



The European Organisation for Civil Aviation Equipment
L'Organisation Européenne pour l'Équipement de l'Aviation Civile

PROCESS FOR SPECIFYING RISK CLASSIFICATION SCHEME AND DERIVING SAFETY OBJECTIVES IN ATM

This document is the exclusive intellectual and commercial property of EUROCAE.

It is presently commercialised by EUROCAE.

This electronic copy is delivered to your company/organisation **for internal use exclusively**.

In no case it must be re-sold, or hired, lent or exchanged outside your company.

ED-125

March 2010

102 rue Etienne Dolet
92240 MALAKOFF, France
Web Site: www.eurocae.net

Tel: 33 1 40 92 79 30
Fax: 33 1 40 92 79 30
Email: info@eurocae.net
Documents
Document Sharing Hub

PROCESS FOR SPECIFYING RISK CLASSIFICATION SCHEME AND DERIVING SAFETY OBJECTIVES IN ATM

This document is the exclusive intellectual and commercial property of EUROCAE.

It is presently commercialised by EUROCAE.

This electronic copy is delivered to your company/organisation **for internal use exclusively**.

In no case it must be re-sold, or hired, lent or exchanged outside your company.

ED-125

March 2010

FOREWORD

1. The development of these guidelines was accomplished by the European Organization for Civil Aviation Equipment (EUROCAE) WG-64. It is well understood that related regulatory requirements are intended to be modified in the future (e.g. EASA's new role in and responsibilities for ATM, ...). This environment together with co-existing related initiatives (e.g. Mandate for a quantitative Risk Classification Scheme to complement SES 2096/2004 Common Requirements, SES II Performance Framework, ...) caused different views what should be covered by the final document. However, the work was progressed aiming at satisfying existing regulatory requirements with a useful document. Under these conditions ultimate consensus was not achieved, leading to a consultation cycle satisfying not all but the majority of contributions. Full details of the comments received during the consultation process can be obtained from the EUROCAE secretariat.

Noting that the document is helpful as it is being used and referenced, it was accepted by the Council of EUROCAE on March 2010.

2. EUROCAE is an international non-profit making organisation. Membership is open to European users and manufacturers of equipment for aeronautics, trade associations, national civil aviation administrations and, under certain conditions, non-European organisations. Its work programme is principally directed to the preparation of performance specifications and guidance documents for civil aviation equipment, for adoption and use at European and world-wide levels.
3. EUROCAE performance specifications are recommendations only. EUROCAE is not an official body of the European Governments; its recommendations are valid as statements of official policy only when adopted by a particular government or conference of governments.
4. Copies of this document may be obtained from:

EUROCAE
102 rue Etienne Dolet
92240 MALAKOFF
France

Tel: 33 1 40 92 79 30

Fax: 33 1 46 55 62 65

Email: eurocae@eurocae.net

Web Site: www.eurocae.net

TABLE OF CONTENTS

FOREWORD	I
CHAPTER 1 INTRODUCTION	1
1.1 Purpose	1
1.2 Scope	1
1.3 Target audience.....	2
1.4 Document description.....	2
1.4.1 Mandating and recommending phrases.....	2
1.4.2 Document organization	2
1.4.3 How to use this document.....	2
1.4.4 When to use this document	3
1.4.5 Acronyms	3
1.4.6 Glossary of Terms	4
1.5 Mathematical nomenclature	6
1.6 Relationships to other documents	7
1.6.1 ESARR.....	7
1.6.2 EUROCONTROL Safety Assessment Methodology	7
CHAPTER 2 RISK CLASSIFICATION SCHEME (RCS)	8
2.1 Introduction	8
2.2 What are Severity Classes?	8
2.3 What are Safety Targets?	9
2.4 Approach	9
2.5 Ambition Factor (AF)	11
2.6 Conversion into “per year”	11
2.7 Examples.....	12
2.8 Advantages and limitations of ATMSP RCS	12
CHAPTER 3 SAFETY OBJECTIVES	14
3.1 Introduction.....	14
3.2 Approach to derive Safety Objectives	15
3.2.1 Safety Objectives in an operational environment	15
3.2.2 How to use Safety Objectives	15
3.2.3 Assumptions.....	15
3.3 Safety Objective units.....	15
CHAPTER 4 INTRODUCTION TO THE MODELS.....	16
4.1 Overall applicability.....	16
4.2 Models description summary.....	16
4.3 Selection and application of model.....	17
4.4 Airspace complexity.....	17
4.4.1 APP and ACC complexity	18
4.4.2 Airport Complexity.....	18
4.5 Number of hazards	19
4.6 “Pe”	21

CHAPTER 5	MODELS DESCRIPTION	24
5.1	Quantitative Model – Model 1	24
5.1.1	Process description	24
5.1.2	Advantages of using this method	26
5.1.3	Limitations of this method	27
5.1.4	Example	27
5.2	Semi-Quantitative Model – Model 2	29
5.2.1	Process description	29
5.2.2	Advantages of this method	31
5.2.3	Limitations of this method	31
5.2.4	Example	31
5.3	Semi-Prescriptive Model – Model 3	32
5.3.1	Process Description	32
5.3.2	Advantages of this method	38
5.3.3	Limitations of this method	38
5.3.4	Example	39
5.4	Fixed-Prescriptive Model – Model 4	40
5.4.1	Process Description	40
5.4.2	Advantages of this method	45
5.4.3	Limitations of this method	45
5.4.4	Example	46
APPENDIX A	THEORETICAL MODEL	47
APPENDIX B	RATIONALE FOR SUSTAINING VARIOUS QUANTITATIVE VALUES	59
B.1	Safety Targets	59
B.2	Ambition Factor	60
B.3	Number of hazards	60
B.4	Peij	61
B.5	Safety Objective	61
B.6	Comparison with some other related material in aviation	62
B.6.1	EASA CS 25-1309	62
APPENDIX C	COMMITTEE MEMBERSHIP	63
APPENDIX D	HISTORY AND TERMS OF REFERENCE OF WG-64	64
D.1	Introduction	64
D.2	Terms of Reference	64
D.3	Relationship of WG-64 Document to Terms of Reference	65
APPENDIX E	IMPROVEMENT SUGGESTION FORM	66

LIST OF TABLES

Table 1: Specification of National Regulatory RCS.....	10
Table 2: Specification of ATMSP RCS	10
Table 3: Example of Safety Targets for various fh/y	12
Table 4: Example of ATMSP RCS	27
Table 5: Assumptions – Hazard distribution for ACC	34
Table 6: Assumptions – Hazard distribution for APP	35
Table 7: Assumptions – Hazard distribution for AD	36
Table 8: Example - Complexity and Traffic per ATSU	39
Table 9: Example - RCS (Safety Targets) for each ATSU	39
Table 10: Model 3 Example - SOCS for each ATSU.	40
Table 11: ACC SOCS (/fh)	41
Table 12: APP SOCS (/fh).....	41
Table 13: AD SOCS (/fh).....	42
Table 14: Assumptions – Hazard distribution and $Pe_{i,j}$ values for ACC	43
Table 15: Assumptions – Hazard distribution and $Pe_{i,j}$ values for APP	43
Table 16: Assumptions – Hazard distribution and $Pe_{i,j}$ values for AD	44
Table 17: Model 4 Example - SOCS for each ATSU.	46

LIST OF FIGURES

Figure 1: Safety Objective	14
Figure 2: Pe	22
Figure 3: Quantitative Model Process Description	24
Figure 4: Hazard, Severity, Cause and Consequence	26
Figure 5: Model 1 Example Hazard Safety Objective	28
Figure 6: Semi-Quantitative Model Process Description.....	29
Figure 7: Semi-Prescriptive Model Process Description	32
Figure 8: Fixed-Prescriptive Model Process Description	40
Figure 9: Cause/Hazard/Effect model	47
Figure 10: Many hazards and their effects (1 st view)	49
Figure 11: Many hazards and their effects (2 nd view).....	50
Figure 12: Simplification-1: Separate all effects and relate to an individual hazard.....	51
Figure 13: Alternative: Regroup per effect whatever the hazard.....	53
Figure 14: Simplification-2: Regroup the effects per Severity Class	54
Figure 15: Simplification-3: Evenly distribution of the Safety Targets ST_i	56
Figure 16: Simplification-3: other representation	57
Figure 17: Simplification-4: Consider the Worst Credible effect.....	58

REFERENCES

1. ESARR 4 "Risk assessment and mitigation in ATM, V1.0, 05/04/2001
2. EUROCONTROL Safety Assessment Methodology (SAM) V2.
3. Performance Review Reports (including ACE (ATM Cost Effectiveness) benchmarking report 2002 & 2004)
4. SRC DOC 12 V2.0 (date: 26/10/2009) "Assessment of EATM Air Navigation System Safety Assessment Methodology as means of compliance with ESARR 4"
5. EASA CS25-1309 "Certification Specifications for Large Aeroplanes"

CHAPTER 1

INTRODUCTION

Risk assessment and mitigation in Air Traffic Management (ATM) has to be performed by applying a process throughout the lifecycle of the procedures, people and equipment that form the ATM system.

When performing risk assessment and mitigation in ATM, the emphasis has to be placed on the process (namely hazard identification, effects identification and mitigation means identification). However, quantification ensures that clear, unambiguous and agreed levels of safety risks can be specified and that demonstration of their satisfaction can be made with an appropriate level of confidence that these levels of safety risks can be achieved when actually delivering an ATM service.

1.1

PURPOSE

- This document provides guidelines for the specification of a Risk Classification Scheme (RCS) within the framework of EUROCONTROL Safety Regulatory Requirements ESARR 4 “Risk Assessment and Mitigation in ATM” (Ref[1]).
- This document may be used in supporting National Regulators and ATM Service Providers (ATMSP) to specify a common and harmonized Risk Classification Scheme and to derive quantitative Safety Objectives tailored to the ATM service provision in their operational environment in order to drive their ATM system design.
- This document does not provide guidelines on how the risks associated with hazards at the ATM Service Provision can be systematically and formally identified, assessed, and managed within safety levels. A reference to SAM [Ref 2] is provided for ED-125 users not knowing how to perform some steps of the risk assessment process in compliance with ESARR 4. (Statement of Compliance of SAM with ESARR 4 can be found in SRC DOC 12 V2.0 [Ref 4]). However, ED-125 users have the freedom to use any other guidance material to perform these steps while ensuring that this alternative guidance material complies with ESARR 4.

1.2

SCOPE

- This document applies when specifying a Risk Classification Scheme (RCS) and deriving Safety Objectives for hazards at the ATM Service Provision level:
 - o This document covers the ATM System (airborne and ground (including spatial) components) as well as its environment of operations. It also includes the interaction between system elements as well as interactions between the system under assessment and other systems;
 - o This document does not address the assessment of introducing and/or planning organisational or management changes to the ATM service provision.
- This document provides quantitative Safety Objectives for hazards at the ATM Service Provision level of an Air Traffic Service Unit (ATSU) only. This document provides typical guidelines that can be used when quantifying Safety Objectives in the framework of a UFHA (Unit Functional Hazard Assessment).
- This document does not provide guidelines for quantifying Safety Objectives for a reduced scope (only a part of an ATM Service Provision).

1.3 TARGET AUDIENCE

This document provides guidance to:

- o National Regulators - in setting their Risk Classification Scheme (RCS);
- o ATMSP - in setting their Risk Classification Scheme and in specifying quantitative Safety Objectives for hazards at the ATM Service Provision level.

1.4 DOCUMENT DESCRIPTION

1.4.1 Mandating and recommending phrases

This document uses the words “shall,” and “should” as follows:

- **“shall”** indicates a mandated criterion; i.e., in order to claim compliance with this document (ED-125) all the “shall” criteria have to be satisfied. However, the word “shall” as used in this document must **not** be interpreted as “regulatory requirement” as this document provides only guidance;
- **“should”** indicates that although the criterion is regarded as the preferred option, alternative criteria may be applied without impairing a claim for compliance with this document. In such cases, it is the responsibility of the user to ensure that the alternatives means comply with ESARR 4 as appropriate.

1.4.2 Document organization

- Section 1 provides an introduction.
- Section 2 provides recommendations for a Risk Classification Scheme (RCS)
- Section 3 provides recommendations for Safety Objectives
- Section 4 provides an introduction to the proposed models
- Section 5 provides the description of the proposed models
- Appendix A provides guidance for theoretical calculation of Safety Objectives.
- Appendix B provides rationale for sustaining the choice of quantitative values.
- Appendix C provides a list of participants who contributed to the development of this document.
- Appendix D provides a history and how this document satisfies the terms of reference for WG-64.
- Appendix E provides an improvement suggestion form.

1.4.3 How to use this document

ED-125 provides guidance for the specification of a Risk Classification Scheme (RCS) and the derivation of quantitative Safety Objectives for hazards at the ATM Service Provision level within the framework of a hazard identification and assessment process. Such a process has to be applied in order to identify hazards, their effects and the severity of these effects in accordance with ESARR 4.

The EUROCONTROL Safety Assessment Methodology (SAM) Functional Hazard Assessment (FHA) process is proposed as a reference that has been assessed as a means of compliance with ESARR 4. However, ED-125 users have the freedom to use any other guidance material to perform this step while ensuring that this alternative guidance material complies with ESARR 4.

The method of application of ED-125 for National Regulators is:

1. National Regulators **shall** use the ECAC RCS as provided in §2 (See Table 1).
2. National Regulators **shall** develop from the ECAC RCS their own National Regulator RCS (See §2 - Table 1).

The method of application of ED-125 for ATMSPs is:

1. ATMSPs **shall** use the National Regulator RCS (see Table 1),
2. ATMSPs **should** transform the National Regulator RCS into per operational-time (e.g. year, hour, ...) (see §2.5) of the organisation.
3. ATMSPs **should** develop from it (step2) their own ATMSP RCS (see §2.5).
4. ATMSPs **should** select an appropriate model for deriving Safety Objectives at the ATM Service Provision level (see Chapter 4.2).
5. Once a model for deriving Safety Objectives at the ATM Service Provision level is selected, ATMSPs **should** set the criteria as needed by the model and should apply the model as described in this document (see Chapter 5).

1.4.4 When to use this document

This document applies when National Regulators or ATMSP want to set their Risk Classification Scheme (RCS).

This document also applies when an ATMSP wants to specify Safety Objectives for hazards at the ATM Service Provision level (e.g. UFHA: Unit FHA at the ATSU level).

Note: The ATM Service Provision level refers to a level of functionality at the interface between the ATM Service and the service end-users (e.g. airspace users). It does not refer to system that operates at a level below that interface (e.g. a project to change or redesign a radar site would not use this document to set Safety Objectives. In this case, the project would have to derive Safety Requirements from Safety Objectives that have been specified at the ATM Service Provision level).

1.4.5 Acronyms

ACC	Air Control Centre
AD	Aerodrome
AF	Ambition Factor
AIS	Aeronautical Information Service
AMC	Acceptable Means of Compliance
APP	APProach
ASM	AirSpace Management
ATFCM	Air Traffic Flow & Capacity Management
ATMSP	Air Traffic Management Service Provider
ATSU	Air Traffic Service Unit
ESARR	EUROCONTROL Safety Regulatory Requirement
ETA	Event Tree Analysis
FHA	Functional Hazard Assessment (Part of SAM Ref [2])
FTA	Fault Tree Analysis
GM	Guidance Material
MET	Meteorological Data
NSA	National Supervisory Authority

PSSA	Preliminary System Safety Assessment (Part of SAM Ref [2])
RCS	Risk Classification Scheme
SAM	Safety Assessment Methodology
SO	Safety Objective
SOCS	Safety Objective Classification Scheme
SRC	Safety Regulation Commission
SSA	System Safety Assessment (Part of SAM Ref [2])
ST	Safety Target
UFHA	Unit Functional Hazard Assessment

1.4.6

Glossary of Terms

Term	Definition
Acceptable risk	Acceptable risk defines the target risk for an ATMSP as defined in their Risk Classification Scheme (RCS). Acceptable risk is more demanding than tolerable risk.
Ambition Factor	An Ambition Factor (AF) is a number greater or equal to one that is used by ATMSPs when setting their acceptable Safety Targets by dividing the tolerable Safety Targets set by the National Regulator (NR) by this AF. ($ST_{ATMSP} = ST_{NR} / AF$) (See §2.5)
ATSU	Air Traffic Service Unit (ATSU) A generic term meaning variously: - an air traffic control unit (En-Route (ACC), Approach (APP), Airport (AD)); - a flight information centre or; - an air traffic services reporting office. An ATSU provides Air Traffic Management Service including ASM (AirSpace Management) and ATFM (Air Traffic Flow Management) for which it needs AIS and MET data.
Hazard	ESARR4: Any condition, event or circumstance that can induce an accident. ED-125: Any condition, event or circumstance <u>happening at the ATM Service Provision level</u> that can induce <u>an incident or an accident</u> . Note: This differs from ESARR4 because: - In the framework of this document, hazards are defined only at the ATM Service Provision level; - A hazard may induce incident as well as accident.
National Regulator	In this document no distinction is introduced between the various roles and responsibilities of the Member States: National Regulator (rule maker) or National Supervisory Authority (oversight). Therefore both terms are equally used to encompass both roles and responsibilities with regards RCS. It is the responsibility of appropriate national bodies to split roles as required and as necessary.

Term	Definition
$Pe_{i,j}$	The probability that once a hazard H_i has occurred, it generates an effect of a given Severity Class j SC_j. (See §4.6) In this definition, the word “effect” has to be understood as the class of all effects E_j (see Appendix A Theoretical Model) having the same Severity Class (e.g. Controlled Flight Into Terrain, Mid-Air collision, Ground collision belong to the same cluster or class of effect: Severity Class 1 (SC_1) effect).
Risk	The combination of: - the overall probability or frequency of occurrence of a harmful effect induced by a <i>hazard</i> and, - the <i>Severity</i> of that effect. Note: in the framework of this document, only “frequency” is used.
Safety Objective	ESARR4: Qualitative or quantitative statement that defines the maximum frequency or probability at which a hazard can be expected to occur. EC Regulation 2096/2005: Qualitative or quantitative statement that defines the maximum frequency or probability at which a hazard can be expected to occur. ED-125: <u>Quantitative</u> statement that defines the maximum <u>frequency</u> at which a hazard can be <u>accepted</u> to occur. Note: This differs from ESARR4 because: - In the framework of this document, only “frequency” is used; - Guidance is provided only for “quantitative” SO; - An acceptable level risk has to be achieved as this document aims at setting SO for ATM Service Providers.
Safety Objective Classification Scheme	A matrix proposing Safety Objectives for hazards in accordance with the Severity Class of their Worst Credible effect.
Safety Target	(ST_j) specifies the overall maximum frequency of occurrence of effects of any type having a given Severity Class j (SC_j) whatever the ATM cause.
Severity	Level of effect/consequences of <i>hazards</i> on the safety of flight operations i.e., combining level of : - loss of separation and - degree of ability to recover from the hazardous situation.
Severity Class	Gradation, ranging from 1 (most severe) to 5 (least severe), as an expression of the magnitude of the effects of <i>hazards</i> on flight operations.

Term	Definition
System	ESARR4: A combination of physical components, procedures and human resources organised to perform a function. ED-125: A combination of the three constituent elements: • human, • rules & procedures and • physical equipment (hardware and software) within an operational environment, organised to perform a function/service/application. Note: This differs from ESARR4 as it clarifies the definition within the context of this document.
Tolerable risk	Tolerable risk defines the target risk for a National Regulator as defined in their Risk Classification Scheme (RCS).
UFHA	Unit Functional Hazard Assessment: Functional Hazard Assessment (See SAM Ref [2]) at the level of the overall Service Provision of a specific ATSU.
Worst Credible Effect	‘Worst’ means the most unfavourable conditions – e.g. extremely high levels of traffic or extreme weather disruption. ‘Credible’ implies that it is not unreasonable to expect to experience this combination of extreme conditions within the operational lifetime of the system so that such scenario leading to generate such an effect has to be considered. The Worst Credible Effect aims at identifying the highest contribution of a hazard to the highest risk due to this hazard. See Ref [2] SAM FHA Chapter 3 GM D & G. It is a simplified approach to identify the Safety Objective of a hazard. (See Appendix A Theoretical Model)

1.5

MATHEMATICAL NOMENCLATURE

A number of mathematical formulae are presented in this document. Given below is a summary of the nomenclature adopted in these formulae.

H_i	Hazard number i
N_{ATM}	Total number of hazards at the ATM Service Provision
SC_j	Severity Class j
N_{ATMj}	Total number of ATM hazards having a Worst Credible Effect of Severity Class j (SC_j).
N_j	Number of hazards “significantly” contributing to the satisfaction of a Safety Target ST_j .
$Pe_{i,j}$	See Glossary of Terms. $Pe_{i,j}$ will always be equal to or less than one.
SO_i	Safety Objective related to a Hazard i H_i
ST_j	Safety Target j related to a Severity Class j (SC_j)
ATSUC $_x$	ATSU (ACC, AD, APP) of complexity x ($x = 1, 2, 3$ or 4)
fh	Flight Hour
y	Year
V_{2004}	Volume of traffic in 2004 (number of fh / y)

1.6 RELATIONSHIPS TO OTHER DOCUMENTS

1.6.1 ESARR

ESARR 4: “Risk Assessment and Mitigation in ATM” (Edition V1.0, 05/04/2001)

This document has been prepared by the Safety Regulation Commission.

This requirement concerns the use of Risk Assessment and Mitigation, including hazard identification, in Air Traffic Management when introducing and/or planning changes to the ATM System. In this requirement, Risk Assessment and Mitigation are being addressed, adopting a total aviation system approach.

This requirement shall apply to all providers of ATM services in respect of those parts of the ATM System for which they have managerial control.

SRC DOC 12: “Assessment of ANS Air Navigation System Safety Assessment Methodology as a Means of Compliance with ESARR 4”

SRC DOC 12 V2.0 [Ref. 4] has been prepared by the Safety Regulation Commission. It has been developed, validated and completed by the SRC-AMC (Safety Regulation Commission – Acceptable Means of Compliance) Panel in charge of assessing to which extent the ANS Air Navigation Safety Assessment Methodology, (SAF.ET.ST03.1000-MAN-01-00) Edition 2.0., complies with ESARR 4 “Risk Assessment and Mitigation in ATM” Ed. 1.0.

1.6.2 EUROCONTROL Safety Assessment Methodology

The EUROCONTROL Air Navigation System Safety Assessment Methodology V2 (SAM) is considered as the companion document to this ED-125 document as it provides recommendations to be completed with ED-125 for quantification aspects. Therefore, ED-125 provides only additional material to the SAM and no part of ED-125 neither contradicts nor supersedes SAM.

ED-125 document is referenced in SAM as SAM-FHA Chapter 3 GM E.

The EATM Safety Assessment Methodology (SAM) provides guidance for the safety assessment of Air Navigation Systems.

A reference to SAM [Ref 2] is provided for ED-125 users not knowing how to perform some steps of the risk assessment process in compliance with ESARR 4 (Statement of Compliance of SAM with ESARR 4 can be found in SRC DOC 12 V2.0 [Ref 4]).

However, ED-125 users have the freedom to use any other guidance material to perform these steps while ensuring that this alternative guidance material complies with ESARR 4.

CHAPTER 2

RISK CLASSIFICATION SCHEME (RCS)

2.1 INTRODUCTION

Quantitative levels can be defined to compare the in-service risk of the ATMSP or to specify the overall goal of an organisation as far as safety of new systems or changes to existing systems is concerned.

An ATMSP may define two separate quantitative levels:

1. In service monitoring (Target Level of Safety or Safety Minima)
2. Introduction of new systems or changes to existing systems (Design Safety Target)

In this document, the RCS only applies to point 2 above: introduction of new systems or changes to existing systems.

2.2 WHAT ARE SEVERITY CLASSES?

ESARR 4 requires that the *effects* of identified hazards be classified in accordance with a Severity Classification scheme. The ATMSP **shall** therefore adopt a Severity Classification Scheme which aligns with ESARR4 (e.g. SAM FHA Chapter 3 GM D). The Severity Classification Scheme in ESARR4 comprises:

- Severity Class 1: Accidents
- Severity Class 2: Serious Incidents
- Severity Class 3: Major Incidents
- Severity Class 4: Significant Incidents
- Severity Class 5: No Immediate Effect on Safety

ESARR 4 also provides a maximum tolerable frequency of occurrence within Air Traffic Management (ATM) directly contributing to a Severity Class 1 (SC₁) effect (i.e. 'accidents'). The overall absolute tolerable frequency for the ECAC area for SC₁ effects has been set at a level commensurate with present overall safety performance and the goal is to keep this overall absolute level of safety performance the same (or better) over future years despite changes to the ATM system and changes in traffic levels.

ESARR 4 does not provide a maximum tolerable frequency for effects which are Severity Class 2 (SC₂), Severity Class 3 (SC₃), Severity Class 4 (SC₄) or Severity Class 5 (SC₅). Therefore, in the absence of such information, an estimate has been made of the average tolerable frequencies of events having each of the remaining severity classes. This distribution is assumed to apply for all airspace types. The recommendation is to set the maximum tolerable (for National Regulator) and acceptable (for ATMSP) limits for each Severity Class as indicated in Table 1.

For Severity Class 1 (SC₁), the Safety Targets set in Table 1 are derived from the ESARR 4 Safety Target which represents an average across the ECAC area. In reality, it is possible that an individual regulator may wish to apply more stringent Safety Targets in their airspace.

If many ATMSPs within the same State have to comply with the National Regulator RCS, then each ATMSP needs to inject its own traffic levels to specify its own RCS (See §2.6).

2.3 WHAT ARE SAFETY TARGETS?

An RCS aims at setting the maximum contribution of an ATM organisation to accidents and incidents.

In the framework of ESARR 4, the RCS consists of a table made of 5 Safety Targets (1 Safety Target per Severity Class):

- ST_1 : Safety Target for Severity Class 1 (SC_1) effects (Accidents)
- ST_2 : Safety Target for Severity Class 2 (SC_2) effects (Serious Incidents)
- ST_3 : Safety Target for Severity Class 3 (SC_3) effects (Major Incidents)
- ST_4 : Safety Target for Severity Class 4 (SC_4) effects (Significant Incidents)
- ST_5 : Safety Target for Severity Class 5 (SC_5) effects (No immediate effect on safety)

A Safety Target (ST_i) specifies the overall maximum frequency of occurrence of effects of any type having a given Severity Class x (SC_x) whatever the ATM cause (Cf Appendix A Theoretical Model).

For example ST_1 specifies the overall maximum frequency of accidents (SC_1) whatever the kind of accident (e.g. mid-air collision, Controlled Flight Into Terrain (CFIT), Aircraft collision on the ground, Collision between an aircraft and a vehicle, etc.)

2.4 APPROACH

To set the RCS, the approach chosen is to identify three levels of RCS:

1. ECAC regulatory RCS;
2. National regulatory RCS;
3. ATMSP RCS.

These three levels match three different roles:

- ECAC regulatory (SRC Safety Regulation Commission): is regulating (at pan-European level) the minimum protection of the public against risk of ATM contributing to aviation accidents and incidents (Pan-European tolerable level);
- National regulatory RCS: is regulating (at national level) the minimum protection of the public against risk of ATM contributing to aviation accidents and incidents (National tolerable level);
- ATMSP RCS: In addition to meeting the National regulatory RCS, the aim of the ATMSP is to strive to improve safety and to protect the organisation and its staff against the risk of the ATMSP contributing to aviation accidents and incidents (acceptable level). The ATMSP RCS contributes to protecting the organisation by stating what is an “acceptably safe design”.

The National Regulatory RCS **shall** be specified as follows:

Safety Target	ECAC Regulator Safety Target	National Regulator Safety Target	
	(/ flight hour)	Minimum National Regulator AF	Max Safety Target (/ flight hour)
ST₁	1.55E-08	1.55*	1E-08
ST₂	1E-05	1	1E-05
ST₃	1E-04	1	1E-04
ST₄	1E-02	1	1E-02
ST₅	n/a	n/a	n/a

TABLE 1: SPECIFICATION OF NATIONAL REGULATORY RCS

*: when considering the ECAC Regulator ST1 = 1.55E-08/fh as per ESARR4 V1.0. This AF = 1.55 aims at deleting the fractional part (.55) of ST1 as per ESARR4.

The ATMSP RCS **should** be specified as follows:

Safety Target	ATMSP Safety Target	
	ATMSP AF	Max Safety Target (/ flight hour)
ST₁	10	1E-09
ST₂	10	1E-06
ST₃	10	1E-05
ST₄	10	1E-03
ST₅	n/a	n/a

TABLE 2: SPECIFICATION OF ATMSP RCS

Table 1 and Table 2 explanatory notes:

1. ECAC Regulator Safety Target for Severity Class 1 is taken from ESARR4;
2. Safety Targets for Severity Class 2, 3 and 4 are set by ED-125 through consideration of data and expert judgment (see Appendix B);
3. National Regulator Safety Target = ECAC Safety Target / National AF;
4. ATMSP Safety Target = National Regulator Safety Target / ATMSP AF;
5. ST₅ is not provided in this document as this Target is not safety related (Severity Class 5: “no immediate effect on safety”);
6. Different AFs may be applied to different Severity Classes by National Regulators or ATMSP as required as long as these AFs comply with the minimum values as specified in §2.5, Table 2.

7. This document assumes that National Regulators publish their National RCS in accordance with this document. If National Regulators have already published or will publish National RCS diverting from this document, then ATMSP have to check if their RCS complies with the published National Regulator RCS. This can be an issue only if the National Regulator publishes Safety Targets being more demanding than the ATMSP RCS as recommended in this document. In such case the ATMSP **shall** use the National Regulator Safety Target(s) being more demanding (e.g. $ST_2 = 1E-7/fh$) as input to set its own ATMSP RCS and decide the Ambition Factor for this (ese) specific Safety Target(s) (e.g. $AF = 1$ for ST_2).

2.5 AMBITION FACTOR (AF)

The National Regulatory minimum AF values **shall** be in accordance with Table 1.

The ATMSP has to introduce its own Ambition Factors (AFs).

The minimum ATMSP AF values **should** be in accordance with Table 2.

NOTE: Ambition Factors **shall** not be lower than 1.

NOTE: the AFs chosen do not necessarily have to be the same value for each Safety Target.

ATMSPs set their acceptable Safety Targets as opposed to the tolerable Safety Targets set by the National Regulator because:

1. Safety margin: As compliance with tolerable Safety Targets can be difficult to demonstrate accurately, introducing a margin will increase the likelihood of their satisfaction in view of uncertainty in application.
2. Ambition: An ATMSP may wish to exceed the National Regulator minimum for business reasons (see §2.4 “role of ATMSP”).

An ATMSP may wish to revisit its choice of Ambition Factor (AF) values as a result of a significant period of monitoring of their application or as a result of changes in corporate safety policy. This is provided that the values remain within the mandatory limits specified in this document. However, it is not considered advisable that this is done on a routine basis (e.g. not every year).

Users of this document have to put in place a monitoring system (e.g. SAM-SSA (System Safety Assessment)) that will provide the appropriate feedback to validate these data.

2.6 CONVERSION INTO “PER YEAR”

The Safety Targets defined in Table 2 using “per flight-hour” **should** be converted into Safety Targets using “number of occurrence of an effect of a given Severity Class per year”, by injecting the year 2004 volume of traffic (flight-hours per year).

This can be further converted into “number of occurrence of an effect of a given Severity Class per operational-hour” using an appropriate and justified rationale.

If an ATMSP has an actual volume of traffic in 2004 which is less than 50 000 fh/y, then the ATMSP **should** use 50 000 fh/y as volume of controlled flight-hours for this conversion.

Safety Targets in /y, converted in this way, **shall** be presented as truncated numbers in the ATMSP RCS in the following format: A E-B /unit where A is only one digit and B is an integer. For example if a value of $2.93 E-5 /y$ is derived, then the quoted value in the RCS would be $2 E-5 /y$.

NOTE: The 0.93 part of $2.93 E-8/y$ delivers a confusing message as it gives the erroneous feeling that such precision can be used to define and design either new ATM systems or changes to existing ATM systems and that such precision can be demonstrated.

This conversion into per operational-year allows meaningful specification of Safety Targets and derivation of Safety Objectives at the ATM Service Provision level.

2.7

EXAMPLES

Using the ATMSP RCS derived in Table 2, the conversions given in Table 3 would apply for the three example ATMSPs having the year 2004 flight-hours quoted.

	ATMSP-1	ATMSP-2	ATMSP-3
Traffic Flight hours per year (2004)	e.g. 100 000	e.g. 1 000 000	e.g. 5 000 (will use 50 000, see§2.5)
	ATMSP Acceptable Events frequency (one event every....)		
ST ₁	10 000 years	1 000 years	20 000 years
ST ₂	10 years	1 year	20 years
ST ₃	1 year	1 month	2 years
ST ₄	4 days	10 hours	1 week

TABLE 3: EXAMPLE OF SAFETY TARGETS FOR VARIOUS FH/Y

2.8

ADVANTAGES AND LIMITATIONS OF ATMSP RCS

ED-125 adopts the use of an RCS as a means of setting Safety Targets. The advantages and limitations of this approach are indicated below. The users **should** make allowance as appropriate of any limitations in relation to their use of the scheme.

Advantages:
A clear identification of tolerable and acceptable Safety Targets is defined by setting Ambition Factors.
The RCS covers the Overall service provision of the ATMSP thus allowing to get an overall picture of risk.
Safety Targets are clearly specified per Severity Class.
The RCS is stable to ensure a consistent approach for designing systems (e.g. for a decade).
The RCS is enforcing a minimum Safety Targets whatever the operation and geographical location within the ECAC area.

Limitations:	Mitigation Means
Validation of the assumptions underlying the RCS needs to be performed periodically.	Both users of this document as well as document contributors have to review periodically these assumptions and revisit the document when necessary.
The RCS is based on an empirical model rather than a formal and rigorous ATM performance model. However, validation with some ATMSP actual data has been conducted.	Both users of this document as well as document contributors have to periodically review the model for its suitability and ability to deliver appropriate results.
The derived figure of the RCS cannot easily be validated e.g. one SC ₁ effect per 10 000 years.	Contribution to ST1 satisfaction is not solely based on quantitative argument. ST1 is a design Safety Target, not a safety performance monitoring value.
The RCS is based on the ESARR 4 ECAC average and not per ATMSP.	Using an ECAC average means that for ATMSPs that were performing far better than the RCS values as set in this document, then complying with this document would lead to a degradation of their safety performance. The mitigation means for this category of ATMSP would be to set an even more demanding Ambition Factor (more than 10). For ATMSPs that were not performing as requested by the RCS, then applying this document would lead them to increase their safety performance.
RCS using /fh as a basis assumes that the contribution to an accident or an incident has a linear relationship with the volume of traffic.	For ATMSPs having a low level of traffic the threshold has been set to 50 000 fh/y to be used instead of actual Year 2004 traffic. Today no ATMSPs have such a high level of traffic (beyond 5 E6 fh/y per ATSU) that would lead to develop another way to convert fh/y into /y.

CHAPTER 3

SAFETY OBJECTIVES

3.1 INTRODUCTION

A Safety Objective is defined in ESARR4 (Ref [1]) as a “quantitative or qualitative statement that defines the maximum frequency or probability at which a hazard can be expected to occur” (See §1.4.6).

For the purpose of this document, a Safety Objective is more specifically defined as a quantitative statement that defines the maximum frequency or probability at which a hazard can be accepted to occur. This is because the scope of this document is to set quantitative Safety Objectives to be used in the specification and design of ATM systems.

When designing systems it is important to understand how often a hazard can acceptably occur in order to contribute to an acceptable level of risk. The Safety Objective will influence the level of rigour and type of practices necessary to design a system that, when its performance is demonstrated, is likely to satisfy the Safety Objective. Other objectives (performance, security, interoperability, environmental) may exceed the stringency of the Safety Objectives.

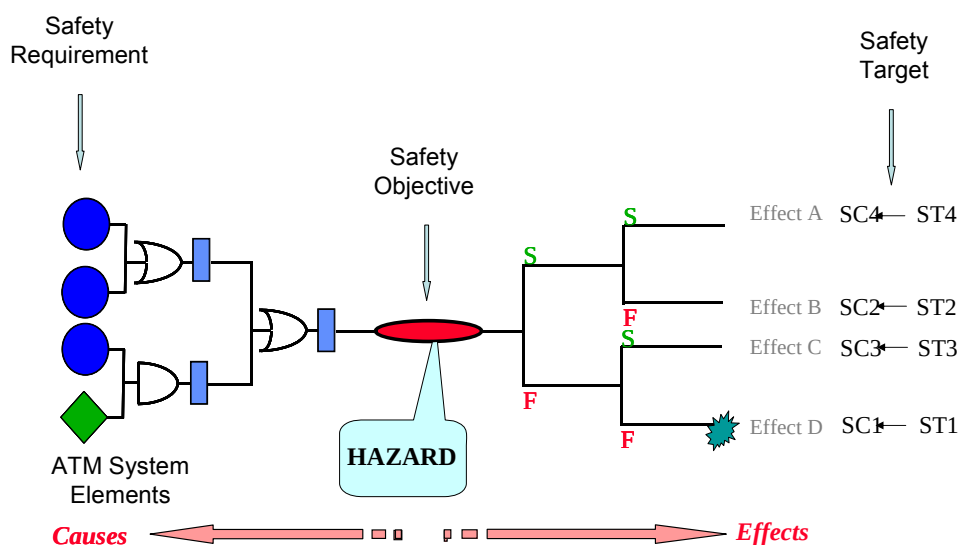


FIGURE 1: SAFETY OBJECTIVE

Figure 1 illustrates the function of the Safety Objective in developing Safety Requirements.

In the context of this document, the scope of applicability of a hazard and its associated Safety Objective **shall** always be at the level of the ATM service provision.

If a safety assessment is performed at a lower scope (sub-function or sub-system contributing to the ATM Service Provision), then this document does not apply. In such cases, the link needs to be provided between the Safety Objectives for the ATM Service Provision as specified in this document and the Safety Objectives of the hazards at the boundary of the sub-system under assessment.

3.2 APPROACH TO DERIVE SAFETY OBJECTIVES

3.2.1 Safety Objectives in an operational environment

The specification of the Safety Objectives (SO) takes into account the external mitigation means between the hazard and their associated effects. Any External Mitigation used to modify the Safety Objectives **shall** be stated as Safety Requirements on the Operational Environment. These Safety Requirements have also to be specified on the Operational Environment in order to derive Safety Objectives from Safety Targets (e.g. SAM-FHA).

3.2.2 How to use Safety Objectives

Each model described in Chapter 5 provides guidance for the derivation of quantitative Safety Objectives.

Safety Objectives will be used to determine Safety Requirements bearing on the system elements within the Service Provision/system design (e.g. SAM-PSSA) within a specific Operational Environment.

3.2.3 Assumptions

The following assumptions regarding derivation of Safety Objectives have been made in the application of the methods presented in this document:

1. The Safety Objectives in this document refer to hazards at the Service Provision level (implemented by people, equipment and procedures) as per ESARR4 and cannot be applied directly and solely to an individual element e.g. equipment;
2. Although completeness in identifying hazards and especially their combinations cannot be guaranteed, the determination of Safety Objectives is sufficiently conservative to compensate for these uncertainties.

3.3 SAFETY OBJECTIVE UNITS

The relationship between different units used to specify Safety Objectives and the ATMSP RCS **shall** be explicit, traceable and sustained with a rationale.