

“Safety Assessment Made Easier”

Part 1

**Safety Principles and
an Introduction to Safety Assessment**

Edition Number	:	1.0
Edition Date	:	15 Jan 10
Status	:	Released Issue
Intended for	:	CND & Stakeholders

DOCUMENT CHARACTERISTICS

TITLE		
"Safety Assessment Made Easier"		
EATM Infocentre Reference:		
Document Identifier	Edition Number:	1.0
	Edition Date:	15 Jan 10
Abstract		
<p>The aim of this document is to present a clear, complete, coherent and integrated approach to safety assessment that will meet the needs of EUROCONTROL and its Stakeholders, now and in the future.</p> <p>Part 1 is aimed at a broad readership. It addresses a wide range of safety issues and explains <u>why</u>, in European ATM, we need to take a much broader approach to safety assessment in the face of emerging new operational concepts. Part 1 provides the foundation for Part 2 of the document</p> <p>Part 2, is aimed mainly at safety practitioners, and provides a theoretical and practical guide on <u>how</u> to safety assessment and develop safety assurance throughout a typical system lifecycle.</p>		
Keywords		
Safety	Safety Case	Safety Assurance
Failure Approach	Safety Argument	Safety Lifecycle
Risk Mitigation	Unit Safety Case	ESARRs
Broader Approach	SMS	Safety Management
		Success Approach
		Risk Assessment
		Hazard
		Human Factors
Contact Person(s)		Tel
Eric Perrin		+33 (0)1 69 88 74 01
		Unit
		EEC – CoE Safety

STATUS, AUDIENCE AND ACCESSIBILITY		
Status	Intended for	Accessible via
Working Draft <input type="checkbox"/>	General Public <input type="checkbox"/>	Intranet <input type="checkbox"/>
Draft <input type="checkbox"/>	Stakeholders <input checked="" type="checkbox"/>	Extranet <input checked="" type="checkbox"/>
Proposed Issue <input type="checkbox"/>	Restricted Audience <input type="checkbox"/>	Internet (www.eurocontrol.int) <input type="checkbox"/>
Released Issue <input checked="" type="checkbox"/>	<i>Printed & electronic copies of the document can be obtained from the EATM Infocentre (see page iii)</i>	

ELECTRONIC SOURCE		
Path:	C:\Documents and Settings\FMy Documents_0 EEC 10_JDFWP3 Methods\S.A.M.E\SAME Part 1 v1.0 released.doc	
Host System	Software	Size
Windows_NT	Microsoft Word 10.0	796 Kb

EATM 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 Help

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

AUTHORITY	NAME AND SIGNATURE	DATE
<i>Please make sure that the EATM Infocentre Reference is present on page ii.</i>		
Senior Team Leader (Safety Assessment and Safety Case) CoE Performance and Methods / Safety	(signed) Eric PERRIN	18 Jan 2010
Manager CoE Safety & ATM Security	(signed) Dr. Bernd TIEMEYER	18 Jan 2010
Safety, Security & Human Factors Activity Manager ESP Programme Manager	(signed) Antonio LICU	18 Jan 2010

DOCUMENT CHANGE RECORD

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

EDITION NUMBER	EDITION DATE	INFOCENTRE REFERENCE	REASON FOR CHANGE	PAGES AFFECTED
0.1	31/07/07		Initial draft	all
0.2	18/09/07		Further draft following initial SAWG comments, including new Chapter 3	all
0.3	05/10/07		Development of new Chapters 4 and 5. Updates to Chapters 1 to 3	Chapters 1 to 5
0.4	19/10/07		Revised Chapters 4 and 5. Creation of two Parts to the document	Chapters 4 and 5
0.5	02/11/07		Revised Chapter 6. New Table A.3 added	Chapters 1, 3 & 6, Appendix A
0.6	05/11/07		Additions to Chapters 1 and 3. Further detail put in Appendix A.3	Chapters 1 and 3. Appendix A
0.7	10/12/07		General update following SAWG review. Removal of Chapter 5 onwards for interim publication as a separate, draft document.	All
0.8	09/01/08		Incorporation of Appendices	Appendices
0.8a	24/01/08		Minor changes in 3.4 and 3.4	29, 30
0.9	25/02/08		Revised Appendices A and C	Appendices A and C
0.91	29/02/08		Appendices transferred to Part 2. Outline of techniques added in a new Chapter 5	Chap 5, Appendices
0.92	11/07/08		Various proposed changes	all
0.93	30/04/09		Update following SAM TF review	all
0.94	10/07/09		Update following Safety Team review	all
1.0	15/01/10		Minor editorial corrections and formal release	various

CONTENTS

EXECUTIVE SUMMARY	7
1. Introduction	9
1.1 Background	9
1.2 Aims and Objectives	9
1.3 Scope	10
1.4 Applicability	10
1.5 Intended Readership & Content	11
1.6 Layout	11
2. Some Safety Concepts and FAQs	12
2.1 What is ‘Safety’?	12
2.2 How Safe do we need to be?	12
2.3 How do we show how Safe we are?	13
2.4 What is a <i>priori</i> Risk Assessment and Mitigation?	13
2.5 Are the Success and Failure Approaches to Risk Assessment new?	14
2.6 Why do we need the Success Approach?	15
2.7 What is meant by “ATM directly contributing to an accident” in ESARR 4?	15
2.8 What is meant by a “Hazard”?	16
2.9 How should Safety Assessments be documented?	16
2.10 What is a Safety Case?	17
2.11 Is there more than one type of Safety Case?	17
2.12 Why use a Safety Case?	18
2.13 Do I need to produce a Safety Case?	19
2.14 If I have an SMS do I need a Unit Safety Case?	20
2.15 What is the relationship between a Safety Plan and a Safety Case?	20
2.16 Where do Assurance Levels fit into the Picture?	21
2.17 What is the Relationship between a Human Factors Case and Safety?	21
2.18 If Safety Assessment includes the Operational Perspective, do Simulations have a part to play in the process?	22
2.19 Conclusions	22
3. A Broader Approach to Safety Assessment	24
3.1 Properties of Safety-related Systems	24
3.2 A Simple Illustration – a Car Airbag	26
3.3 A Simplified ATM Illustration – ADS-B in Non-Radar Areas	27

3.4	A Specification Hierarchy	27
3.5	Summary	29
4.	Safety Argument and the Safety Lifecycle	32
4.1	High-level Safety Argument	32
4.2	The Safety Lifecycle.....	34
4.3	Conclusions.....	42

EXECUTIVE SUMMARY

The aim of this document is to present a clear, complete, coherent and integrated approach to safety assessment that will meet the needs of EUROCONTROL and its Stakeholders, now and in the future.

It has been produced in response to:

- Stakeholder requests for a clearer, more complete and holistic view of the way to conduct safety assessments
- EUROCONTROL's own realization that new concepts currently being addressed by EATM and SESAR needs a broader approach to safety assessment.

It seeks neither to replace nor replicate the EUROCONTROL ANS Safety Assessment Methodology (SAM). Rather it is intended to describe the broad framework on to which the SAM-defined processes, and the associated safety, human-factors and system-engineering methods, tools and techniques, are mapped in order to explain their purpose and interrelationships.

The material is intended to apply to the full range of safety assessments, currently faced by EUROCONTROL and its Stakeholders, from relatively straightforward technological upgrades (eg equipment replacement), through new individual operational concepts, to the full range of new concepts and technologies being addressed by, for example, the SESAR Programme.

Having said that, it is not intended to be prescriptive – rather it may be adopted and adapted for particular applications as appropriate and necessary.

The document is divided into two parts,.

- Part 1 is aimed at a broad readership. It addresses a wide range of safety issues and explains why, in European ATM, we need to take a much broader approach to safety assessment in the face of emerging new operational concepts. Part 1 provides the foundation for Part 2 of the document
- Part 2, is aimed mainly at safety practitioners, and provides a theoretical and practical guide to safety assessment and assurance throughout a typical system lifecycle.

Page intentionally left blank

1. INTRODUCTION

1.1 Background

This guide has been produced by EUROCONTROL safety-assessment staff in response to concerns expressed by their stakeholders (internal and external) on the complexity of safety assessment documentation¹. This stakeholder feedback identified the need for a clearer, more complete and holistic view of the way to conduct safety assessments.

At the same time, it had become increasingly clear to EUROCONTROL safety experts themselves that the ANS Safety Assessment Methodology (SAM) [5], required enhancement in order to meet the needs of the new operational concepts being addressed on recent EATM Programmes and SESAR.

On the latter point, the major concern is that ATM safety assessments in the past have tended to focus on the causes and consequences of failure of ATM systems. This *failure* approach quite correctly seeks to minimize ATM's small negative contribution to the risk of an accident. However, what it cannot do is to address ATM's huge positive contribution to aviation safety – this requires a quite different, complementary approach that is known herein as the *success* approach. There are some references in SAM [5] to a success approach (or success case) but very little guidance on how to conduct one is given therein – hence a major aim of this document is to correct that deficiency.

1.2 Aims and Objectives

The aim of the guide is to present a clear, complete, coherent and integrated approach to safety assessment that will meet the needs of EUROCONTROL and its Stakeholders, now and in the future.

It seeks to demystify some of the more esoteric safety concepts and terminology.

In recognizing that the primary purpose of ATM is to reduce aviation risks, the document also explains, in straight forward terms, why the scope of ATM safety assessment needs to be broadened in order to encompass the *success* approach, including what in the past may have been thought of as “operational” (rather than safety) issues.

It seeks neither to replace nor replicate the EUROCONTROL ANS Safety Assessment Methodology (SAM). What it does is describe the broad framework² on to which the SAM-defined processes, and the associated

¹ Including at the Safety Team Meeting #34 of 3-4 Mar 09

² The “framework” is described from two viewpoints: a safety argument (structured view) and a safety lifecycle (process view). It is hoped that the rationale for this will become clearer to the reader in Chapter 2 onwards.

safety, human-factors and system-engineering methods, tools and techniques, are mapped in order to explain their purpose and interrelationships.

The ideas communicated herein are based on considerable practical experience of, ATM safety developments across EATM Programmes, EEC, SESAR and ANSPs, and on the results of some ATM research activities³.

Although the document represents the EUROCONTROL Agency view on how to conduct safety assessments, the material presented herein is not intended to be prescriptive – rather it may be adopted and adapted for particular applications as appropriate and necessary. It will go through the usual reviewing and commenting process as any other SAM-related document, including endorsement by the Safety Team.

1.3 Scope

In terms of the safety lifecycle, this version of the guide focuses more on the initial stages, through to (and including) the specification and validation of Safety Requirements.

More detail on the later stages of the lifecycle will be covered in subsequent versions of the document.

In order to contribute to a total system approach, the guide encompasses all major elements of the “end-to-end” ATM system – ie airspace design, people, procedures and equipment, including ground-based, airborne and space-based elements.

Although quite a lot of the detail herein is focused on the safety assessment of changes to the ATM service / system (as per ESARR 4), the document also makes numerous references to the safety assessment of on-going operations.

Although some links to relevant safety regulations are given herein, it would not be appropriate for a document such as this to give more than general guidance in this respect. In particular, the specific question as to whether the a *success* approach in safety assessment is essential for compliance with CR 2096/2005 / ESARR 4, or whether it goes beyond the minimum requirements of those regulations, is not addressed - the answer to that depends to some extent on how the regulations are interpreted, and that is a matter best taken up with the appropriate regulatory body.

1.4 Applicability

This guide is intended to apply to the full range of safety assessments, currently faced by EUROCONTROL and its Stakeholders, from relatively straightforward technological upgrades, through new individual operational

³ Includes such things as human factors research, static risk modelling, dynamic risk modelling, resilience engineering etc

concepts, to the full range of new concepts and technologies being addressed by, for example, the SESAR Programme.

1.5 Intended Readership & Content

As described in more detail in section 1.6 below, the document overall is divided into two parts.

- Part 1 addresses a wide range of safety issues and explains why, in European ATM, we need to take a much broader approach to safety assessment in the face of emerging new operational concepts. It provides an important foundation for Part 2 of the document.
- Part 2 is aimed mainly at safety practitioners. It provides a theoretical basis for, and practical guide to, safety assessment and assurance throughout a typical system lifecycle.

1.6 Layout

Part 1 consists of three further Chapters, as follows.

Chapter 2 introduces a number of safety concepts and seeks to provide an initial response to a number of “**frequently asked questions**”. It starts with the regulatory context, leads through the perceived need for a broader approach to safety assessment (than has often been practised in the past), and on to the idea of safety cases and safety assurance.

In **Chapter 3**, it is explained in more detail why a purely failure-based approach to ATM safety assessment⁴ is not sufficient to support the new ATM concepts that are currently being considered in EATM and planned for SESAR. It shows how the addition of a success-based approach leads to a more complete specification of an ATM system’s safety properties, and introduces a high-level Safety Argument framework to support this **broader approach to safety assessment**.

Chapter 4 shows how the broader approach to safety assessment fits into the various stages of a typical **safety lifecycle**, and introduces the concept of **safety assurance**.

A list of **references** is given in **Annex 1**

Annex 2 provides a **glossary** of the terms and abbreviations used in the document.

⁴ As has often been followed on European ATM safety assessments in the past

2. SOME SAFETY CONCEPTS AND FAQs

This chapter introduces a number of safety concepts and seeks to provide responses to a number of “frequently asked questions”.

The issues that are addressed start with the regulatory context, lead through the perceived need for a broader approach to safety assessment (than has often been practised in the past), and on to the idea of safety cases and safety assurance.

This then provides the basis for the subsequent chapters of the document.

2.1 What is ‘Safety’?

Safety is defined in SES CR 2096/2005 and ESARR 4 [1] as ‘freedom from the risk of unacceptable harm’. In these regulations, *harm* is understood to mean an accident involving death / serious injury to personnel and / or major structural damage to aircraft.

SES CR 2096/2005 and ESARR 4 defines risk as the combination of the overall probability, or frequency, of occurrence of a harmful effect induced by a hazard and the severity of that effect.

In other words a safe situation exists when the risk of an accident is *acceptably* low, where *acceptable* is as defined in section 2.2 below.

2.2 How Safe do we need to be?

There are four main sources for this at the overall European ATM level - the first two are closely related to each other:

- ATM 2000+ [2] requires the risk of an accident not to increase [with time] and preferably decrease [despite the continuing increase in traffic levels)
- ESARR 4⁵ provides a quantification of the above ATM 2000+ safety objective, in relation to the design of new systems / changes to existing systems; this is expressed as a maximum [tolerable] risk of an accident of 1.55×10^{-8} per flight hour and takes account of the predicted increase in traffic up to the year 2015

⁵ Although, in the context of *a priori* safety assessment, SES CR 2096/2005 is equivalent to ESARR 4, it does not include the quantified safety target specified in ESARR 4.

- SES CR 2096/2005 and ESARR 3 [3] place a general obligation on ANSPs to "reduce risk as far as reasonably practicable" [*AFARP*⁶]
- SES CR 2096/2005 and ESARR 4 also state that: "As a necessary complement to the demonstration that these quantitative objectives are met, additional safety management considerations shall be applied so that more safety is added to the ATM system whenever reasonable"
- the SES Mandate given to EUROCONTROL to develop an Implementing Rule for a Risk Classification Scheme – this will require the setting of ECAC-wide and national Safety Targets to be used in the design of ATM services / systems.

In EUROCONTROL, we usually say that for risk to be acceptable it must be no higher than tolerable and it must be further reduced *AFARP*.

2.3 How do we show how Safe we are?

By carrying out a Safety Assessment comprising typically:

- an **a priori**⁷ *risk assessment and mitigation* of changes to the ATM system, in compliance with SES CR 2096/2005 and ESARR 4 (see section 2.4 below).
- **in-service safety monitoring** of on-going operations, in compliance with EC directive 42/2003 and ESARR 2 [4].
- *incident investigation and corrective action*, in relation to on-going operations, accordance with EC directive 42/2003 and ESARR 2 – this is a very important contributor to the achievement of the *AFARP* objective
- **in-service safety surveys** of on-going operations in compliance with SES CR 2096/2005 and ESARR 3.

2.4 What is a *priori* Risk Assessment and Mitigation?

It is part of an overall Safety Assessment, and has two facets, as defined in the EUROCONTROL Safety Assessment Methodology (SAM) [5] and amplified in one of the SAM Guidance Material: the EUROCONTROL Safety Case Development Manual (SCDM)⁸ [6]:

⁶ Note that EUROCONTROL does not use the term *ALARP* (as low as reasonably practicable) because that term has a particular meaning in UK Health & Safety legislation

⁷ *A priori* is used here in the sense of reasoning from causes (safety properties of the system) to effects (accidents or incidents). The three bullets that follow are *a posteriori* in that they reason from effects (accidents or incidents) to causes.

⁸ Although the SCDM is part of SAM (ie SAM Part IV Annex I) it is referred to separately, where appropriate

- the **success** approach – which seeks to assess the achieved level of safety when the ATM system in question is working as intended – ie in the absence of failure
- the **failure** approach – which seeks to assess the effect, on the achieved level of safety, in the event of failure (ie deviation from what is intended) internal to the ATM system.

Chapter 3 outlines how the *success* and *failure* approaches should be used together in the developing the Safety Requirements for a new ATM system (or change to an existing ATM system) and showing that satisfaction of those Safety Requirements would result in an acceptable level of safety.

2.5 Are the Success and Failure Approaches to Risk Assessment new?

From a safety perspective, the formal demonstration of the *success* approach is new in ATM – the *failure* approach is not new.⁹

For historical reasons (largely to do with the origins of the SAM) most European ATM risk assessments have, until recently at least, focussed on a negative, failure-based view of ATM – ie have been concerned mainly with what happens if the system under assessment fails in some way¹⁰.

The more positive view of ATM system behaviour – eg its effectiveness in reducing the risk of collision between aircraft through the provision of separation - has also been addressed in the past but largely from an “operational” perspective and was not formally requested to be demonstrated from a safety point of view. It was mainly based on *a priori* operational judgement via simulation or trials and on *a posteriori* adjustments using operations feedback.

What is new is inclusion of this operational perspective within the scope of risk assessment, to form what is known as the *success* approach. The *success* approach is already mentioned in the SAM [5] (with some amplification given in the SCDM [6]) but only limited guidance on how to go about it is given in those documents.

The *success* approach also expands the definition of “hazard” as per ESARR 4: “*Any condition, event, or circumstance which could induce an accident.*” The *success* approach is based on the interpretation of ESARR 4 definition of a hazard being also a “normal” event in the sense that hazards that are inherent in aviation are what ATM continuously mitigates to the maximum degree and extent possible, in normal operation – see section 2.8 below.

⁹EC Regulation 552/2004, Annex II, Part A, section 3 does however, state that “A harmonized set of safety requirements for the design, implementation, maintenance and operation of systems and their constituents, both for normal and degraded modes of operation, shall be defined with a view to achieving the agreed safety levels, for all phases of flight and for the entire EATM Network.

¹⁰ See section 2.8

The success approach has been applied by EUROCONTROL to recent operational changes (e.g. FASTI, Anticipated Landing Clearance, ADS-B in Non-Radar Areas, ADS-B RAD and to some major ANSP changes)¹¹.

2.6 Why do we need the Success Approach?

It is acknowledged that a restricted view of safety (ie a view restricted to consideration of failure only) may not have been a major problem in the past (because of the then gradual evolution of ATM systems, relying on the assumption / operational experience that ATM was intrinsically safe when no failure occurs).

However, experience on recent EATM programmes has shown that such a pre-occupation with failure-related properties of the system (leading to neglect of consideration of the intended operations / functions) cannot be sustained in the face of more radical changes being considered for ATM over the next 20 years or so¹².

2.7 What is meant by “ATM directly contributing to an accident” in ESARR 4¹³?

The answer to this question is fundamental to understanding the need for the *success* approach. The following quote from the EUROCONTROL public website gives some insight:

“Safety is the top priority in aviation. The main purpose of ... ATM services is to ensure the safe separation of aircraft in the air and on the ground, while maintaining the most efficient operational and economic conditions. ... ATM services are rarely implicated in fatal aviation accidents. However, the ATM community remains at the forefront of initiatives aimed at improving aviation safety”

It seems, therefore, that SES CR 2096/2005 and ESARR 4 are concerned with maximizing the likelihood of ATM preventing aviation accidents that would otherwise have happened, and not just with minimizing accidents (or incidents) caused by *failure* of ATM and that would otherwise not have happened.

This interpretation is also entirely consistent with SESAR Deliverable D4 [8], which makes the following key points concerning ATM safety:

“...the need for ATM to maximize its contribution to aviation safety and

¹¹ It was also implicit in the EUROCONTROL and ANSP EUR RVSM safety cases, although not described as such at the time

¹² An example of this, using ADS-B in Non-radar airspace, is given in section 3.3 below – this explains that a simple, failure approach would not answer the fundamental question as to whether it would be safe to use ADS-B to support 3 or 5 nm separation

¹³ The EUROCONTROL Agency Safety Policy uses the term “ATM-induced accidents”

the need for ATM to minimize its contribution to the risk of an accident”.

We will see in section 3.1 below that it is the *success* approach that is concerned with maximizing ATM’s contribution to aviation safety and that it is the *failure* approach that is concerned with minimizing ATM’s contribution to the risk of an accident.

2.8 What is meant by a “Hazard”?

ESARR 4 defines a hazard as being “any condition, event, or circumstance which could induce an accident”.

SAM FHA Chapter 3, under the heading of “*Identify Potential Hazards*” describes this step as identifying “*What could go wrong with the system and what could happen if it did*”. Unfortunately, this leads to a rather narrow interpretation of a hazard that is related only to the second point quoted from SESAR D4, in section 2.7 above – ie ATM’s (negative) contribution to the risk of an accident.

What it misses is ATM’s (positive) contribution to aviation safety – in order to address this, we need to understand that:

- aviation is an inherently hazardous occupation
- those hazards that are inherent in aviation are not associated with failure of the ATM system
- the ATM system is required to reduce the risk associated with those inherent hazards as much as possible
- it is the functionality and performance of the ATM system that determines how successful ATM is in reducing such risks.

Thus we need a much broader interpretation of what a hazard is than that implied in SAM and, therefore, section 3.1 below addresses two types of hazard, in relation to the ATM system:

- “pre-existing” hazards, which the ATM system has to mitigate
- “system-generated” hazards, which are created by failure of the ATM system.

2.9 How should Safety Assessments be documented?

The way of documenting the results of Safety Assessments recommended in SAM is as follows:

- individual reports, recording the results of a *a priori* risk assessment processes (eg risk modelling, design analysis, simulations, Functional

Hazard Assessment (FHA) (Cf: SAM-FHA Chapter 5 GM A), Preliminary System Safety Assessment (PSSA) (Cf: SAM-PSSA Chapter 5 GM A), and System Safety Assessment (SSA)) (Cf: SAM-SSA Chapter 5 GM A), safety monitoring and incident investigation / corrective action

- a Safety Case (see SCDM [6]) report to bring all the main findings of the individual reports together in a single document in order to show, in a clear unambiguous way, that an acceptably level of safety is being (or will be) achieved.

2.10 What is a Safety Case?

A Safety Case is similar to a legal case – indeed that is where the idea originally came from.

Under an adversarial legal system, cases are prepared by both the prosecution and the defence. Each case is presented as a series of **arguments**, deriving from an overall claim of guilt (or innocence), followed by the presentation of **evidence** to show that each argument is true.

The same idea applies to a Safety Case, except that the overall Claim is invariably that something (eg a service or system) is acceptably safe. The Safety Case then breaks the Claim down into a set of **Safety Arguments**, each supported by rationales and **Evidence**, such that the Claim may be considered to be valid if (and only if) the Evidence shows each Argument to be true.

However, the analogy with a legal case breaks down in one very important respect - for a Safety Case, the *burden of proof* rests with the “defence” and it is up to the authors of a Safety Case to prove that something is safe, rather than for some other body (eg a regulator) to prove that it isn’t safe!

2.11 Is there more than one type of Safety Case?

The EUROCONTROL SCDM [6] identifies two main types of Safety Case:

- those which are intended to demonstrate the on-going safety of a service and/or system
- those which are intended to demonstrate the safety of a significant change to a service and/or system

In the EUROCONTROL SCDM [6], the former is known as a **Unit Safety Case** and the latter as a **Project Safety Case**. They are interrelated, as explained below, but since they are somewhat different in approach it is important to decide which is applicable in a particular situation.

Whereas it may be appropriate to produce a (Project) Safety Case whenever a substantial change¹⁴ to an existing safety-related system (including the introduction of a new system) is to be undertaken, if that is all that we do - ie we do not also establish the absolute safety of the on-going service – then there is a danger that:

- such changes are being built on weak foundations, and/or
- after several changes to the ATM system have been made (especially when changes are made to earlier changes) the task of providing coherent safety assurance information might become increasingly difficult.

Therefore, in order to provide a solid foundation for change, a provider of a safety-related service / facility may decide that it is appropriate and efficient to have, and maintain, a Unit Safety Case which shows that the on-going, day-to-day operations are safe.

Project Safety Cases would then be used to update, and usually subsumed into, the Unit Safety Case, such that a clear baseline for future changes is always maintained.

2.12 Why use a Safety Case?

SES CR 2096/2005 and ESARR 3 state that:

*“The prime responsibility for the safety of an ATM service rests with the service provider. Within the overall management of the service, the service provider has a responsibility to ensure that all relevant safety issues have been satisfactorily dealt with and **to provide assurance that this has been done**”.*

In his report on the investigation into the Piper Alpha Oil Platform accident [7] Lord Justice Cullen wrote that:

*“**Primarily** the Safety Case is a matter of ensuring that every company produces a formal safety assessment **to assure itself that its operations are safe**.*

*Only **secondarily** is it a matter of demonstrating this to a regulatory body. That said such a demonstration both meets a legitimate expectation of the workforce and the public and provides a sound basis **for regulatory control**.”*

It can be seen that these two quotes are perfectly consistent, in that:

¹⁴ The definition of “substantial change” in this respect is very application-specific and should be defined in the relevant Safety Management System. The fact that a formal safety case may not be needed for smaller changes, it does not mean that some form of safety assessment and report is not required – but see sections 6.2.3 and 8.3 of SRC guidance document EAM4 / GUI1 [12]

- they both place responsibility for safety clearly with the service provider
- SES CR 2096/2005 and ESARR 3 state the requirement for assurance to be provided, without prescribing how it should be documented, and Cullen recommends the use of the Safety Case for the provision of assurance.

A Unit Safety Case would, therefore, be one way of documenting the assurance required by SES CR 2096/2005 and ESARR 3.

Whereas the above is more concerned with the on-going situation, SES CR 2096/2005 and ESARR 4 are concerned with the risk assessment of changes to that situation - in particular, item 3.2.3 of Annex II to SES CR 2096/2005 states the following:

*“The results, associated **rationales** and **evidence** of the risk assessment and mitigation processes, including hazard identification, shall be collated and documented in a manner which ensures that:*

- *complete **arguments** are established to demonstrate that the constituent part under consideration, as well as the overall ATM functional system are, and will remain tolerably safe by meeting allocated safety objectives and requirements. This shall include, as appropriate, specifications of any predictive, monitoring or survey techniques being used,*
- *all safety requirements related to the implementation of a change are traceable to the intended operations / functions”.*

Since Safety Cases, as described in SCDM [6], are based on arguments, evidence and rationales, then a Project Safety Case would be an appropriate way of addressing the SES CR 2096/2005 / ESARR 4 requirement.

2.13 Do I need to produce a Safety Case?

No - there is no explicit regulatory requirement to produce Safety Cases. EAM 4 / GUI 1 [12] merely states the following as guidance:

“In addition, documenting the results and related evidence that the system is adequately safe for its specified operational objectives and operational environment will help in the safety regulatory review and related safety approval.

ESARR 4 does not provide any guidance on how this documentation should be done, especially with regard to the imbrications [sic] of / interfaces between various safety arguments for an ATM System.

Depending on the national situation, various options could be considered in terms of scope of the safety documentation, ranging from:

- a single safety argument/case for the whole national ATM system and airspace, in the case of a single ANS service provider in a small country,
- a set of safety arguments/cases for each of the operational units (ACC, TWR), and related major system/operational capabilities (e.g. RVSM, RDPS) with appropriate traceability and cross references to, and
- a safety case/argument for each and every change to the ATM System”.

Therefore, although section 2.12 above proposes that suitable Safety Cases may be one way of satisfying the regulatory requirements quoted in that section, it is important to note that there may well be other, equally valid ways of satisfying those same requirements.

2.14 If I have an SMS do I need a Unit Safety Case?

ESARR 3 defines a *Safety Management System* (SMS) as a systematic and explicit approach to defining the activities by which safety management is undertaken by an organization in order to achieve acceptable safety.

Thus an SMS will define what is acceptably safe in the local context and will describe the specific **responsibilities and procedures** (including risk assessment, safety monitoring, incident investigation / corrective action, safety documentation etc) for demonstrating, in a visible and traceable way, that an acceptable level of safety is being achieved.

As indicated in section 2.12 above, a Unit Safety Case (USC) is one way of documenting the **results** of applying the SMS processes. This is not intended to imply that a USC is limited by the content of the SMS. On the contrary, the introduction of a comprehensive USC may well reveal (and facilitate correction of) limitations in a pre-existing SMS.

So, an SMS and a USC are complementary.

2.15 What is the relationship between a Safety Plan and a Safety Case?

A Safety Plan is produced at the start of a project and should identify (inter alia) all the activities that are needed in order to generate the evidence needed for the Safety Case that is issued at the end of the project. It also helps scheduling of safety-related activities in coordination with the Project activities (eg when to reconcile safety, performance, security, interoperability requirements).

The most effective way of ensuring that nothing has been missed is to produce a Safety Argument very early in a project and base the activities in

the Safety Plan on generating the Evidence needed to support the Safety Argument.

Because the Safety Argument also forms the framework of the Safety Case this approach also facilitates management and traceability of the assurance activities.

This is explained further in section 4.2.1 below.

2.16 Where do Assurance Levels fit into the Picture?

As discussed above, a Safety Case presents Argument and Evidence that a system or service is safe.

The weakness (but also the strength) of the Argument approach is that Arguments are deliberately expressed as predicates – ie statements that can only be true or false. Evidence is then collected, and presented, to show that the Argument is true¹⁵. The problem is that such Evidence is rarely absolutely conclusive and so we are left with the question – how much confidence do we need that the Evidence is complete, correct and satisfies the Argument?

In essence, the purpose of Assurance Levels, as currently set out in SAM for software, maintenance intervention and operational procedures¹⁶, is to specify how much Evidence is needed, how that Evidence should be obtained, and the rigour required of that Evidence, all of which are determined by the safety-criticality of the subject of the Safety Assessment / Safety Case.

In Chapter 4.2 onwards we will see how Assurance Levels are used in practice, for the human, procedure and software aspects of the system, together with the additional need for system-level assurance to support the success and failure approach described in Chapter 3.

In addition, Assurance Levels per system element contribute to provide a certain level of confidence that the risk is acceptable, especially when the quantitative aspect of the demonstration is impracticable and/or there is insufficient data to give the required level of confidence on their own.

2.17 What is the Relationship between a Human Factors Case and Safety?

The purpose of the HF Case process [9] is to identify, document and manage, from beginning to end, all significant issues relating to the role of human operators in ATM systems that arise during an ATM project.

Many of these issues may, of course, relate directly (or indirectly) to the safety of the ATM Service and would therefore need to be captured within the safety assessment process and the resulting Safety Case.

¹⁵ By convention, Arguments are usually expressed in a positive sense – such that the desired outcome is that they are shown to be true.

¹⁶ ALs for human tasks are currently being developed as Human Assurance Level (HAL).

The HF Case process is complementary to, not a substitute for, a rigorous safety assessment. In Part 2, we will see how the safety-related issues, from the HF Issues Analysis in particular, should be integrated into the Safety Lifecycle.

2.18 If Safety Assessment includes the Operational Perspective, do Simulations have a part to play in the process?

Yes – simulations (both real-time and fast-time) are a very important source of evidence concerning the dynamic behaviour of the system.

It is very important, in planning a project, to identify safety issues relating to dynamic behaviour as early as possible so that addressing them can be included in the simulation plan.

2.19 Conclusions

This chapter has proposed that we need a broader approach¹⁷ to safety assessment and assurance, which comprises:

- a *success* approach, assessing the achieved level of safety when an ATM system when working as intended (ie in the absence of internal failure), and addressing ATM's (positive) contribution to aviation safety, and
- a *failure* approach, assessing the effect on the achieved level of safety of possible failures (ie deviation from what is intended) internal to the ATM system, and addressing ATM's (negative) contribution to the risk of an accident.

It has also proposed (in line with the SAM) the use of a Safety Argument and Assurance Levels, for planning safety activities, and the use of a Safety Case to bring together, in a summary form, the results from all those activities.

The next section explains further the rationale for, and form of, the broader approach to Safety Assessment.

¹⁷ Broader in relation to some past practices in ATM safety assessment.

Page intentionally left blank

3. A BROADER APPROACH TO SAFETY ASSESSMENT

This chapter expands on the broader (ie success- and failure-based) approach to Safety Assessment that was introduced in section 2.

It explains why a purely failure-based approach to ATM safety assessment is not sufficient to support the new ATM concepts that are currently being considered in EATM and planned for SESAR. It shows how the addition of a success-based approach leads to a more complete specification of an ATM system’s safety properties, and introduces a high-level Safety Argument framework to support the broader approach.

3.1 Properties of Safety-related Systems

Consider the two systems shown in Figure 1 below.

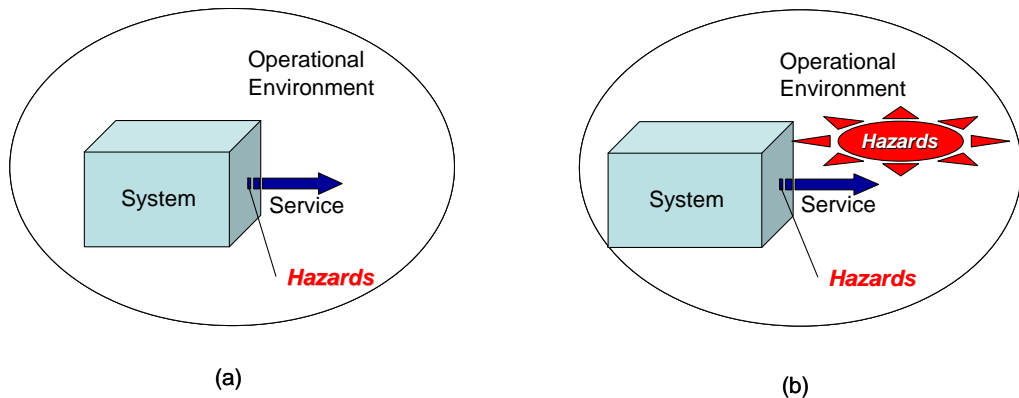


Figure 1 – Safety-related Systems

Figure 1(a) is intended to portray (in a very simple way) a model that is applicable to systems which provide a service (or generate a product) in a way that is inherently dangerous – eg an overall nuclear-power plant¹⁸. As well as providing a service / product (eg electrical power), such systems present **hazards** to the environment in which they operate – these hazards (and associated risks) are system-generated, in that they result from some sort of failure within the system and are, by convention, shown at the boundary of the system.

From a safety point of view, we don’t really care whether the system produces an output or not, provided any risks associated with the (system-generated) hazards are acceptably low.

¹⁸ For the very simplified illustration in Figure 1(a), we are considering the overall plant. If, however, we were to consider the control systems within those plants then Figure 1(b) would apply

Figure 1(b) portrays a very different model. In this case, the main hazards (and associated risks) are pre-existing in the operational environment of the system. These hazards are, therefore, not caused by the system – rather, the sole purpose of introducing the system is to eliminate those pre-existing risks or at least maintain them at an acceptably low level - this is the case for, for example, a car airbag (see below), a railway-signalling system or an **ATM system**¹⁹. Of course such systems, like those represented by Figure 1(a), may also bring with them new hazards, as indicated also in 1(b).

Now, from a safety point of view, we do care whether the system in case (b) generates an output (service) because it is what this service does (ie its functionality), and how well it does it (ie its performance), which determine how effective the system is in managing the hazards risks that pre-exist. In so doing, we must also ensure that, as in the case (a), that any risks associated with the (system- generated) hazards are acceptably low.

This leads to two different sets of **safety properties**:

- In **case (a)**, provided the system does not fail (in a hazardous way) then it must be safe. Thus we are concerned only with the **integrity** of the system and with ensuring that the integrity is sufficiently high to make the risks generated by the system acceptably low.
- Applying that reasoning to **case (b)** would be wholly inadequate, since we must ensure not only that risks generated by the system are acceptably low (ie the system has sufficient **integrity**), as in case (a), but also that the **functionality and performance** of the system are sufficient to reduce the pre-existing risks to an acceptably low level.

The former bullet is called a **failure approach** since it is concerned only with failure of the system.

The latter bullet is called a **success and failure** approach since it covers not only new hazards and risks caused by failure of the system under consideration but also how successful that system needs to be in addressing pre-existing hazards²⁰ and reducing the associated risk. It is this broader approach that is now being applied by EUROCONTROL to ATM safety assessment.

¹⁹ In ATM systems, the physical boundary between the system and its operational environment is becoming blurred by the incorporation of parts of the environment into the systems. Therefore, it is sometimes better to think of the operational environment as being simply the domain of the users of the ATM service.

²⁰ In section 2.7 above, it was inferred that ESARR 4 is concerned as much with maximizing the *success* of ATM in preventing aviation accidents that would otherwise have happened, as it is with minimizing accidents (or incidents) caused by *failure* of ATM and that would otherwise not have happened. If that interpretation is correct, then it follows that the ESARR 4 references to “hazards” must include pre-existing aviation hazards as well as hazards caused by failures of the ATM system.

3.2 A Simple Illustration – a Car Airbag

Figure 2 shows a simplified single-axis risk graph for a car front-seat airbag. R_U is the risk associated with driving a car without an airbag – therefore, it fits the definition of pre-existing risk.

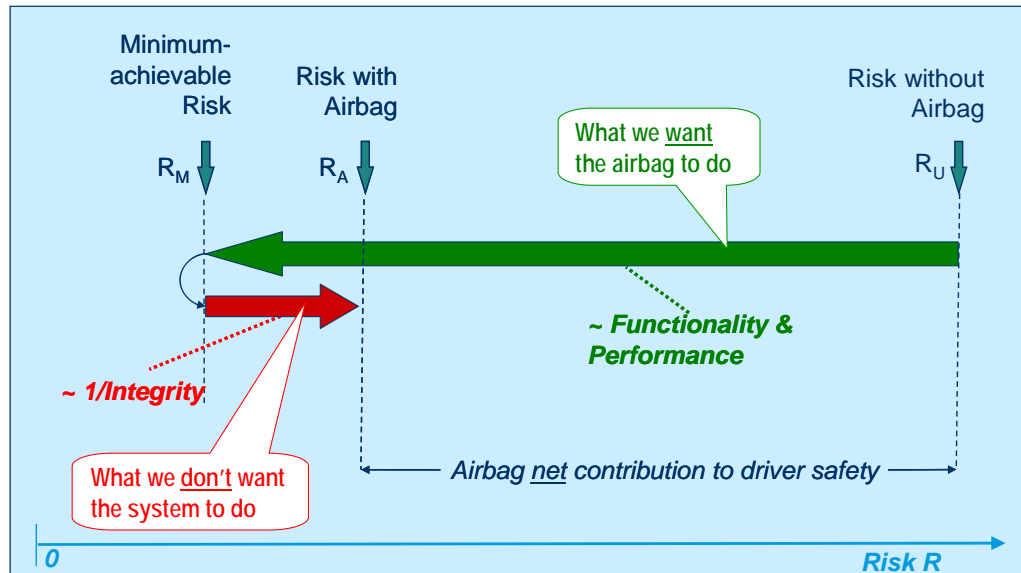


Figure 2 – Risk Graph for a Car Airbag

There are two things that we need to consider regarding safety:

- the *success* approach, or what we want the airbag to do - ie reduce the pre-existing risk of death / serious injury in the event of a head-on collision as much as possible. The lowest level of risk achievable, in the absence of failure, is shown as R_M and will be determined by what we could describe as the *functionality and performance* of the airbag – eg its size, strength of the material, inflated volume, compressibility, location, sensitivity of the deployment mechanism, speed of deployment etc
- the *failure* approach, or what we don't want the system to do – ie to fail to deploy when needed or to deploy when not needed. Such system-generated failures will cause the risk to increase from the level R_M to a level R_A , the amount of that increase being determined by the integrity of the airbag including, in the case of spurious deployment, over-sensitivity of the deployment mechanism.

Thus the net contribution of the airbag to driver safety is $R_U - R_A$, and the case for the airbag would be based on R_A being $\ll R_U$.

Although a car airbag is a “safety net”, operating only on demand, the above principles can be applied equally to a continuously-operating safety function – eg a car steering system.

3.3 A Simplified ATM Illustration – ADS-B in Non-Radar Areas

ADS-B in NRA is a programme being undertaken by EUROCONTROL and some ANSPs. EUROCONTROL’s responsibility is, inter alia, to specify Safety Requirements such that ADS-B in NRA would be safe, whereas ANSPs are responsible for implementation based on EUROCONTROL’s (or their own derived) Safety Requirements.

The objective is to introduce a radar-like ATC service into what are currently non-radar areas using only ADS-B technology for surveillance. The aim is to reduce separation minima, from current procedural levels, down to “radar” levels – ie 5 nm or 3 nm, depending on the area of application.

Clearly, the ADS-B end-to-end system needs to be reliable but, even if it were 100% so, that would not give us the answer to the key question as to whether ADS-B would be safe enough to support 3-5 nm separation – so what would give us that answer?

First of all it needs to be remembered that separation provision is a major part of ATM’s positive contribution to aviation safety and that some of the key considerations in determining “radar” separation minima are the accuracy, resolution, refresh rate etc of the surveillance information presented to the Controller. Thus, for example, if these properties of the surveillance information were to be significantly degraded then it would be necessary to increase the separation minima otherwise ATM’s contribution to aviation safety would be degraded – equivalent to shortening the green arrow in Figure 2.

The **success** approach taken in the EUROCONTROL Safety Case for ADS-B in NRA is to use the huge amount of operational experience of ATC radar services, based on 3-5 nm separation. Therefore, by assuming that such services are accepted as being safe, and by showing²¹ that ADS-B can provide the same functionality (ie data presented to the Controller / support tools) and performance (data accuracy, resolution, latency, refresh rate, coverage etc), we have the basis of a very good case for ADS-B being able to support the same separation minima, and make at least the same contribution to reducing aviation risk, as radar systems have done and continue to do.

Having established that, the **failure** approach is being used to ensure that potential failures in the ADS-B system are controlled such that positive contribution of ADS-B to ATC is not diminished significantly by such failures.

3.4 A Specification Hierarchy

Figure 3 shows an ATM specification hierarchy, capturing the *success* and *failure* approaches and the related safety properties.

It is based on, but also expands upon, the existing SAM approach.

²¹ This was done in the Operational Performance Assessment carried out under ED-78A

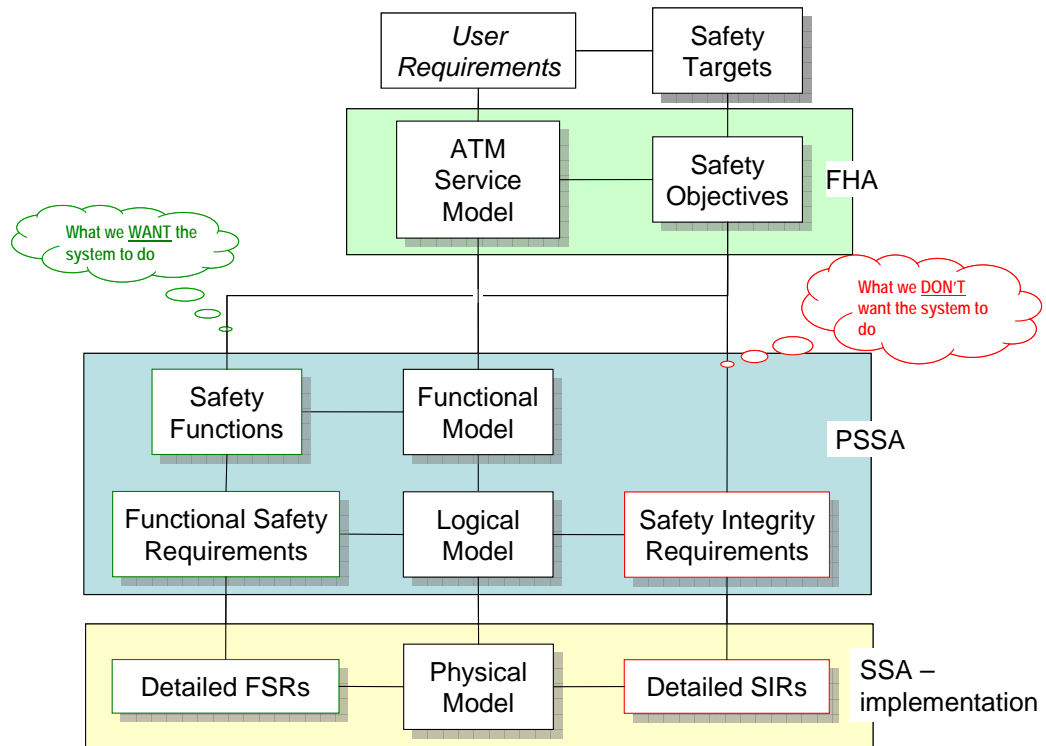


Figure 3 – Specification Hierarchy

The whole process is driven by an identified User Need – eg to increase capacity, improve safety etc.

Safety Targets in effect define what we mean by ‘safe’ in the context of the User Need, for example:

- if the User Need was to **increase capacity** then it might be sufficient to set Targets such that safety²² would not be degraded in satisfying that Need
- on the other hand, if the User Need was to **improve safety** then it would be necessary to set Targets to require the improvement to be not only substantial but also as great as reasonably practicable under the circumstances.

Safety Objectives are defined at the ATM-service level; they determine the (positive) contribution to reducing pre-existing risk as well as the maximum occurrence rate of the system-generated hazards that are required in order to satisfy the Safety Target(s).

The **failure**-based approach, detailed in the SAM, is indicated mainly by the right-hand column of boxes²³, supported by appropriate representations of the

²² In relation to pre-existing and system-generated risks

system shown down the centre. This approach deals solely with system failure – ie what we don't want the system to do - and results in:

- Safety Integrity Requirements²⁴, which determine the integrity required of the elements of the system **logical** architecture (see below), in order to limit the system-generated risk as specified in the Safety Objectives
- Detailed Safety Integrity Requirements, which apportion the high-level Safety Integrity Requirements on to the **physical** architecture.

The **success** approach is additional to what is currently detailed in the SAM and is indicated by the left-hand column of boxes. It deals with what we do want the system to do – ie to make a substantial contribution to the reduction of aviation risk – and results in:

- Safety Functions – eg *Tactical Conflict Resolution* and *Surveillance* – which specify the functionality and performance required of each element of the Functional Model, in order to deliver the positive contribution to pre-existing risk specified in the Safety Objectives. The Functional Model is a high-level, abstract representation of the system functionality that is entirely independent of the logical design and of the eventual implementation of the system. It describes the Safety Functions but not who or what performs them
- Functional Safety Requirements, which result from allocating the Safety Functions on to the elements of the Logical Model. This model is a high-level, architectural representation of the system design that it is independent of the eventual physical implementation of that design. It describes the main human tasks, machine functions and airspace design and what each of those “actors” provides in terms of safety functionality and performance – it normally does not show elements of the physical design, such as hardware, software, human-machine interfaces, procedures, training etc.

3.5 Summary

The following matrix summarizes the main features of the broader (success and failure) approach to safety assessment.

²³ Mitigations derived in the failure approach are actually captured in the left-hand column, since they are functional in nature

²⁴ SAM does not use the specific terms Safety Integrity Requirements (or Functional Safety Requirements – see overleaf) – only the more general term Safety Requirements. The former terms are used here only to emphasize the distinction between the main outputs of the success and failure approaches. ||

	Success	Failure
Hazard-types Addressed	Pre-existing Hazards	System-generated Hazards
Safety Contribution	Maximize ATM contribution to aviation safety	Minimize ATM contribution to risk of an accident
Dominant Safety Properties	System Functionality and Performance	System Integrity

Having thus established the need for the broader approach to safety assessment by this point in the document, it is unnecessary (indeed it might unhelpful²⁵) for this to be continued to be expressed in terms of distinct, *success* and *failure* approaches.

Therefore, the remaining Chapters do not make that distinction – rather they provide an integrated approach to the assurance of both the **functionality & performance** and the **integrity** of the ATM system, throughout its lifecycle.

²⁵ For example, although the matrix shows the dominant safety properties in each case, in practice there is degree of “cross-over” between the two sets of safety properties and the two approaches.

Page intentionally left blank

4. SAFETY ARGUMENT AND THE SAFETY LIFECYCLE

This chapter describes the high-level safety argument and its relationship with the safety lifecycle.

4.1 High-level Safety Argument

The key point about the broader approach to safety assessment is that it is argument-driven – there is a process to be followed but that process comprises a series of safety assurance activities which themselves are defined by the safety argument.

If we wanted to demonstrate (in, say, a Safety Case, just prior to entry into operational service) that a proposed change Subject X would be *acceptably safe* (as defined by the agreed Safety Targets), in a defined operational environment, then we could do so by showing that²⁶:

1. *Subject X* ATM System has been **specified** to be *acceptably safe*
2. *Subject X* ATM System has been **designed** to be *acceptably safe*
3. *Subject X* ATM system design has been **implemented** completely and correctly
4. The **transition** from current state to full *Subject X* ATM system will be *acceptably safe*
5. *Subject X* ATM system will be shown to **operate** *acceptably safely* throughout its service.

We would probably also want to justify why the change was being made (eg increasing capacity to meet airspace user demands) and also declare any fundamental assumptions that were being made (eg that the ATM system before the change was at least tolerably safe).

Figure 4 presents exactly the same information in pictorial form, using what is called Goal-structuring Notation (GSN – this is the format suggested in the EUROCONTROL Safety Case Development Manual [6]).

The logic underlying Figure 4 is that the top-level Argument (Arg 0) can be claimed to be true if (and only if) Arg 1 to Arg 5 are shown to be true.

²⁶ This Safety Argument is adapted from that shown in section 5 of the EUROCONTROL Safety Case Development Manual [6].

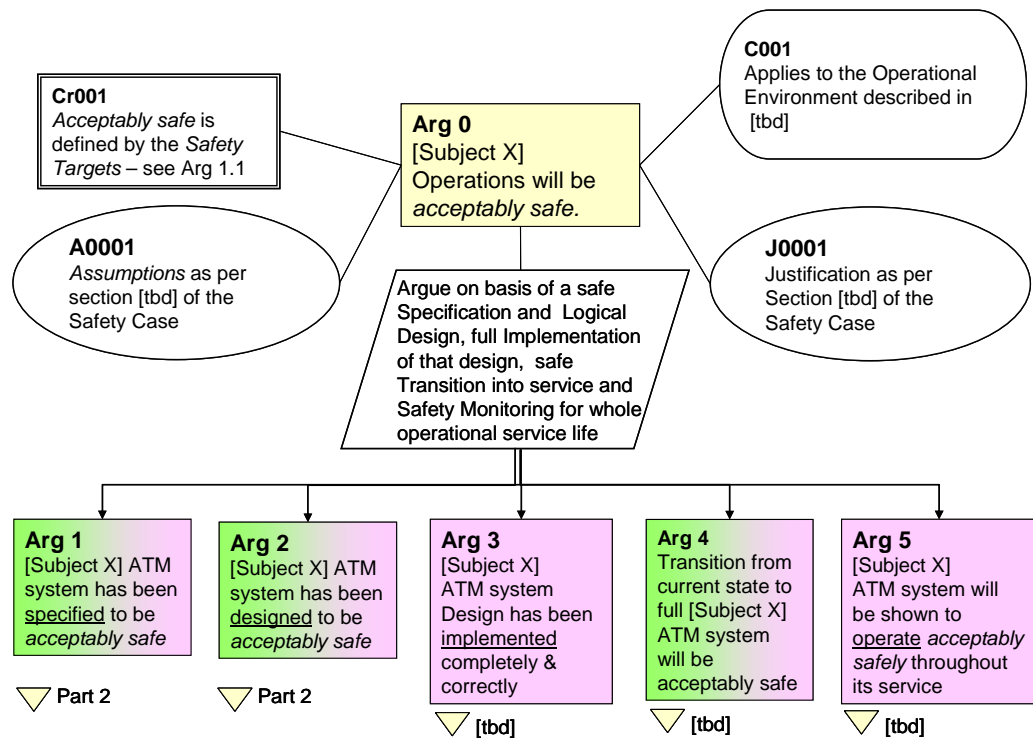


Figure 4 – Generic Safety Argument – Level 0/1

Arg 1 is concerned with specifying the functionality, performance and integrity properties of the ATM system at the level of the ATM Service, such that the Safety Targets would be satisfied.

Arg 2 is concerned with the design of the ATM system at the level of a logical architecture and showing that:

- the design satisfies what has been specified under Arg 1, and
- the design is realistic (ie achievable) in terms of the requirements it places on the human and technological elements of the system.

Arg 3 is concerned with transposing the high-level, logical design into a detailed, physical design and implementing it in the physical ATM system.

Arg 4 is concerned with preparing the system (people, equipment and procedures) for bringing it into operational service. It also covers the question as to how the system can be brought into service without adversely the safety of the on-going ATM service during the period of the transition from the current situation to the new situation.

Arg 5 is concerned with monitoring the safety performance achieved by the system during operational service, including investigations and corrective actions in relation to incidents associated with the system.

The above five Arguments are further decomposed and elaborated in Part 2.

4.2 The Safety Lifecycle

4.2.1 Overview

Although it is very much argument-driven, the safety-assessment approach has to end up with a process that is to be followed throughout the project safety lifecycle. This is illustrated at the highest level in Figure 5.

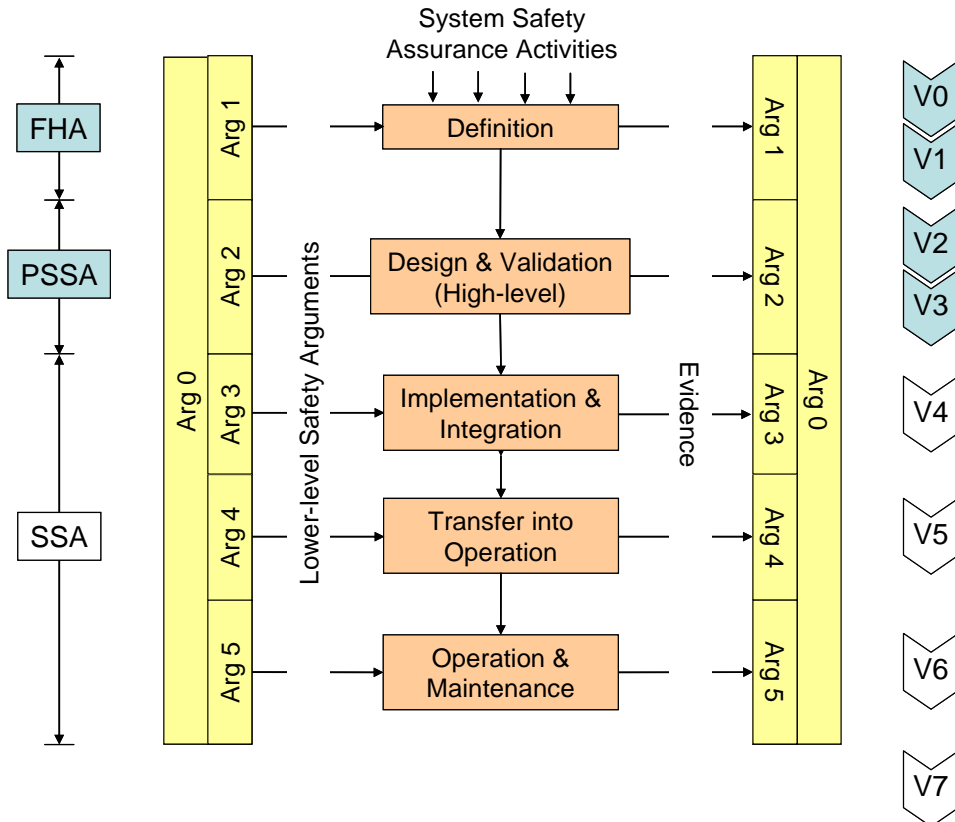


Figure 5 - Overall Safety Lifecycle Process

This diagram is intended to show that:

- each of the five safety-lifecycle stages²⁷ comprises Safety Assurance Activities which are determined by the related Safety Argument²⁸ and
- those Activities produce Evidence that the Argument²⁹ has been satisfied.

²⁷ These are as defined in SAM [5]

²⁸ It is very important thing to understand that the assurance activities in each phase of the lifecycle are determined by the need to satisfy the argument in each case, not the other way around – ie the argument is not limited by the activities

²⁹ The Arguments on the left and right are the same!

Relating this back to some of the issues discussed in section 2.15 above:

- the Safety Plan would include the Argument and the corresponding Activities
- the Safety Case would include the Argument and the Evidence produced by the Activities

For information, the diagram also shows (on the left) how the three stages of safety assessment of the SAM and (on the right) the seven phases of the EUROCONTROL Operational Concept Validation Methodology (E-OCVM) map on to the safety lifecycle³⁰.

It may be noticed that there is no reference to safety assurance objectives as used in SAM. This is because, when safety assurance is put into a safety argument framework, the safety assurance objectives become simply the lowest level of decomposition of the safety argument.

Sub-sections 4.2.3 onwards give a brief description of each phase of the lifecycle – much more detail, including full decomposition of the Safety Argument and a generic set of Assurance Activities, is given in Part 2. Firstly though, section 4.2.2 describes the Safety Considerations process.

4.2.2 Preparation and Initiation

Safety Considerations is a process, recommended in the EUROCONTROL SCDM [6], to identify the main safety issues associated with a project as soon as possible after an Operational Concept has been developed and to help in deciding whether a full Safety Plan and Safety Case are required. Safety Consideration is an expansion of the SAM-FHA Chapter 1 GMA).

It provides an initial assessment of the safety implications of the project, as the basis for developing a Safety Plan in which the detailed safety assurance activities will be specified, as above. It addresses what the project is seeking to achieve (e.g. to deliver benefits in capacity, efficiency and/or safety), the possible impact on safety (in general terms only, since a safety assessment would not have been started at this stage), and the strategy for demonstrating safety.

A key point to be considered is the extent of the change, being introduced by the project, in relation to the hierarchy shown in Figure 3 above. The process described in the rest of this chapter covers the entire hierarchy – ie starts on the basis that a new (or modified) operational concept is being introduced. Where this is not the case, it would be appropriate to adapt the process, and the related safety arguments, according to the scope of the change³¹.

Also, for projects where there are a number of possible options – in terms of,

³⁰ Note however that the scope of the Assurance Activities is much greater than currently described in SAM (or E-OCVM)

³¹ The rationale and justification for this must, however, be explained in the related safety case.

say, the concept and/or design – these should be identified at this stage and a strategy for addressing them developed (at least in outline). This strategy may include defining iterations of the relevant stages of the lifecycle process.

It would often be useful to conduct the first (fact-finding) stage of the HF Case development during this part of the process.

Further details on Safety Considerations can be found in Part 2.

4.2.3 Definition Phase

The Definition Phase addresses how safe the system needs to be, in order to satisfy the Safety Targets. It should provide sufficient evidence to satisfy **Argument 1**, in Section 3, Figure 4 above.

At the core of this phase is the **FHA** process, carried out on a representation of the system under consideration at the level of the ATM service.

Details of the FHA are given in the **SAM** [5]. It is important to note that the current version of SAM (Version 2.1) provides guidance mainly on what Chapter 3 above calls the *failure approach*. Therefore, SAM should be read in conjunction with the following text and **Part 2, Chapter 6** hereto.

The process identifies, in the context of system in its specified operational environment, the pre-existing hazards that are inherent in the operational environment, and those hazards that are associated with potential failures modes of the system itself.

It assesses the consequences of the occurrence of these hazards on the safety of aircraft operations, and results in the specification of Safety Objectives³², which state:

- what the system, at the level of the ATM Service, is required to do, in terms of functionality and performance, in order to reduce (or at least maintain) the level of pre-existing risk (see section 2.8 above)
- the integrity required of the system, at the level of the ATM Service, in order to limit the risk caused by failure of the system
- any additional functionality (or Assumptions, where appropriate) to capture any external means of mitigating the consequences of the hazards caused by failure of the system.

An essential pre-requisite for this process is a clear and complete operational concept document, including a complete description of the operational environment and an agreed set of User³³ Requirements / Safety Targets and a

³² Note that in the context of the broader approach to safety assessment, Safety Objectives are NOT limited to frequency of system failures but include service-level functionality and performance as well.

³³ That is, users of the ATM Service

suitable service-level model of the system.

4.2.4 Design & Validation Phase

4.2.4.1 Overview

The Design & Validation Phase assesses whether the proposed system logical design is able to achieve the level of safety specified in the Definition Phase. It should provide sufficient evidence to satisfy **Argument 2**, in Section 3, Figure 4 above.

At the core of this phase is the **PSSA** process, which is intended to demonstrate that the proposed system logical design can reasonably be expected to deliver the required functionality and performance and achieve the required level of integrity, derived in the FHA.

Details of the PSSA are given in the **SAM** [5]. It is important to note that the current version of SAM (Version 2.1) deals mainly with what Chapter 3 above calls the *failure approach*. Therefore, SAM should be read in conjunction with the following text and **Part 2, Chapter 6** hereto. For the Success approach, SAM-PSSA training material Session 3 “Modelling the intended operation of the system” also provides guidance.

The PSSA is performed before the design and implementation of the physical system has been decided. It considers what the physical system will need to do, but without prejudging how the elements of the physical system should actually implement the required functionality – the latter is the purpose of the SSA, as below.

Therefore, an essential pre-requisite for conducting a PSSA is a description of the intended operation of the system at abstract-functional and logical-architecture levels.

4.2.4.2 Safety Requirements Determination

The process produces a set of Functional Safety Requirements – ie what each element of the design has to do, in terms of functionality and performance, in order to mitigate the pre-existing risks identified in the Definition Phase.

It is essential at this stage to show not only that two-way traceability exists between the FHA ATM service-level specification and the PSSA Functional Safety Requirements but also that the system design, as represented by the logical architecture, would actually work as intended under all expected normal and abnormal conditions.

For simpler and less critical systems, the correct operation of the logical architecture could be demonstrated by a “desk-top” analysis by the appropriate operational and technical experts.

For more complex and/or more critical systems, the demonstration of the correct operation of the logical architecture may require more sophisticated system-engineering methods such as the Structured Analysis & Design Technique (SADT) or Unified Modelling Language (UML) for static analysis of the design and the use of **Fast-time / Real-time Simulations (FTS / RTS)** to assess the dynamic behaviour of the design.

The process then identifies the causes of the system-generated hazards – ie those that are associated with potential failures modes of the system itself – and specifies the Safety Integrity Requirements for each element of the design such that the integrity requirements specified at the ATM Service level, in the FHA, are satisfied.

The main output of the PSSA is as follows:

- Functional Safety Requirements for each element of the logical architecture, as necessary to provide the functionality and performance specified in the FHA
- Safety Integrity Requirements for each element of the logical architecture, as necessary to satisfy the integrity specified in the FHA
- additional Functional Safety Requirements (or Assumptions, where appropriate) to capture any internal means of mitigating the causes of the hazards arising from failure of the system.

4.2.4.3 Safety Requirements Achievability

Since the system architecture can only attain the required level of safety if the architectural elements each meet their Safety Requirements, it is necessary at this stage to show, not only that the Safety Requirements are sufficient to ensure the safety of the overall system but also that these Safety Requirements are achievable!

SAM-PSSA Chapter 3 §3.5 formally request to demonstrate that Safety Requirements are credible. The achievability of Safety Requirements is also covered in the PSSA Verification & Validation process described in the **SAM [5]** (SAM_PSSA Chapter 4). In the particular case of Safety Requirements for human elements it may be necessary also to carry out a **Human Reliability Assessment (HRA)** in order to show that the tasks to be carried out by human operators are reasonable, for the intended application and that the expected maximum (human) error rates for those tasks are realistic.

Further guidance on specific HRA techniques is given in **Part 2, Chapter 6** hereto.

4.2.5 Implementation & Integration Phase

4.2.5.1 Overview

The Implementation & Integration Phase addresses whether the physical system as designed and built achieves the required level of safety. It should provide sufficient evidence to satisfy **Argument 3**, in Section 3, Figure 4 above.

At the core of this phase is a substantial part of the **SSA** process. Unlike FHA and PSSA, which are concerned solely with requirements specification, SSA is mainly a requirements-satisfaction process.

Details of this part of the SSA are given in the **SAM** [5]. It is important to note that, at the system level, the current version of SAM (Version 2.1) provides guidance mainly on what Chapter 3 above calls the *failure approach*. Therefore, SAM should be read in conjunction with the following text and **Part 2, Chapter 7** hereto (when issued).

4.2.5.2 Proving System Functionality and Performance

As indicated in Figure 3, in section 3.4 above, the first stage of SSA is a specification of a detailed set of Safety Requirements for the physical system design. The detailed Functional Safety Requirements are obtained by allocating the Functional Safety Requirements for the logical design (derived in the PSSA, as above) on to the physical architecture.

It is essential at this stage to show not only that two-way traceability exists between the Functional Safety Requirements of the logical and physical system designs but also that the system design, as represented by the physical architecture, actually works under all expected normal and abnormal conditions.

For simpler and less critical systems, the correct operation of the physical architecture could be demonstrated by a “desk-top” analysis by the appropriate operational and technical experts.

For more complex and/or more critical systems, the demonstration of the correct operation of the physical architecture may require more sophisticated methods for static analysis of the design and the use of operational evaluation to assess the dynamic behaviour of the physical design.

This design-analysis activity is then followed by testing at component, subsystem and integrated-system levels, and by operational evaluation of the overall system, in order to confirm (under all expected normal and abnormal operational conditions) that the required functional safety properties of the system, which were proved during the design analysis, are still provided by the system as built.

4.2.5.3 *Proving System Integrity*

The final part of the Implementation & Integration phase is to:

- derive a set of detailed Safety Integrity Requirements for the physical architecture
- show that these detailed Safety Integrity Requirements satisfy those specified in the PSSA for the logical architecture
- show that no, new undesired properties of the system have emerged in the physical design and/or system as built.

It is at this stage that the system implementer often encounters a major problem – ie the limited ability of, inter alia, test-based validation & verification to show, with sufficient confidence, that the required safety integrity properties of the system have actually been satisfied in practice.

It is to address this problem that the SAM Task Force has been developing an assurance-based approach as a pragmatic (though somewhat indirect) means of demonstrating the satisfaction of Safety Integrity Requirements (and in some cases, Functional Safety Requirements) in the main elements of the physical system – software, procedures and humans.³⁴

This approach is based on the assignment of **assurance levels** (ALs), determined by the safety-criticality of the system element concerned, and which themselves determine the related assurance process in the form of objectives, activities and evidence requirements.

It is very important to note that ALs do not replace Safety Requirements; rather, they set the level of assurance at which satisfaction of Safety Requirements has to be demonstrated.

Currently the **SAM** [5] specifies assurance levels and processes for software (**SWAL**), and maintenance interventions and procedures (**PAL**).

A similar process for human elements of the system (**HAL**) is under development. For HW, the aviation industry approach is recommended when needed (Cf: ED-80).

4.2.6 Transfer into Operation

The Transfer into Operation Phase addresses whether the fully proven system is ready to be brought into operational use, and without affect the continuity and safety of the on-going ATM service. It should provide sufficient evidence to satisfy **Argument 4**, in Section 3, Figure 4 above.

³⁴ Assurance levels also have a part to play in proving the functionality and performance of this system – this is addressed in Chapters 5 and 6 below.

At the core of this phase is the second part of the **SSA** process, details of which are given in the **SAM** [5]. It is important to note that the current version of SAM (Version 2.1) provides guidance mainly on what Chapter 3 above calls the *failure approach*. Therefore, SAM should be read in conjunction with the following text and **Part 2, Chapter 8** hereto (when issued).

Evidence needs to be produced to show that, inter alia:

- All preparations for bring the individual systems / subsystems in to service, and for supporting them in service, have been completed. These preparations should include such things as publication of operational procedures, airspace changes (if any), publication of engineering procedures, provision of resources (people, equipment spares, maintenance facilities etc) and training of operational and technical personnel. They should also include arrangements for safety management, change management, configuration control etc.
- The process of switching over from the old systems to the new systems has been fully planned and resourced. This should include switchover procedures, allocation of responsibilities and the training / briefing of all personnel involved.
- All hazards associated with switch-over from the old systems to the new systems have been assessed and mitigated sufficiently. This assessment should include a sort of FHA/PSSA/SSA of the switchover and should result in the additional procedures, allocation of responsibilities and training / briefing of personnel necessary to prevent (as far as possible) things going wrong, and to take the appropriate action should something go wrong

4.2.7 Operation & Maintenance Phase

The Operation & Maintenance Phase provides monitoring of the safety performance of the system during its operational lifetime, and provides evidence that the physical system in practice achieves an acceptable (or at least a tolerable) level of risk, as captured in the Safety Requirements. It should provide sufficient evidence to satisfy **Argument 5**, in Section 3, Figure 4 above.

At the core of this phase is the third part of the **SSA** process, details of which are given in the **SAM** [5]. It is important to note that the current version of SAM (Version 2.1) provides guidance mainly on what Chapter 3 above calls the *failure approach*. Therefore, SAM should be read in conjunction with the following text and **Part 2, Chapter 9** hereto (when issued).

Evidence needs to be provided to show that, inter alia:

- the Safety Targets are met in practice. This is a very important cross-check of the results of the *a priori* safety assessments (FHA, PSSA,

and SSA) all of which are necessarily based on predictive analysis techniques

- all safety-related incidents are reported, investigated and the appropriate corrective action taken. This is a very important contribution to the achievement of “AFARP” type Safety Target – see section 2.2 above
- safety assessments are carried out of any maintenance and/or other planned interventions, to ensure that risks induced by any maintenance and/or planned intervention are known and are acceptable.

4.3 Conclusions

This Chapter has provided an outline of a typical safety lifecycle. It has emphasized the importance of providing sufficient safety **assurance** throughout the lifecycle that the system under consideration has been properly specified and then implemented in accordance with that specification.

Part 2 explains in much more detail how the assurance approach is applied in the five stages of the safety lifecycle.

Page intentionally left blank

Annex 1 - References

- [1] EUROCONTROL, 2001, *ESARR 4 - Risk Assessment and Mitigation in ATM*, Ed 1.0
 - [2] EUROCONTROL, 1999, *Air Traffic Management Strategy for 2000+*
 - [3] EUROCONTROL, 2000, *ESARR 3 - Use of Safety Management Systems by ATM Service Providers*, Ed 1.0
 - [4] EUROCONTROL, 2000, *ESARR 2 - Reporting and Assessment of Safety Occurrences in ATM*, Ed 2.0
 - [5] EUROCONTROL, 2006, *Air Navigation System Safety Assessment Methodology (SAM)*, SAF.ET1.ST03.1000-MAN-01, Edition 2.1
 - [6] EUROCONTROL, 2006, *SAM Part IV Annex I - Safety Case Development Manual*, Edition 2.2,
 - [7] HMSO Publications Centre, *The Public Inquiry into the Piper Alpha Disaster*, Volumes 1 & 2, November 1990, ISBN 0-10-113102-X
 - [8] SESAR Consortium, the ATM Deployment Sequence, D4, DLM-0706-001-02-00, January 2008
 - [9] EUROCONTROL, 2007, *Human Factors Case*, Edition 2.0, dated 29.06.2007, reference 07/06/22-35
 - [10] EUROCAE ED-125, *Process for Deriving Risk Classification Scheme and Specifying Safety Objectives in ATM "in compliance" with ESARR 4*, proposed V1.0, Nov 2007.
 - [11] EUROCONTROL *Airspace Planning Manual, Section 5, Terminal Airspace Design Guidelines*, Ed 2.0, Amendment 1, 17 Jan 05
 - [12] SRC EAM 4 / GUI 1, *Explanatory Material on ESARR 4 Requirements*, version 2.0, 1 Mar 05
-

Annex 2 - Glossary

ADS-B	Automatic Dependent Surveillance - Broadcast
AFARP	As Far as Reasonably Practicable
AL	Assurance Level
FHA	Functional Hazard Assessment
FSR	Functional Safety Requirement
FTS	Fast-time Simulation
GSN	Goal-structuring Notation
HAL	Human Assurance Level
HF	Human Factors
HFIA	Human Factors Issue Analysis
HRA	Human Reliability Assessment
IRP	Integrated Risk Picture
NRA	Non-Radar Area
PAL	Procedure Assurance Level
PSC	Preliminary Safety Case
PSSA	Preliminary System Safety Assessment
RCS	Risk Classification Scheme
RTS	Real-Time Simulation
SAM	Safety Assessment Methodology
SCDM	Safety Case Development Manual
SESAR	Single European Sky ATM Research programme
SIR	Safety Integrity Requirement
SMS	Safety Management System
SSA	System Safety Assessment
SWAL	SoftWare Assurance Level
TLS	Target Level of Safety

UML Unified Modelling Language

USC Unit Safety Case