TRACKER	A failure in the system that produces tracks from the surveillance data for display on the CWP (see assumption PSSA34)
	WAM CP	Undetected failure of the WAM Central processor, (see assumption PSSA34)
AND	CORRUPTION	Corruption occurring for multiple aircraft is dominated by the probability of occurrence for two aircraft simultaneously.
	H06-U1 OUTPUT1	Aircraft identity is corrupted for one aircraft (as calculated in Hazard H06-U1).
	H06-U1 OUTPUT2	Aircraft identity is corrupted for one aircraft (as calculated in Hazard H06-U1).

Table 48: Additional notes for Hazard H06-Umany

The results of the fault tree analysis are listed in the following table.

Airspace	Safety objective (per ATSU hour)	'Q' achieved (per ATSU hour)	Result
En-route	6.0E-2	8.3E-5	Achieved availability exceeds order of magnitude of safety objective
Terminal	2.8E-2	2.9E-5	

Table 49: Results for Hazard H06-Umany

The table shows that the safety objective is met.

L.4.9 Hazard H01-U1: Undetected Total Loss of all Parameters for One Aircraft

L.4.9.1 General

This hazard is interpreted to mean that the track and label is lost from the CWP and there is a simultaneous loss of flight strip information. This hazard is therefore the same as Hazard 1 with the additional loss of flight strip information.

L.4.9.2 WAM Sole Means Scenario

The figure below shows the fault tree for this hazard with probabilities calculated for the terminal area, additional notes are provided in the accompanying table.

Compared with Hazard 1 this fault tree is identical but with a *simultaneous* loss of the aircraft's flight strip as well.

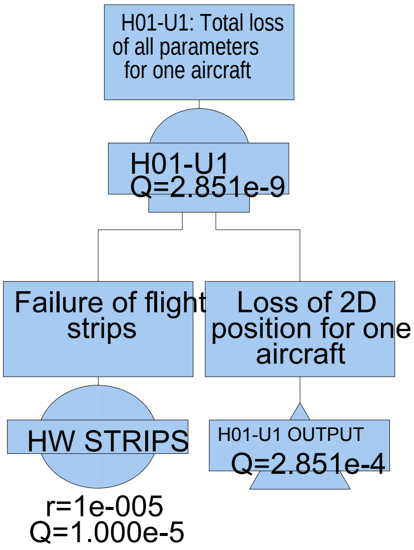


Figure 32: Hazard H01-U1 (Undetected total loss of all parameters for one aircraft)

This tree introduces just one new failure event: the failure of the flight strip processing system.

Gate or Event		Failure
	FLIGHT STRIP FAILURE	Unannunciated loss of flight strip for one aircraft only. Q = 1.0E-5.

Table 50: Additional notes for Hazard H01-U1

The results of the fault tree analysis are listed in the following table with a comparison of the Q value achieved against that specified as the safety objective.

Airspace	Safety objective (per ATSU hour)	'Q' achieved (per ATSU hour)	Result
En-route	6.0E-1	6.9E-9	Achieved availability exceeds order of magnitude of safety objective
Terminal	2.8E-2	2.9E-9	

Table 51: Results for Hazard H01-U1 with initial fault tree

The table shows that the safety objectives are met with a substantial margin.

L.4.10 Hazard H01-Dmany: Detected Total Loss of all Parameters for more than One Aircraft

L.4.10.1 General

This hazard is interpreted to mean that the track and label is lost from the CWP and there is a simultaneous loss of flight strip information. This hazard is therefore the same as Hazard H01-Dmany for the "all parameters" rather than the position data case.

L.4.10.2 WAM Sole Means Scenario

This hazard is the loss of all parameters for one aircraft *as undetected by the ATC system* and therefore not raised as an alarm to the controller.

The figure below shows the fault tree for this hazard with probabilities calculated for the terminal area.

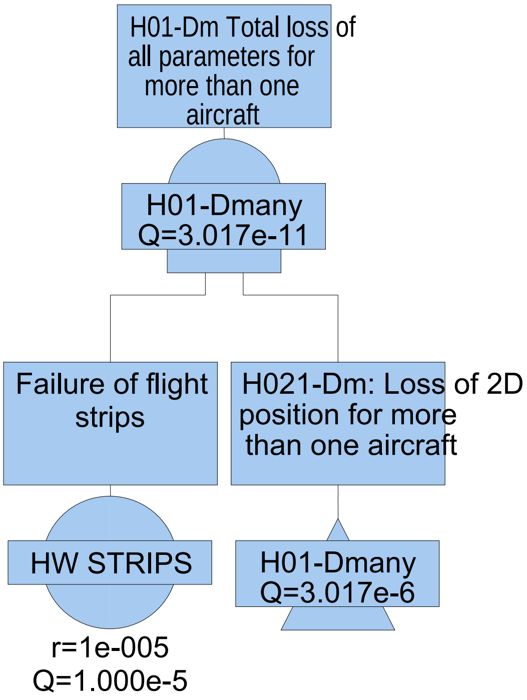

H01-Dm Total loss of all parameters for more than one aircraft
H01-Dmany
Q=3.017e-11
Failure of flight strips
H021-Dm: Loss of 2D position for more than one aircraft
HW STRIPS
r=1e-005
Q=1.000e-5
H01-Dmany
Q=3.017e-6

Figure 33: Hazard H01-Dmany (Detected total loss of all parameters for more than one aircraft)

The results of the fault tree analysis are listed in the following table with a comparison of the Q value achieved against that specified as the safety objective.

Airspace	Safety objective (per ATSU hour)	'Q' achieved (per ATSU hour)	Result
En-route	6.0E-4	7.6E-11	Achieved availability exceeds order of magnitude of safety objective
Terminal	2.8E-5	3.0E-11	

Table 52: Results for Hazard H01-Dmany

The probability of multiple aircraft loss meets the specified safety objective because the fault tree is dominated by the fact that the flight strips and surveillance display will have to fail simultaneously.

L.4.11 Conclusions and Summary of Safety Objectives

This annex has provided example fault trees to illustrate how a PSSA can be undertaken for WAM.

For most hazards considered, it was found that the unavailability achieved was less than the unavailability of the safety objective (i.e. the expected system availability exceeds the required availability). Therefore, no additional safety requirements were required.

In the case of Hazard H01-Dmany (detected loss of 2D position for multiple aircraft) however, additional ground system redundancy had to be added. This was achieved through the addition of SR28 and SR29. (In a real implementation, alternative safety requirements might have been proposed. We chose these only as an illustration.)

The following table provides a summary of the safety targets for the various hazards identified in this chapter and the unavailability achieved from this fault tree analysis once the proposed safety requirements have been applied.

Airspace	Safety objective for unavailability	Unavailability achieved	Result
Hazard H01-U1: Undetected Loss of 2D position for one aircraft			
En-route	6.0E-1	7.0E-4	Exceeds by more than order of magnitude
Terminal	2.8E-2	2.9E-4	Exceeds by more than order of magnitude
Hazard H01-Dmany: Detected Loss of 2D position for more than one aircraft			
En-route	6.0E-4	7.6E-6	Exceeds by more than order of magnitude
Terminal	2.8E-5	3.0E-6	Exceeds by about an order of magnitude
Hazard H02-U1: Undetected Display of erroneous 2D position for one aircraft			
En-route	6.0E-1	3.0E-5	Exceeds by more than order of magnitude
Terminal	2.8E-2	3.0E-5	Exceeds by more than order of magnitude
Hazard H02-Umany: Undetected Display of erroneous 2D position for more than one aircraft			
En-route	6.0E-1	2.0E-5	Exceeds by more than order of magnitude
Terminal	2.8E-2	2.0E-5	Exceeds by more than order of magnitude
Hazard H05-D1: Detected Loss of identity for one aircraft			
En-route	6.0E-2	1.3E-3	Exceeds by about an order of magnitude
Terminal	2.8E-2	5.0E-4	Exceeds by more than order of magnitude
Hazard H06-U1: Undetected Display of erroneous identity for one aircraft			
En-route	6.0E-1	8.0E-3	Exceeds by more than order of magnitude
Terminal	2.8E-1	3.0E-3	Exceeds by more than order of magnitude
Hazard H06-Umany: Undetected Display of erroneous identity for more than one			
En-route	6.0E-2	8.3E-5	Exceeds by more than order of magnitude
Terminal	2.8E-2	2.9E-5	Exceeds by more than order of magnitude
Hazard H01-U1: Undetected total loss of all parameters for one aircraft			
En-route	6.0E-4	6.9E-9	Exceeds by more than order of magnitude
Terminal	2.8E-4	2.9E-9	Exceeds by more than order of magnitude
Hazard H01-Dmany: Detected Total loss of all parameters for more than one aircraft			
En-route	6.0E-4	7.6E-11	Exceeds by more than order of magnitude
Terminal	2.8E-5	3.0E-11	Exceeds by more than order of magnitude
Units are unavailability (known as ‘Q’) per ATSU hour.			

Table 53: Safety objectives (revised assessment) & achieved unavailability

As noted in para L.1.1 the original assessment was more stringent. However, even these more stringent requirements could be met, as shown immediately above in detail and summarised in the table below.

Airspace	Safety objective for unavailability	Unavailability achieved	Result
Hazard H01-U1: Undetected Loss of 2D position for one aircraft			
En-route	6.0E-4	7.0E-4	Similar order of magnitude
Terminal	2.8E-4	2.9E-4	Similar order of magnitude
Hazard H01-Dmany: Detected Loss of 2D position for more than one aircraft			
En-route	6.0E-7	7.6E-6	Similar order of magnitude
Terminal	2.8E-7	3.0E-6	Similar order of magnitude
Hazard H02-U1: Undetected Display of erroneous 2D position for one aircraft			
En-route	6.0E-4	3.0E-5	Exceeds by about order of magnitude
Terminal	2.8E-4	3.0E-5	Exceeds by about order of magnitude
Hazard H02-Umany: Undetected Display of erroneous 2D position for more than one aircraft			
En-route	6.0E-4	2.0E-5	Exceeds by about order of magnitude
Terminal	2.8E-4	2.0E-5	Exceeds by about order of magnitude
Hazard H01-U1: Undetected total loss of all parameters for one aircraft			
En-route	6.0E-4	6.9E-9	Exceeds by more than order of magnitude
Terminal	2.8E-4	2.9E-9	Exceeds by more than order of magnitude
Hazard H01-Dmany: Detected Total loss of all parameters for more than one aircraft			
En-route	6.0E-7	7.6E-11	Exceeds by more than order of magnitude
Terminal	2.8E-7	3.0E-11	Exceeds by more than order of magnitude
Units are unavailability (known as ‘Q’) per ATSU hour.			

Table 54: Safety objectives (original assessment) & achieved unavailability

L.4.12 Alternative Scenarios

This section discusses the alternative scenarios of WAM+SSR, WAM+PSR and WAM+ADS-B.

Combining WAM with additional surveillance techniques can increase the availability and other aspects of performance. It can particularly enhance ground system availability, since it can provide an independent processing chain on the ground.

However, transponder reliability can remain as a limiting factor (as, for example, in the case of Hazard 2). PSR is the only surveillance sub-system that can be used to increase the availability of the airborne information, since it does not rely on the aircraft transponder.

In this analysis, some safety objectives were added to introduce ground system redundancy. If alternative surveillance techniques had been used in combination with WAM then these safety requirements may not have been required. The actual safety requirements would then need to be determined by developing new fault trees containing all the safety techniques present.

It should also be noted that introducing alternative surveillance techniques could *reduce* availability of the overall system. The key issue here is how the system responds to failures or errors in one system only. For example, imagine that WAM and ADS-B outputs are combined into a single track. If one of these systems has an error in position, the tracker may not be able to produce a single track with confidence. It may therefore stop outputting any track at all. Therefore, the system may have a higher integrity of position display but a lower availability. This trade-off must be considered in the local safety case.

Finally, it is worth noting that introducing alternative surveillance techniques can still leave the tracker and surveillance display as single point of failures. The analysis should always focus on overall system performance, even when additional performance is added into some of the system components.

M Example Safety Requirements

M.1 Overview

During the generic analysis, a number of safety requirements have been identified. These are listed in this annex.

The requirements arise from the process of building fault trees and identifying areas where the safety objectives are not met by previous assumptions on minimum equipage in the WAM sole means scenario.

As an example, it could be anticipated that a result of the fault tree analysis might be the necessity for a SDP alarm to monitor the presence of data elements displayed to the controller or for a minimal WAM sub-system to be augmented by another method of surveillance (ADS-B, SSR or PSR for example). This conclusion would then have to be added as a safety requirement and fed back into both the functional architecture and the fault trees themselves to see how close the combined failure rates would now come to meeting their safety objectives.

It must be remembered that Annex L is provided solely as an example of an output from a process ANSPs should consider undertaking when implementing a WAM sub-system.

M.1.1 General considerations:

ID	Safety Requirement	Comment
WAM sub-system element requirements		
SR01 **(Ref Annex L.3.5.2)**	Failure of an individual WAM sensor must be considered in analysis	For the safety case, assuming performances are met for the required coverage area, this has an effect on hazards related to loss or degradation of data.
SR02 **(Ref PSSA25 in Annex L)**	WAM sub-system overload must be considered in the analysis	In a sole means case, this could be equivalent to loss of all data.
SR03 **(Ref Annex L.3.5.3)**	Failure of the data links between the WAM sensors and the WAM central processor must be considered in the analysis	Without redundancy, this is one of the key causes of severe hazards (with relatively high failure rates experienced in operation).
SR04 **(Ref Annex L.3.5.4)**	Failure of data links between WAM central processor and the tracker must be considered in the analysis	Shown for completeness, but should be internal to the ATCC

SR05 **(Ref Annex L.3.5.1)**	Failure of the interrogator function must be considered in the analysis	Important to ascertain position of any aircraft not squittering signals (i.e. non-TCAS, non-ADS-B), and to gain all data required.
SR06 **(Ref Annex L.3.5.5)**	Failure of the timing function in the WAM sub-system must be considered in the analysis	Leads to position corruption (in particular, there may be a problem with "graceful degradation" of position, which may not be easily detectable by the controller)
SR07 **(Ref Annex L.3.5.6)**	WAM central processor failures must be considered in the analysis	Total loss of WAM derived data may result (for a sole means scenario, the criticality may be similar to a tracker/SDPS).
SR08 **(Ref Annex L.3.3.1)**	Failure of WAM reference transponder must be considered in the analysis	Originally viewed as a mitigation to timing failures, but now included as a basic component of the WAM sub-system. Failure leads to lack of integrity in the timing function (leading to position errors).
SR09 **(Ref K.2.6 and PSSA10 in Annex L)**	Failure of WAM elliptical ranging function must be considered in the analysis	Again, originally viewed as a mitigation to increase position accuracy and integrity, but now included as a basic component of the WAM sub-system as a positioning method in its own right (alongside TDOA methods).
Other ground system element requirements		
SR10 **(Ref Annex L.3.5.6)**	Failure of the surveillance data display (Controller Working Position) must be considered in the analysis	Not a specific focus of this safety assessment, but included as part of the end-end system.
SR11 **(Ref Annex L.3.5.6)**	Failure of the tracker must be considered in the analysis	Detailed functions of the tracker are not examined in this study – however, implementers may need to understand tracker functional failure rates (e.g. in fusing data correctly, in losing data entirely, in producing an accurate track).
SR12 **(Ref Annex L.3.5.6)**	Failure of flight strips must be considered in the analysis	Not a focus of the WAM safety assessment, but included as part of the end-end system.

Airborne system element requirements		
SR13 **(Ref Annex L.3.3.5)**	Incorrect decoding of the 24-bit aircraft address or Mode A code must be considered in the analysis	Incorrect decoding leads to loss of position for that aircraft (due to the non formation of a track for the aircraft).
SR14 **(Ref Annex L.3.4.3)**	The possibility of duplicated 24-bit addresses must be considered in the analysis	The tracker may not be able to process duplicate 24-bit addresses. This leads to a corruption or loss of position for the aircraft with duplicated addresses.
SR15 **(Ref Annex L.3.4.1, L.3.4.2, L.3.4.3)**	Filtering of the target report due to inaccuracy (as a result of multipath effects or proximate aircraft transmitting the same Mode A code) must be considered in the analysis	Multipath effects, and overlapping Mode A code replies, are included in this basic cause. A filtering of the data leads to a loss of position for the aircraft concerned.
SR16 **(Ref Annex L.3.3.1)**	Effects on the data due to aircraft antenna failure, or aircraft transponder failure must be considered in the analysis	No airborne transmission results. As WAM relies upon the transponder transmitting a signal, this leads to a total loss of WAM derived data for the affected aircraft.
SR17 **(Ref Annex L.3.3.5, L.3.3.2, L.3.3.1)**	Transponder RF pollution (“stuck” transponder) must be considered in the analysis	RF pollution may affect the ability of the system to derive positions for many aircraft in the vicinity.
SR18 **(Ref Annex L.3.3.1)**	Effects on the data due to multiple aircraft antenna failure, or multiple aircraft transponder failure must be considered in the analysis	See SR16.
SR19 **(Ref Annex L.3.3.4**	Effects due to the flight crew entering incorrect Mode A code must be considered in the analysis	Although not testable (for a quantitative safety requirement to be assigned), the effect of an incorrect Mode A code (for a Mode A/C aircraft) may be mitigated by ground system alarms, extrapolation of tracks, and direct R/T communication (so the controller can inform the flight crew of the error).
SR20 **(Ref Annex L.3.4.3)**	Effects due to multipath in transmission of signals from aircraft to WAM sensors must be considered in the analysis	This is not thought to be measurable or testable, and therefore may need to be the subject of a conservative assumption in the eventual Safety Case (see SR15).

Interoperability requirements		
SR21 **(Ref Section 4.6)**	Continuous interoperability, during the implementation, migration and ongoing operational processes, of all system components must be considered in the analysis	This includes the airborne equipment, the replacement WAM surveillance sub-system and the reversionary procedures/operations to the previous sub-system (until such a time when this system can be taken off-line without causing a degradation of system safety).
Controller interface requirements		
SR22 **(Ref Section, 4.3)**	The controller interface is the same for WAM and the reference sub-system in terms of ▪ Data items presented; ▪ Update rates; ▪ Format of presentation.	This will allow the new sub-system to be used with current controller procedures allowing a safe migration to the new sub-system.
SR23 **(Ref Section, 4.3)**	The quality of the presented WAM data is at least as good as the reference sub-system	Needed to ensure controller confidence and maintain high safety standards.
SR24 **(Ref Section 4.6)**	The operational service volume is completely supported by the WAM sub-system	To allow a safe separation service to be provided within a defined volume i.e. to correctly design and validate the WAM sub-system to meet the required performance in the specified coverage volume (the need for performance testing of the system in its operational environment - i.e. using initial flight tests and ongoing monitoring processes).
Validation requirements		
SR25 **(See Annex N)**	These safety requirements are validated against the local implementation case	The safety requirements contained in this table are only provided to illustrate typical generic outputs from the safety assessment process. Each local case must be validated against them
Surveillance system functionality requirements		
SR26 **(See Section 4.6)**	The WAM sub-system can track both Mode A/C and S aircraft	

SR27 **(See Section 4.6)**	The WAM sub-system can successfully track aircraft transmitting the same Mode A or S codes in the same airspace	Care must be taken to ensure that closely-spaced aircraft with the same Mode A code or 24-bit address can be tracked.
Requirements arising from Fault Tree Analysis		
SR28 **(Ref. Section 5.4,and L.4.11)**	All ground components are duplicated	Needed to let Hazard 2 meet its safety objective
SR29 **(Ref Section , 5.4 and L.4.11)**	The data link from sensor to WAM CP is triplicated	Needed to let Hazard 2 meet its safety objective
Common mode failure requirements		
SR30 **(Ref Annex K.2.5)**	Any common mode failures due to the use of GNSS in multiple ATC systems must be considered	This requirement depends on the timing system implementation, which may require GNSS timing in order to function correctly.

Table 55: Example Safety Requirements

Note that conditions regarding the WAM sub-system assumed during the worked example are shown in L.2. These are not included in the high level assumptions as they are specific to this worked example. However, implementers may wish to use them as a guide to their own safety case.

N General Guidance to Implementers

N.1 Scope and Limitations of this Generic Safety Assessment

The analysis presented in this document is generic. It does not replace individual safety assessments that implementers have to develop. It considers the system in generic terms and assesses safety aspects within a typical implementation environment. In particular, its conclusions rely on all the assumptions being true and valid. ANSPs, regulators and other readers should ensure that the assumptions made in this document are applicable to their airspace, using this document as a contribution to their local safety case. The key assumptions are summarised in Annex F.

In addition, this document does not follow a full safety assessment methodology. It does not allocate objectives to various components of the actual system in its actual context (basic causes), and therefore no quantitative safety requirements are set. The allocation of safety objectives and requirements (through a fault tree analysis) will be the responsibility of individual implementers, who should consider carrying out a System Safety Analysis (SSA) on the exact WAM sub-system that is to be installed in the exact and detailed context of the rest of their ATM system. The SSA process is a more detailed refinement of the PSSA that is provided in this document as an example.

N.2 Roles and Responsibilities of EUROCONTROL, ANSPs and Regulators

This section explains the relative roles and responsibilities of EUROCONTROL, ANSPs and regulators in the safety assessment and assurance of WAM, in relation to a typical project safety lifecycle. It is based on similar guidance developed for A-SMGCS safety cases [21].

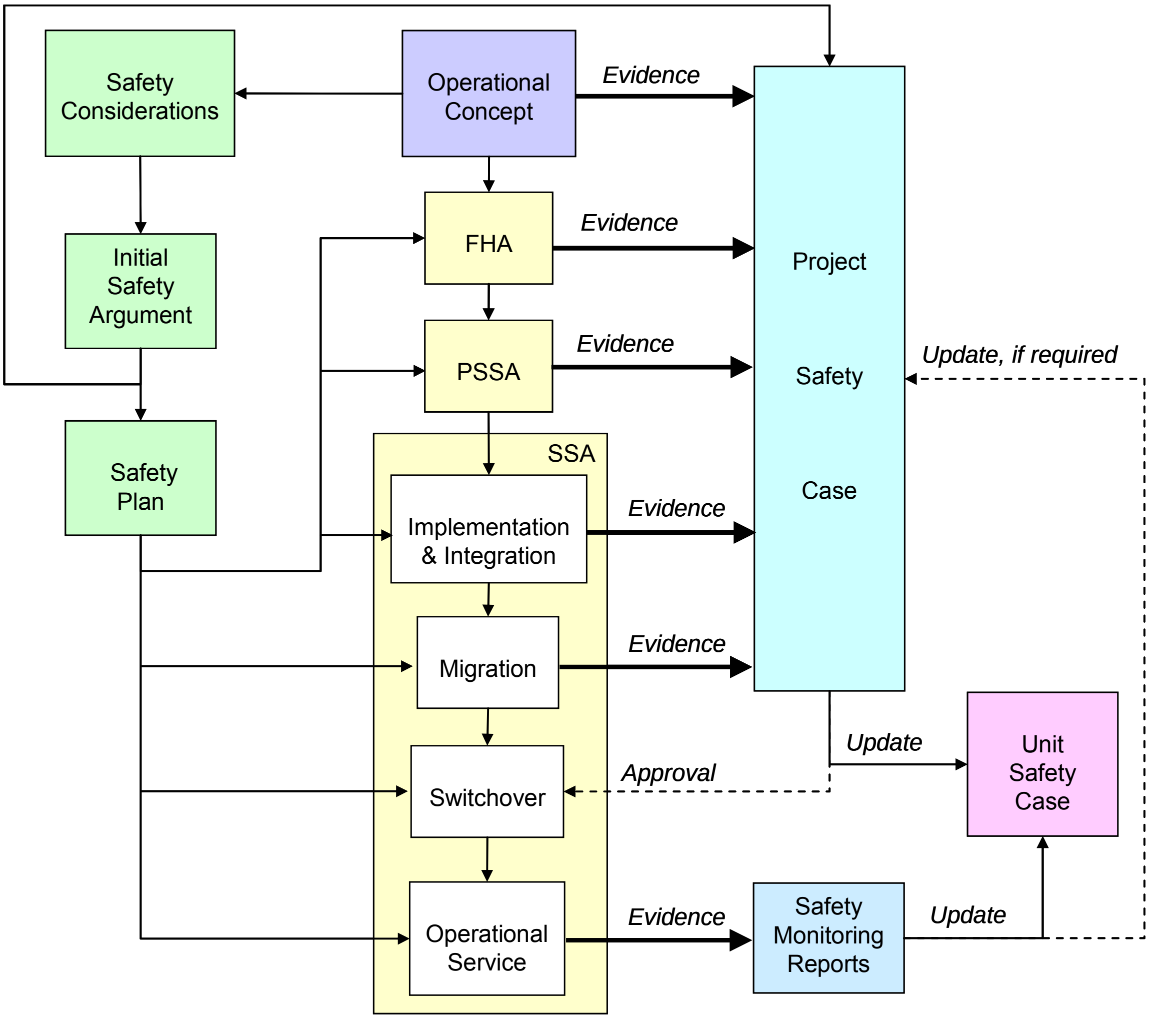


Figure 34: Stages in the development of a safety case

A simplified view of a typical project lifecycle is shown in the figure above.

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

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

The *Safety Plan* specifies the safety activities (mainly the assessments - FHA, PSSA, SSA - and gathering of Evidence) to be conducted throughout the project lifecycle and the allocation of responsibilities for their execution.

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

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

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

Once this process is complete, it would be appropriate to update the Unit Safety Case (if one exists) with the information from the Project Safety Case thus establishing a new safety baseline for the on-going service.

Decommissioning of a system, at the end of its operational life, is not shown explicitly in Figure 34 but may be thought of as a special case of a change.

For many EUROCONTROL EATM areas of work such as WAM, EUROCONTROL is not responsible for implementation of the concept concerned. In those cases, EUROCONTROL would carry out a safety assessment up to the PSSA stage and would document the resulting assurance in a subset of the eventual Project Safety Case, known as a *Preliminary* Safety Case. For this WAM study however, EUROCONTROL has developed a generic safety assessment, examining the OSED, FHA and initial PSSA steps, but not allocating quantitative safety requirements. The implementing authority would then be responsible for development of a full Project Safety Case, including carrying out all the steps in the SSA process.

The table below shows the division of roles and responsibilities between EUROCONTROL, as developer of the Concept at a generic level, and the ANSPs and regulators, as implementers and approvers of the Concept at a local level. It also provides internal and external references to where the related guidance can be found.

Activity	EUROCONTROL	Implementers	Remarks
Safety Considerations	☑	☒	This is initially an internal EUROCONTROL process, to understand whether a full safety case is necessary. Implementers may accept the results of the EUROCONTROL process or form their own view.
Safety Argument	☑	☑	The EUROCONTROL generic safety assessment for WAM contains a safety argument. The details of the local safety case are not expanded within this document. The Implementer should develop a safety argument in relation to the specific implementation in more detail than the example given here to satisfy themselves their argument is logical and complete.
Safety Plan	☑	☑	EUROCONTROL produces a Safety Plan for its own purposes – the Implementer should do the same in relation to the specific implementation.
FHA	☑	☑	EUROCONTROL has completed a FHA for a ‘generic’ application of WAM. The Implementer should at least confirm the results including the Safety Objectives in the context of the specific implementation. See Annex H and section 6 for guidance.

Activity	EUROCONTROL	Implementers	Remarks
PSSA	☑	☑	EUROCONTROL has completed an example PSSA, and produced a complete set of Safety Requirements, for a ‘generic’ application of WAM. The Implementer should at least confirm the results, including the Safety Requirements, in the context of the specific implementation. See section 6. Note that EUROCONTROL has provided qualitative safety requirements; States will now need to develop quantitative safety requirements. A worked example of PSSA is provided to show how this might be done.
SSA – Implementation & Integration	☒	☑	Implementation & Integration and development of appropriate safety analysis to provide evidence for the Safety Case are entirely the Implementer’s responsibility.
SSA – Migration	☒	☑	Planning and execution of the migration from the pre-WAM state to a fully operational WAM sub-system is entirely the Implementer’s responsibility
SSA – Switchover	☒	☑	Planning and risk management of the switchover from the pre-WAM state to a fully operational WAM sub-system is entirely the Implementer’s responsibility. This should be supported by the system supplier.
SSA – Safety Monitoring in Operational Service	☑	☑	EUROCONTROL may aid Implementers in providing “best practice” guidelines derived from compilations of States’ safety monitoring results. Nevertheless, the responsibility for ensuring that the WAM sub-system remains safe in operation lies solely with the Implementer.

Activity	EUROCONTROL	Implementers	Remarks
Project Safety Case	☑	☑	EUROCONTROL has produced a Generic Safety Assessment containing the Safety Argument (see above) and Evidence for the generic FHA and PSSA (see above). The Implementer should confirm the information presented in the Generic Safety Assessment, and modify / expand it as necessary to produce a full Safety Case for the specific implementation.
Unit Safety Case	☒	☑	Unit Safety Cases, if produced, are entirely the Implementers' responsibility.

Table 56: Allocation of roles and responsibilities

N.3 Guidance to Implementers on using the OSED (Argument 2.1)

A generic OSED is described in Annex E.

Implementers should review the OSED, taking note of any assumptions that are made (see Annex F). These should be validated or changed depending on the local environment to produce a local OSED [SR25].

N.4 Guidance to Implementers on using the FHA

N.4.1 Introduction

This section describes guidance to the Implementers of WAM on how to use the EUROCONTROL WAM FHA within this safety assessment in Annex H. Further Guidance material on how to apply the process can be found in the EUROCONTROL Safety Assessment Methodology [3] and EUROCONTROL Safety Case Development Manual [4] although other processes may be applied as appropriate.

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

- The acceptable risk of an accident influenced by the WAM in the en-route environment (the TLS)
- The relations between the different severity classes in the risk classification scheme
- The logical architecture of WAM
- The procedures applied for the use of WAM

- Safety Objectives development

Each of these items is discussed in the following paragraphs, with reference to the relevant sections of this safety assessment.

N.4.2 Derivation of a TLS

The TLS used in this safety assessment is specified in line with ICAO, with guidance given by EUROCAE ED-125 [6], as described in Annex section H.2 of the FHA.

It is based on the probability of an accident being 1.55 x 10^{-8} / flight hour or less.

During the Safety Objectives calculation, the WAM sub-system is considered to contribute towards a portion of the overall Target Level of Safety. This is discussed in section H.2.1.

N.4.3 Derivation of Severity and Risk Classification Schemes

The severity classification scheme used in the safety case is based on the EUROCONTROL ESARR 4 Severity Classification Scheme, detailed in Annex J. Further guidance is given by ED-125 [6].

For the risk classification scheme, Safety Targets are derived for each severity class. Within this safety assessment, ECAC regulator safety targets are used.

Each Implementer may wish to define their own Ambition Factor, a ratio above the minimum Safety Target to which they will aim. This provides a safety margin to the acceptable Target Levels of Safety.

Question 1

Does the Implementer wish to re-use ECAC regulator safety targets, with respect to the relationship between each severity class?

Question 2

Does the Implementer use an Ambition Factor in their safety cases, or are the values used in this safety assessment (Table 16: Risk Classification Scheme) suitable for their local environment?

Note that any addition of Ambition Factors will make the Safety Objectives harder to achieve, unless less conservative assumptions are used during the identification of probabilities of effects of hazards. This may be justified, given that the Implementer will have greater knowledge of their local environment, and should be able to justify more realistic values (for example, for traffic density, or controller detection probabilities).

N.4.4 Definition of Architecture and Operating Procedures

The safety assessment was based upon a generic WAM architecture, defined in Annex K.

Implementers must base their FHA upon the functional and logical architectures of their specific implementations.

The FHA contains a number of assumptions concerning WAM operations. These are listed in Annex H.4.1, and should be reviewed and validated or adjusted by implementers.

Question 3

Does the Implementer have a different functional architecture to that shown in Annex K? If so, have differences been clearly identified, and taken forward throughout the safety analysis?

Question 4

Has the Implementer validated each operational assumption [ASSUMP16] shown in Annex F for the local situation?

Question 5

Does the Implementer wish to use the WAM derived data for operations other than the provision of an ATC service? Have the new operational requirements been taken into account in the Functional Hazard Analysis?

N.4.5 Identify Hazards

The method used for the identification of hazards is described in Annex H.3.

The local FHA must identify the failure modes to be considered. As part of the EUROCONTROL FHA, the WAM data elements were considered to be:

- 2D Position;
- Altitude;
- Aircraft identity (e.g. call sign);
- Short intent/history;
- ALL

The potential failure modes were considered and consolidated as:

- Loss of data (including misdirected or delayed data over a certain threshold);
- Corruption of data (e.g. inconsistent or delayed non-filtered data, spurious or malicious data).

The hazard analysis assessed the severity of each WAM failure. The method by which this was done is described in Annex H.4 and the findings are recorded in Annex H.5.

Implementers should follow a similar process and provide assumptions that are specific to the WAM sub-system and en-route environment. Detailed notes on the basis for allocating the severity are provided in Annex J.

Question 6

Has the Implementer validated that all data elements, failure modes and hazards are identified for their local environment and operational service?

Question 7

Does the Implementer wish to use the failure mode classifications employed in this safety assessment (for example, hazards are defined as affecting one aircraft, or more than one aircraft)?

Question 8

Has the Implementer validated the severity assessment for each failure? Is there justification provided (traceability) for each identified worst credible effect and its derived severity?

N.4.6 Safety Objective Development

The method used to derive the safety objectives is described in Annex H.5.

Implementers should follow a similar process using information for their specific environment and also:

- customise the Event Trees with any specific additional conditions which would impact the safety consequence;
- re-validate the assumptions regarding the detection probability with which a controller will detect a failure;
- agree the proportion of overall hazards attributable to the WAM derived data.

In addition to these specific guidelines, implementers should review all assumptions made during the development of the safety objective and validate or adjust them based on the local environment.

Question 9

Does the Implementer agree with the “barriers” chosen in this safety assessment? (See Table 6 and Table 21 for their description.) Do they wish to alter the probability of the barriers? For example, is the controller detection rate for a hazard appropriate for their operations and environment?

Question 10

Does the Implementer wish to define a different probability of effect per hazard-effect pair (thus adding detail and more justification to the safety analysis)? Given the importance of the Pe value, and its effect on the overall safety assessment (several orders of magnitude difference to safety objectives), it is critical that Implementers and regulators are happy with assumptions made and decisions taken at this stage. Putting it a different way, this is a key stage at which the balance between the system's and human's role in ensuring safe operations is determined.

Question 11

Has the Implementer re-validated the allocation of the safety budget to the WAM sub-system (= N)? If necessary, have they developed a schema to allocate a budget per hazard severity (rather than applying a proportional allocation)?

N.5 Guidance to Implementers on using the PSSA

N.5.1 Introduction

EUROCONTROL has not completed a full PSSA within this safety assessment. The first steps have been completed, with an identification of basic causes of hazards. However, no quantitative allocation of safety objectives has been made.

The Implementer should use this safety assessment as a basis for building a fault tree analysis of the contributors to each hazard. A worked example is given in Annex K for this purpose.

Safety Requirements are set to ensure the Implementer examines and justifies each of the basic causes identified in this study. Further Safety Requirements are derived from External Mitigation Means, applied during the derivation of the FHA.

Quantitative Safety Requirements will be derived by the Implementer reflecting local operations and environmental conditions.

Further Guidance material on how to apply the process can be found in the EUROCONTROL Safety Assessment Methodology [3] and EUROCONTROL Safety Case Development Manual [4] although other processes may be applied as appropriate.

N.5.2 Safety Requirements Development

It is recommended that Implementers review the worked example in Annex K to gain understanding of which areas may be most critical in the safety requirements derivation process (i.e. which failures contribute most to the safety objective).

The worked example is intended to show that it is possible to meet the safety objectives using the WAM sub-system. Failure rates were derived from experience where possible, and conservative assumptions where not possible (e.g. failure rate for a hardware component of 1.0E-5). Where safety objectives have not been met, safety recommendations have been compiled, identifying mitigation means for the components which contribute most to the safety objective.

These safety recommendations should be used as a guide to the kinds of internal mitigation means possible for the Implementer to use when designing their system (at the Preliminary System Safety Assessment stage). There will always be a choice of different redundancies and extra monitors / alarms, which in combination may still allow the safety objective to be met. It is therefore up to the Implementer which combination of Internal Mitigation Means they use for their local PSSA.

The conditions assumed during the worked example, shown in detail in L.2 should be reviewed and (if reused) validated for the local PSSA.

N.5.3 Note on Transition to Operations

It was identified during the study that the phase of operations when WAM derived data is being used may require slightly different safety requirements.

Controller's trust in the new system, along with the engineer's ability to predict and prevent faults, may be lower than later in the system's life when experience has been gained.

Certain checks on the WAM derived data may be thought necessary by the local Implementer to ensure the safety during transition to operations.

Nevertheless, because WAM derived data is intended to be the same as SSR derived data, the operational procedures and controller behaviours should not change markedly.