EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

ESARR ADVISORY MATERIAL/GUIDANCE DOCUMENT
(EAM/GUI)

EAM 4 / GUI 1

EXPLANATORY MATERIAL ON ESARR 4 REQUIREMENTS

Edition	**:**	**2.0**
Edition Date	**:**	**01 March 2005**
Status	**:**	**Released Issue**
Distribution	**:**	**General Public**
Category	**:**	**ESARR Advisory Material**

SAFETY REGULATION COMMISSION

F.2 DOCUMENT CHARACTERISTICS

TITLE		
EAM 4 / GUI1 **Explanatory Material on ESARR 4 Requirements**		
Document Identifier :	**Reference :**	EAM 4 / GUI 1
eam4gui1_e20_ri_web	**Edition Number :**	2.0
	Edition Date :	01-03-20045

Abstract :

This guidance material has been prepared by the Safety Regulation Commission to provide guidance for ATM safety regulators and support the implementation of ESARR 4.

The main purpose of this document is to provide guidance about the provisions established in ESARR 4 and more specifically in its Section 5 'Safety Requirements'. Each requirement is illustrated by giving explanatory material that includes a rationale, the most significant implications mainly for Regulator but also sometimes for Provider, and information about further development.

This is one element of a series of guidance documents to be developed by SRC to support the implementation of ESARR 4.

Keywords :

ESARR 4	Risk Mitigation	Risks
Safety Requirements	Safety Argument	Safety Objectives
Risk Assessment	Hazard	

Contact Person(s) :	**Tel :**	**Unit :**
Françoise GIRARD	+32 2 729 51 65	DGOF/SRU

DOCUMENT STATUS AND TYPE					
Status :		**Distribution :**		**Category :**	
Working Draft	☐	General Public	☑	Safety Regulatory Requirement	☐
Draft Issue	☐	Restricted EUROCONTROL	☐	Requirement Application Document	☐
Proposed Issue	☐	Restricted SRC	☐	ESARR Advisory Material	☑
Released Issue	☑	Restricted SRC Commissioners	☐	SRC Policy Document	☐
		Restricted SPG	☐	SRC Document	☐
		Restricted SRU	☐	Comment / Response Document	☐

SOFTCOPIES OF SRC DELIVERABLES CAN BE DOWNLOADED FROM :

www.eurocontrol.int/src

F.3 DOCUMENT APPROVAL

The following table identifies all management authorities who have approved this document.

AUTHORITY	NAME AND SIGNATURE	DATE
Quality Control (SRU)	***signed by Daniel Hartin*** (Daniel HARTIN)	01.03.2005
Head Safety Regulation Unit (SRU)	***signed by Peter Stastny*** (Peter STASTNY)	01.03.2005
Chairman Safety Regulation Commission (SRC)	***signed by Martin Radusch*** (Martin RADUSCH)	01.03.2005

Note: For security reasons and to reduce the size of files placed on our website, this document does not contain signatures. However, all management authorities have signed the master copy of this document which is held by the SRU. Requests for copies of this document should be e-mailed to: sru@eurocontrol.int.

(Space Left Intentionally Blank)

F.4 DOCUMENT CHANGE RECORD

The following table records the complete history of this document.

EDITION NUMBER	EDITION DATE	REASON FOR CHANGE	PAGES AFFECTED
0.01	01-Aug-01	Creation – First working draft 0.01 from OBIZO to SRU for kick off meeting.	All
0.02	19-Sep-01	New working draft including initial contents for all sections. Circulated to SRU for review and as an input to 1st progress meeting (24/9/01).	All
0.03	08-Oct-01	Draft version incorporating feed back from SRU. All Sections updated. Circulated to SRU and RTF for comments.	All
0.04	27-Jul-02	New Draft incorporating comments received from SRU and RTF (as agreed at RTF16).	As noted
0.05	18-Oct-02	Updated on basis of comments received from ICAO for RTF Working Group approval. New document format.	All
0.1	11-Nov-02	Document status amended to 'draft issue' following approval at RTF17.	All
1.0	18-Feb-03	No comments received following SRC consultation, therefore document formally released.	All
1.01	29-Oct-04	SRU quality check and update to paragraph 4.3 as a result of SPG11.	15
1.1	17-Dec-04	Document status amended following RTF consultation (RFC No. 0435). Document forwarded to SRC for formal consultation/approval.	All
2.0	01-Mar-05	Document released following formal consultation and approval by SRC (RFC No. 0440).	-

F.5 CONTENTS

F.6 EXECUTIVE SUMMARY

This guidance material has been prepared by the Safety Regulation Commission to provide guidance for ATM Safety Regulators and to support the implementation of ESARR 4.

Within the overall management of their ATM services, ATM service-providers shall have in place risk assessment and mitigation in ATM in accordance to ESARR 4.

Within their national legislative arrangements, ATM safety regulators shall have in place ESARR 4 related safety regulatory functions, resources and procedures in order to enforce and verify compliance with ESARR 4.

The main purpose of this document is to provide clarifications on provisions established in ESARR 4, and more specifically in its Section 5 ‘Safety Requirements’. Each requirement is illustrated by giving explanatory material that includes a rationale, the most significant implications mainly for Regulator but also for Provider, and when applicable, information about further development.

This documents forms part of a series of guidance documents being developed by SRC in order to support the implementation of ESARR 4.

(Space Left Intentionally Blank)

1. INTRODUCTION

A standardised approach to the formatting of EUROCONTROL Safety Regulatory Requirements is used to reference and to clarify the status of information contained in the document.

The requirement template used for ESARR 4, edition 1.0 includes a number of sections. Some includes provisions considered as mandatory and others provisions which are of advisory nature;

- The mandatory provisions are currently captured in sections 3, 5, 6 and 7 of the current ESARRs template; and
- Related advisory material is currently captured in sections 1, 2, 4 and 8 of the current ESARRs template.

Note: Work is on going to modify the ESARRs template and better separate the mandatory provisions from related advisory material.

Section 5 '*Safety Requirements'* provide a statement of precise actions which are considered necessary to achieve the safety objectives stated in Section 4. Section 5 section includes only mandatory requirements (expressed using the word "shall"), including those relating to implementation.

The main purpose of this document is to illustrate and clarify the provisions of Section 5 *'Safety Requirements'* established by ESARR 4 and facilitate its interpretation.

In addition, similar clarifications are being also provided for all other sections in ESARR 4, to facilitate its rationale, understanding and uniform implementation across States.

After a brief overview of each section of ESARR 4, each section and safety requirement is illustrated by providing explanatory material that includes a rationale, the most significant implications for both Regulator and Provider, and information about further development, whenever applicable.

2. SECTION 1 – SCOPE

2.1 Overview

ESARR 4, Section 1 '*Scope'*, includes advisory material and is formed by four sub-sections: 1.1, 1.2, 1.3 and 1.4.

2.2 Section 1.1

2.2.1 General

Section 1.1 states what ESARR 4 is about;

- Quantitative risk based approach,
- Air Traffic Management, and
- When changing the ATM System.

2.2.2 Contents

Section 1.1 states that;

"This requirement concerns the use of a quantitative risk based-approach in Air Traffic Management when introducing and/or planning changes to the ATM System[1]."

2.2.3 Rationale and Implications

Air Traffic Management

The rationale for limiting the scope of ESARR 4 from Air Navigation Services to Air Traffic Management is simply that the Terms of Reference of the Safety Regulation Commission are limited to "Air Traffic Management".

This implies theoretically that only changes to Air Traffic Flow Management, Airspace Management and Air Traffic Services are subject to ESARR 4.

Note: It is however advisable to apply ESARR 4 to all changes to the Air Navigation System which could have a potential safety impact (e.g. Aeronautical Information Service).

As no other exclusion or limitation is mentioned in that sub-section, this implies that;

- ATM Services provided to both commercial air transport and general aviation operations are being addressed in ESARR 4[2]; *(Note: It is recognised that the level of safety achieved today by commercial air transport is higher than the safety level achieved by General Aviation and this will probably drive the level of safety required from ATM System providing services to both types of operations)*, and
- All airspace classes are addressed in ESARR 4; airspace management and related airspace design may well induce unacceptable risks, and is therefore subject to ESARR 4 *(Note: It is recognised that there might be a difference in the levels of safety achieved today in controlled airspace and in non-controlled airspace).*

Quantified Risk Based Approach

The rationale is that;

- From previous experience in a number of ECAC States, a risk based approach is considered as meeting the objectives of the SRC in assessing and controlling risks related to changes in ATM,
- A risk based approach is the most commonly used approach in aviation[3], both internationally and in the aircraft community (Refer to both Federal Aviation Requirements and Joint Aviation Requirements applicable to aircraft certification),

[1] *Considering its airborne and ground (including spatial) components.*

[2] *Even if the quantified elements provided in Appendix A do not apply to airspace where only general aviation operates.*

[3] *As well as in other safety critical industries such as chemical and nuclear.*

- There is an added value in using quantitative objectives, as it avoids diverging understandings by States on the range of frequencies of occurrences included in a risk classification scheme,
- Quantitative criteria provide a clear target and, when derived and applied to lower level events, allow manufacturers to get on designing their equipment without having to analyse the entire ATM System[4],
- The safety performance measurement of actual safety occurrences (with ATM contribution) may enable the verification *a posteriori* of whether or not quantitative objectives allocated to specific failures in a 'fault tree' for example are being met. Indeed, quantitative objectives could be derived from ATM safety minima and allocated to specific failures in a 'fault tree', hence providing for a range of probabilities which can be reasonably assessed over a short or medium period of time[5],
- In addition to the measurement of accidents and serious incidents rate with associated ATM contributions, such a feed back from experience on events of a lower level would enable to measure the effectiveness of the qualitative processes selected for software, human, or procedures and the identification of related appropriate "good working practices" to be used in ATM as acceptable measures to show compliance with quantified objectives[6],
- SRC decided therefore to provide quantified ATM Safety Minima for the ECAC region in a manner consistent with the safety objectives included in the ECAC ATM 2000+ strategy, but to remain, as a safety regulator, at a very high level (i.e. ATM) , the ATM System architect(s) being the only one(s) to be in a position to derive the top level objective down to the lower levels of the system,
- SRC decided also to document in SRC POL DOC 1 "ECAC Safety Minima in ATM" all assumptions made when developing the high level safety minima in ATM (and to invite States to do the same when developing their national minima); indeed, past experience has shown that the assumptions on which a safety objective is being based are easily forgotten and those objectives may then be used beyond the original intent, and
- SRC decided also to test periodically its assumptions to verify that they remain valid and that its top-level safety minima remain acceptable. Care will also be taken not to change the top-level safety minima too often to avoid placing a "moving target" as a requirement on the ATM System.

(Space Left Intentionally Blank)

[4] *Of which they often do not have the necessary visibility.*

[5] *This would hopefully not be true for ATM induced accidents.*

[6] *An example in aircraft certification would be the assurance levels of ED12C/DO178C where a priori associations were made between some qualitative requirements and the quantified levels of JAA AMJ 25.1309.*

Notes:

1) The feasibility of setting quantitative objectives/targets for specific parts of the ATM System was discussed, especially when it comes to their allocation to human contributions, procedures and software. It is recognised that demonstration of compliance won't always be quantitative- based, as it does not seem feasible to demonstrate a priori and in a quantified manner that a good working process, such as training, Safety Management System, or software codes of practices, enable specific quantitative objectives to be met. This will only be based on professional judgement and potentially verified over time.

2) The feasibility of setting quantitative objectives/targets was also discussed for another reason: the review of existing safety data in ATM across the ECAC region has identified limitations and inconsistencies. Relying solely on historical data to derive ATM safety minima could lead to very high constraints being placed on the ATM system[7]. This is why it is advised to combine professional judgement with historical data when setting safety minima[8].

This implies that;

- An equivalent minimum level of safety should be provided to aircraft wherever they fly in the ECAC airspace,
- Further quantitative refinements of the ECAC Safety Minima in ATM should be undertaken at national level, possibly by the national ATM safety regulator, according to the principles described in SRC POLICY DOC 1 and ESARR 4 Appendix A, and
- A priori demonstration of compliance of the quantified objectives won't necessary rely on quantified demonstration and a posteriori verification of the quantified objectives with statistical data will rely on the implementation of a safety performance measurement system at the lower levels of the 'fault tree'.

2.2.4 Further Development

The SRC is developing a Guidance Material to States to help them develop their national ATM safety minima and national ATM risk classification scheme according to SRC POLICY DOC 1 (ref: EAM 4 / GUI 4).

The SRC is also developing a Guidance Material to national ATM Safety regulator to help them develop their ESARR 4 Safety Oversight function (ref: EAM 4 / GUI 2).

(Space Left Intentionally Blank)

[7] *For the only reason that ATM may be reported as being safer than it actually is.*

[8] *This was done when developing SRC POLICY DOC 1.*

2.3 Section 1.2

2.3.1 General

Section 1.2 defines the elements of the ATM System which are subject to ESARR 4.

2.3.2 Contents

Section 1.2 states that ESARR 4;

"covers the human, procedural and equipment (hardware, software) elements of the ATM System, as well as its environment of operations".

2.3.3 Rationale and Implications

The rationale is that causes to accidents and incidents can originate from equipment, procedures and human beings and from their interactions. Similarly, the risk mitigation measures will impact not only the "equipment" but also the other elements of the ATM system, hence placing requirement on staff, procedures, airspace design, and aeronautical publication services. They could even limit accepted capacity.

It should be noted that Communication, Navigation and Surveillance (CNS) is considered as the enabling infrastructure to support the provision of ATM services and is therefore included in the scope of ESARR 4.

Changes to the environment of operations may have a safety impact as some of the characteristics of environment may be used as safety assumptions in the assessment of a change to the ATM system; environment characteristics may therefore be used as mitigation factors when assessing the severity of effects of hazards, hence when allocating safety objectives.

Note: It could be argued that risk assessment and mitigation should be also performed for any changes in the environment of operations (inclusive of airspace and traffic characteristics). There are at least two ways of addressing this;

- *either as a systematic assessment of the changes in the environment of operations, or*
- *by way of tractability of the safety assumptions placed on the environment followed by a regression analysis if these assumptions are not valid anymore. (This is the approach implicitly adopted in ESARR 4). Indeed, according to ESARR 4, safety related assumptions are expected to be traced to the intended functions when used to allocate a severity class and/or mitigate a risk. As such, they have become safety requirements and should be monitored during operations. If these safety assumptions/requirements are not valid anymore, the safe operations of the ATM system won't be valid anymore and an analysis of the safety impact of those deviations will be necessary to find remedial measures.*

2.4 Section 1.3

2.4.1 General

Section 1.3 defines the phases of the life cycle during which ESARR 4 applies.

2.4.2 Contents

Section 1.2 states that ESARR 4;

"This requirement covers the complete life-cycle of the ATM System, and, in particular, of its constituent parts."

2.4.3 Rationale and Implications

The rationale is that;

- Hazards originate often during the transition phases of a system,
- Safety requirements will not only impact the initial definition, design, implementation and commissioning of an ATM system but will also place constraints on the operations and maintenance of the system, and
- It is not enough to verify that an ATM system is safe before and when being transferred into operations but it shall also continue to be safe over time, and at least as safe as when initially approved;

The implications are that;

- Safety Regulators should check that safety objectives and requirements are well promulgated to those responsible for all phases of the life cycle, from design, transfer into operations, operations and maintenance and that responsible entities should formally commit to their continuous implementation;
- Safety regulators should ensure that safety arguments submitted to them include a specific argument for all phases of operations, including the transition/transfer ones, and
- Safety regulators should implement both initial and on going safety oversight functions to verify compliance with ESARR 4 (refer to EAM 4 / GUI 2).

2.5 Section 1.4

2.5.1 General

It limits the scope of application of ESARR 4.

2.5.2 Contents

Section 1.4 states that ESARR 4;

"This requirement does not address the assessment of introducing and/or planning organisational or management changes to the ATM service provision[9]."

[9] *The implementation of Safety Management System is being addressed in ESARR 3 « Use of Safety Management Systems by ATM Service Providers ».*

2.5.3 Rationale and Implications

It is recognised that changes into the organisation providing ATM services may have safety impacts and that these should be assessed and mitigated.

However, it is expected that the acceptability of those changes would be assessed as part of the implementation of an organisation's "Safety Management System" (Refer to ESARR 3) as well as of related ESARR 3 safety oversight by ATM safety regulator.

In addition, work is on going defining a set of recommendations for ESARR 3 Safety Oversight and this should pave the way to the implementation of harmonised national safety regulatory regimes aiming at verifying that ESARR 3 is being met, for a specific implementation of SMS within an organisation.

This would include assessment, audit and continuous acceptance of an SMS, with related approval of proposed changes to the SMS in before they are implemented (refer to EAM 3 / GUI 3).

3. SECTION 2 – RATIONALE

3.1 General

This sub-section includes advisory material and elaborates on the need for ESARR 4. It confirms the need to go beyond the provisions of ESARR 3 in the area of risk assessment and mitigation in ATM.

3.2 Contents

Sub-section 2.1 recognises that;

"The increasing integration, automation and complexity of the ATM System requires a systematic and structured approach to risk assessment and mitigation, including hazard identification, as well as the use of predictive and monitoring techniques to assist in these processes".

Sub-section 2.3 recognises that;

"Errors in the design, operation or maintenance of the ATM System or failures in the ATM System could, through a decrease in safety margins, result in, or contribute to, a hazard to aircraft. Increasingly, more reliance and therefore a greater safety burden, is being placed upon all parts of the ATM System. In addition, the increased interaction of ATM across State boundaries requires that a consistent and more structured approach be taken to the risk assessment and mitigation of all ATM System elements throughout the ECAC States".

Section 2.3 specifies that;

"In addition, and in certain cases, the implementation of ESARR 3 (Use of Safety Management Systems by ATM Service Providers) also necessitates the provision of more specific requirements to be used. ESARR 4 provides such detailed requirements, hence developing further sections 5.2.4 and 5.3.4 of ESARR 3".

Sub-section 2.4 concludes that;

"Accordingly, a harmonised approach to the identification, assessment and management of risk is a necessary step in ensuring high levels of ATM safety across the ECAC area".

3.3 Rationale and Implications

The rationale is that aviation is not anymore a puzzle built out of autonomous elements, but a mosaic of inter-related constituent parts and elements, with functions transcending equipment, and services not being performed through a unique organisation. There is therefore a need to better allocate safety responsibilities to the various stakeholders involved in ATM. A process such as that of ESARR 4 allows for safety responsibilities to be developed in co-ordination and allocated without ambiguity to all stakeholders.

In addition, recent experience in implementing FANS[10] have raised a number of issues which can not but be resolved by a more formal assessment and control of risks induced by new operational concepts. Errors in the process of design and operations indeed led to air proximity reports and aircraft hazards. Also, analysis of past accidents and incidents have also identified ATM causes and has demonstrated the need for a more systematic a priori assessment and control of ATM risks in an ever changing environment. It should be noted that ICAO is mandating the use of safety assessment of significant changes to ATS in amendment 40 to Annex 11. The provisions of ESARR 4 are consistent with the requirements of Annex 11 in this area and enable to strengthen them (refer to EAM 4 / ICAO).

Finally, at ECAC level, MATSE IV also decided in its institutional strategy upon a harmonisation of safety levels in ECAC. Furthermore, it falls within the SRC Terms of Reference to develop harmonised safety standards and requirements.

ESARR 3 only provides high level requirements in the area of risk assessment and mitigation and is considered as not being sufficient to ensure harmonised and consistent processes and outcomes to be found at ECAC level.

This implies that ESARR 4 is now in force and is to be enforced and implemented throughout ECAC by;

- Service providers of ATM, and
- ATM safety regulators.

(Space Left Intentionally Blank)

[10] *Future Air Navigation System*

4. SECTION 3 – APPLICABILITY

4.1 General

Section 3 specifies to which categories of ATM service providers ESARR 4 applies.

4.2 Contents

Section 3.1 of ESARR 4 specifies that;

"This requirement shall apply to all providers of ATM services in respect of those parts of the ATM System and supporting services, within their managerial control[11]."

Section 3.2 of ESARR 4 specifies that;

"This requirement shall apply to military ATM service providers except in those cases in which military ATS or Air Defence are only and exclusively involved in the control of military aircraft, in a segregated military airspace environment."

4.3 Rationale and Implications

Also refer to § 2.2.3.

In accordance with the set of definitions used by SRC, a provider of ATM service(s) is an organisation responsible and authorised to provide service(s) for the purpose of ATM (ATS, ASM and ATFM). Furthermore, ATS is comprised of the following types of services: Air Traffic Control (i.e. Area Control service, Approach Control Service, Aerodrome Control service, and Air Traffic Advisory Service, Flight Information Service and Alerting Service). In addition, these services can be applied in the 7 types of airspace (A through G) as defined in ICAO Annex 11. All these services and airspaces are therefore within the scope of ESARR 4.

The rationale for limiting the applicability of ESARR 4 to exclude the case of exclusive military operations and services is that the causes of hazards may vary significantly and be military specific.

In addition, hazards related to those exclusive military services/operations would not impact at all the operations falling within the scope of the SRC.

Note: Care should however be taken to any potential civil impact in this exclusion, as airspace design and implemented mechanisms of airspace segregation may in itself constitute a hazard.

This also implies that any delegation of ATM service provision responsibilities should also cater for the implementation of ESARR 4 in the service provider organisation. A safety regulatory function should also be in place to oversee the actual implementation of risk assessment and mitigation according to ESARR 4.

In addition, this also implies ESARR 4 applies to ATM services provided at airports. Related implementation of ESARR 4 should be well scoped and co-ordinated with the non-ATM elements of the airport.

[11] *Whatever the national or international institutional arrangements supporting the provision of ATM services, the provisions of this requirement have to be met.*

5. SECTION 4 – SAFETY OBJECTIVE

5.1 General

Section 4 includes advisory material and specifies the objective pursued by the SRC in developing ESARR 4.

5.2 Contents

Section 4 states that;

"Within the overall objective of ensuring safety, the objective of this requirement is to ensure that the risks associated with hazards in the ATM System are systematically and formally[12] identified, assessed, and managed within safety levels, which as a minimum, meet those approved by the designated authority".

5.3 Rationale and Implications

Risk assessment and mitigation does not represent an end in itself, but should contribute to controlling risks to a tolerable level.

In accordance with the Chicago Convention, a State has complete and exclusive sovereignty over the airspace above its territory. Nevertheless, on adhering to the ICAO and EUROCONTROL Conventions, States agree on certain principles, in order that international civil aviation may be developed in an orderly and safe manner. In order to discharge its responsibilities, each State should therefore enact a basic aviation law, which provides for the development and promulgation of a code of air navigation rules and regulations.

As a minimum, those rules and regulations should state the target level of safety (i.e. safety minima in ATM) for the national airspace and airports. They should be in that regard consistent with the safety objectives agreed in the ECAC ATM strategy for the years 2000+. They should also include regulations addressing both a priori and a posteriori assessment of risks to better anticipate and control risks (i.e. ESARR 4) as well as to measure and improve safety based on feed back from experience (i.e. ESARR 2).

It is the duty of safety regulators to ensure as far as possible that those safety minima are and will be met, both in anticipation of a planned operations and during operations. Hence the need to establish a safety regulatory requirement which specifies minimum rules to be followed *a priori* to assess and mitigate potential risks induced by changes to ATM so that the safety of the national airspace remains within agreed tolerable levels.

This implies that the risk classification scheme provided in ESARR 4 Appendix A includes some quantified elements directly derived and consistent with the ECAC Safety Minima in ATM derived in SRC POLICY DOC 1[13]. A similar link would be expected at national level, between the national safety minima in ATM and the quantified criteria against which the tolerability of risks are assessed at national level.

---

[12] *Used in its common English sense.*

[13] *Implementing in a quantified manner some safety objectives of the ECAC ATM 2000+ strategy.*

6. SECTION 5 – SAFETY REQUIREMENTS

6.1 Overview

ESARR 4, Section 5 '*Safety Requirements'*, is formed by three sub-sections and one appendix:

- 5.1
- 5.2
- 5.3
- Appendix A- Risk Classification Scheme
- A-1- Hazard Identification and Severity Assessment in ATM
- A-2- Risk Classification Scheme in ATM

6.2 Section 5.1

6.2.1 General

It requires the implementation of hazard identification, risk assessment and mitigation for changes to the ATM System.

- Implemented by all ATM service-provider organisation;
- Implemented for any change to its ATM services, but also those supporting services that are under its managerial control;
- Addressing the complete life cycle;
- Adopting a total system approach addressing both the airborne and ground components of the ATM System ;
- Addressing procedures, equipment and human; and
- Addressing all internal and external interaction/interface issues.

6.2.2 Requirement

The requirement states that;

"An ATM service provider shall ensure that hazard identification as well as risk assessment and mitigation are systematically conducted for any changes to those parts of the ATM System and supporting services within his managerial control, in a manner which addresses the;

1) complete life-cycle of the constituent part of the ATM System under consideration, from initial planning and definition to post-implementation operations, maintenance and de-commissioning,

2) airborne and ground[14] components of the ATM System, through co-operation with responsible parties, and

[14] *Including spatial components.*

3) three different types of ATM elements (human, procedures and equipment), the interactions between these elements and the interactions between the constituent part under consideration and the remainder of the ATM System.

6.2.3 Rationale and Implications

Any changes

The rationale is that no change to the ATM System can be implemented without a clear indication that safety won't be jeopardised. Indeed, if only some changes to the ATM system were to be subject to ESARR 4, there would be no other mechanism which would allow to rule out a change on the ground that it has no safety impact.

This implies obviously, that the level of analysis and demonstration required by ESARR 4 should be adjusted to the anticipated and demonstrated safety significance of the proposed changes.

Also refer to § 8.3.

Complete life cycle

Refer to § 2.3.2.

Total System approach

The rationale is that;

- Each State is responsible for the safety of the national airspace (Refer to § 5.3); this includes the specification and promulgation via the national AIS of the required aircraft equipage to fly in the national airspace and related airspace classes,
- The overall safety of an airspace is related, among other things, to the level of equipage and adequacy of operations of aircraft flying into that airspace. For example, for the safety offered by an RNAV route to be implemented according to the planned tolerable level of safety, aircraft must be equipped and must fly according to a minimum set of requirements. Equally, If a number aircraft fly into a specific class of airspace (e.g. 8.33 kHz or RVSM airspace) without being equipped according to required equipment/performance, they jeopardise the safety of this airspace, hence the safety of all other aircraft flying into that airspace,
- ECAC, at MATSE IV (1997), requires in its institutional strategy that a total system approach be adopted to the management of safety in aviation,
- The ATM System is being considered in EUROCONTROL as one part of the Air Navigation System, composed of a Ground Based ATM component and an airborne ATM component,
- Hazards usually result from a chain of events. Therefore, some hazards will result from a combination of failures/errors, originating from both the airborne and ground segment of the ATM System,
- There may also be more than one solution available to reduce the severity of effect of hazards, their probability of occurrence, some implying safety requirements bearing on the ground part of the ATM system, others on the airborne part and finally others on both,

- The increased integration of ATM functions between the aircraft and the provision of ATM, and the contemplated delegation of ATM responsibilities to aircraft, implies that the aircraft is not autonomous anymore and should be taken into account as one enabler to ATM in any risk assessment and mitigation process, and
- Aircraft related studies such as those related to Flight Management Systems (FMS) have suggested that incompatibility between the aircraft system and the wider environment, such as ATC, seems more apparent than lack of understanding on the part of the crew. Validation of FMS requirements against user experience and the ATC environment, requirements, for example, was considered as incomplete[15].

Note: Some changes to the ATM System may not necessitate such a total system approach as it implies no direct interaction with the aircraft segment. In that case, there will only be a need to show that no interaction exists.

The implications are that;

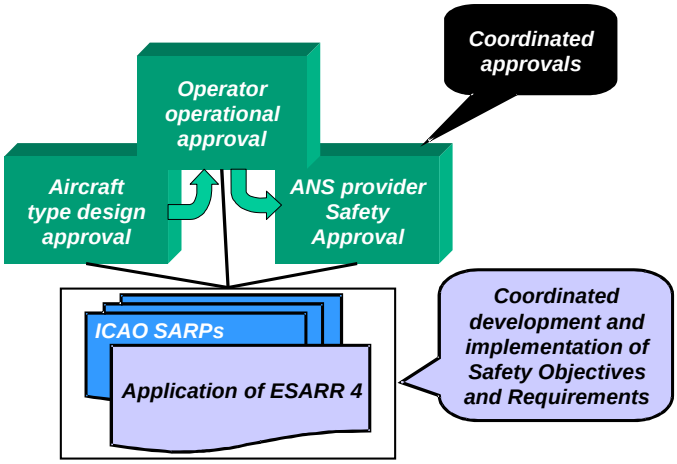
- ESARR 4 requires that any risk mitigation strategy be developed and validated in a co-ordinated manner, involving all stakeholders involved in the implementation[16] of a change to the national ATM System, so that the safety requirements bearing on the various parts of the ATM System are feasible, effective and consistent,
- Potential ATM related safety requirements bearing on the aircraft segment (be it equipage or operations) should then be promulgated in Aeronautical Information Services by the State having sovereign jurisdiction over that airspace[17],
- ATM Safety regulators should verify that adequate co-ordination took place between the ATM service provider(s) and other stakeholders not only during requirement development and validation, but also during design, implementation and commissioning; ATM Safety regulators should also verify that provisions have been made for continuing co-ordination to take place, specifically for future modifications and for on going monitoring of the ATM system,
- ATM safety regulators should also verify the consistency of what is being promulgated via AIS with the safety requirements included in the safety argument/safety assurance documentation,
- ATM safety regulators should co-ordinate related safety oversight activities to the extent that it is feasible with national authorities in charge of issuing the airworthiness certificate(s) and Operational approval(s) for aircraft/operator flying into the national airspace,

[15] *Reference:- Assessing error tolerance in FMS- Hazel Courteney- UK CAA SRG*

[16] *Such as aircraft manufacturers, operators, equipment manufacturers, communication service providers.*

[17] *It can reference to appropriate ICAO, EUROCONTROL, RTCA/EUROCAE standards if they exists.*

- The national authorities in charge of issuing the airworthiness certificate(s) and Operational approval(s) for aircraft/operator flying into specific airspace should then ensure, as part of their safety regulatory functions that ATM related safety requirements are enforced (Rule making) and that aircraft will indeed meet the set of criteria required in the national AIS(s) of the airspace(s) where aircraft are going to fly[18] (Safety Oversight).



(Fig 1:- Total System Approach)

Note: For changes to the ATM System not having a direct link with the aircraft segment, there will only be a need to show that no direct interaction exists. No extensive analysis of the interactions will be required but the demonstration should be unambiguous.

Note: For changes to the ATM System being implemented against standards and safety requirements which have been developed and validated against ESARR 4, the need for co-ordination may be limited to the implementation and operations phases.

At European level, a mechanism exists and aims at addressing this co-ordination of ATM/CNS requirements development between EUROCONTROL and the Joint Aviation Authorities (JAA). Indeed, the JAA have implemented a working group, called JAA CNS/ATM, to deal more specifically with these issues.

EUROCONTROL EATMP co-ordinates among ATM service providers the development of requirements and related implementation of a number of European-wide changes to the ATM System. As part of their tasks, they must apply ESARR 4 and assess/mitigation potential risks related to those changes, in co-ordination with all appropriate stakeholders. They produce a list of safety objectives and requirements, with associated safety assurance that safety will be kept within tolerable safety minima.

This safety argument is subject to SRC review, leading to a harmonised SRC view on the acceptability of those changes[19]. Some of the safety requirements identified in the safety argument bear on the airborne segment; therefore, aircraft flying into the airspace where the change is implemented will need to meet these safety requirements.

---

[18] *Some States, such as the US, have promulgated a specific requirement whereby foreign operators flying into the US airspace are subject to FAR 129 and related safety oversight, by FAA inspectors. In Europe, no similar requirements have been agreed.*

[19] *Which is then being used by ATM national regulators when deciding on the approval of related implementation at national level.*

There is thus a need for the aircraft community to identify those requirements and to document them in the airborne standards which are being used when developing new avionics. As such, these safety requirements need to be considered by the JAA CNS/ATM.

The JAA CNS/ATM can provide a validation of proposed safety requirements[20] and then develop appropriate regulatory material (e.g., Temporary Guidance Leaflets, Advisory Material Joint) addressing not only safety requirements derived from applicable JAA regulatory material but also from the application of EUROCONTROL regulatory material[21] to a specific ATM/CNS change (e.g., RVSM, RNAV).

This co-ordination of requirements still allows for various detailed architectures to be implemented both in the airborne and ground elements of the ATM System, provided they meet the allocated safety objectives/requirements.

The safety assurance evidence provided to the aircraft certification authorities to show compliance with TGL and AMJ (or equivalent) to an appropriate level of confidence can still rely fully on usual airborne standards and practices. The same applies to the ground part of the ATM System.

The FAA and CASA (CAA Australia) participate to the JAA CNS/ATM and this could ensure, if successful, a certain level of international harmonisation of CNS/ATM standards bearing on the airborne segment (in addition the service provider side of the FAA also co-ordinates some of their changes with EUROCONTROL EATMP).

Interactions and Interfaces/Elements

The rationale is that:

- Providing safety is more than making sure that each element of a wider system functions properly safe. The complex interaction between the various elements of ATM significantly determine safety,
- At a time of increased automation and system distribution, the adequacy of the equipment with its mode of operations and the impact on the human operator of that equipment become areas of specific safety interest,
- Hazards will often result from a chain of event, from a combination of failures of equipment and human errors,
- Hazards resulting from a failure in a part of a system can not be taken in isolation. Hazards may result from a combination of failures in that part of the system and other parts , or from the interface between two parts of the ATM System,
- There is a risk that addressing a part of a system in isolation leads to assumptions being made on other parts (or on environment) which are not correct, and
- Common Cause/Mode of failures must also be addressed.

[20] *Providing feed back on the feasibility, effectiveness, costs and schedule implications of draft safety requirements, as well as compatibility with other JAA applicable regulations.*

[21] *Such as ESARR 4.*

The implications are:

- The internal interactions within the system under consideration must be addressed by the ATM service provider and closely reviewed by regulators,
- Human factor assessment and related adequacy of procedures and equipment to the future operator and maintenance staff become more and more an area of safety importance, at a time of significant operational and technical changes,
- The safety regulator should verify that all stakeholders involved in a change, either directly or indirectly, as being responsible for a part of a system with which the system under assessment interfaces with, are involved; this applies in particular to ATM related changes at an airport (also, referred to as 'Total System Approach'), and
- A specific focus should be placed on how external interfaces are addressed. Entities responsible for a part external to the one under assessment should be involved at least in the validation of the safety assumptions made on their system/part and on the validation of safety requirements placed on them when applying ESARR 4; furthermore, the regulator should verify that they have committed to the continuous implementation of those safety requirements they have responsibility for.

6.3 Section 5.2.1 A and B as well as related appendices

6.3.1 General

It requires the implementation of a risk assessment and mitigation process which includes;

- definition of the system under assessment, with related environment, scope, interface and functions ; and
- determines safety objectives, with;
  - identification of credible hazards and failure conditions, with combined effects;
  - assessment of severity of their effects; and
  - determination of their tolerability.

6.3.2 Requirement

The requirement states that "*the hazard identification, risk assessment and mitigation processes shall include a determination of the;*

1) scope, boundaries and interfaces of the constituent part being considered, as well as the identification of the functions that the constituent part is to perform and the environment of operations in which it is intended to operate,

2) safety objectives to be placed on the constituent part, incorporating;

(i) an identification of ATM-related credible hazards and failure conditions, together with their combined effects,

(ii) an assessment of the effects they may have on the safety of aircraft, as well as an assessment of the severity of those effects, using the severity classification scheme provided in Appendix A, and

(iii) a determination of their tolerability, in terms of the hazard's maximum probability of occurrence, derived from the severity and the maximum probability of the hazard's effects, in a manner consistent with Appendix A;

(Note: It is considered as essential that the activities depicted in a), b), c) and d) are fully co-ordinated between those parties responsible for developing and implementing the safety requirements bearing on the constituent parts of the ATM System). See 5.1 (b) above.

(Note: It is recognised that a combination of quantitative (e.g., mathematical model, statistical analysis) and qualitative (e.g. good working processes, professional judgement) arguments may be used to provide a good enough level of assurance that all identified safety objectives and requirements have been met)."

Text Appendix A is not included here as too lengthy. However, relevant explanations are being provided in this section.

6.3.3 Rationale and Implications

Definition of the system under assessment

The 'system' is determined by what the ATM service provider wants to introduce at the time. Defining exactly the 'system' may be sometimes difficult. This is however an essential first step to start an assessment of the safety impact of proposed changes.

The rationale is that this definition should enable to identify the extent of ESARR 4 analysis a priori necessary as well as the main interfaces to the 'system' and related organisations having managerial control over them.

In addition, the ATM System could be unscrupulously divided in a number of systems, each of them using up the full regulatory limit[22], without leaving any room for the others. Defining the system and how it fits in a wider ATM and aviation system should avoid that pitfall.

Furthermore, without the identification of intended functions/services to be performed as well as the environment of operations in which the system will operate, it is impossible to assess the severity of effects of hazards. From this perspective, risk assessment and mitigation is one of the primary filters in ATM concept development.

For example, loss of surveillance for five minutes will have a completely different safety impact in an oceanic environment than in a dense TMA.

This implies that;

- ATM safety regulators should ensure that intended function/operational capabilities which will be offered thanks to the change is documented in clear manner; or alternatively, for any trial system, that clear assumptions are made on intended functions/services and operational environment,

[22] *ATM safety minima and related safety objectives*

- ATM safety regulators should verify that the definition and scope of the system highlight how it is integrated into the overall ATM system,
- ATM safety regulators will need to be convinced one way or another of the validity of the assumptions made on intended functions/services/environment of operations, and
- Obviously, related assumptions made on intended functions, services, and environment of operations, in the course of a cost/benefit assessment of a proposed change will have to be consistent with those made in the risk assessment and mitigation process.

Identification of credible Hazards and Failure Conditions

Hazard is to be used according to its very generic definition.

The scope of the hazard analysis is not limited to the boundaries of the system being changed, but should include all components and systems involved in the service provided in the environment of operations. It should consider the combined effect of hazards.

When assessing a hazard at the outer boundary of the ATM/CNS System, hazards will usually be related to the operations of aircraft (e.g. aircraft deviating from cleared flight level) and provisions of ATM services (e.g. transfer of communication between FIRs); failure conditions will then relate to the functions enabling the provision of ATM service (e.g. loss of surveillance function);

- Going down the relative hierarchy of hazards, failures will generally be associated to equipment, and errors or mistakes to human, and
- Focusing on credible hazards and failure conditions should avoid distract from areas where there may be more safety benefit to be gained.

In addition, ESARR 4 does not specify if hazard should or should not be described with qualifiers attached (e.g. loss of surveillance for more than 30 seconds). Indeed, this choice belongs to the HOW to CONDUCT the risk assessment process. *(Note: The final outcome-safety objectives and requirements-should be similar whatever approach is adopted. However, for ATM, the assessment of the severity of hazards may require other factors such as 'time duration' to be used to qualify failure conditions and hazards).*

Assessment of effect on safety of aircraft operations

Hazards are to be classified according to the severity of their identified effects and Appendix A- Fig. A-1 gives a scale for the severity of the effects or consequences of a hazard.

The rationale is that, in practice, many hazards are encountered that will only conditionally lead to any of the consequences mentioned in the table. In this case, the severity has to be estimated by following the "hazard tree" upward and finding the effect on operations that is most likely.

Severity of effects

The ultimate criteria used to assess the severity of hazards at the outer boundary of the ATM/CNS system is the impact on aircraft operations (expressed in terms of *ATM induced* accidents and incidents[23]).

The rationale is that the events of ultimate concern to society, passengers, industry and regulators are most often considered to be aircraft accidents/ incidents in which people are, or could be, harmed. The ultimate aim of any aviation safety assessment should therefore be to minimise the chance (probability or frequency) of aircraft incidents / accidents, and the number of resulting deaths and injuries.

Explicit consideration of the extent or number of injuries and deaths does not seem to be justified and very helpful when assessing ATM services, since these will depend on many circumstantial and widely varying factors, such as aircraft size, speed, collision geometry, survivability and the availability of rescue services, and not on ATM. The uncertainties in such factors may tend to obscure the objective of the risk assessment and mitigation process in ATM. As these factors are considered as outside the control of ATM, their consideration would therefore not add any additional inputs to the safety constraints placed on ATM.

This implies that ESARR 4 severity scale is not 100% aligned to the FAR/JAR AMJ 25.1309 as both schemes do not address the same purpose. However, should there be a need for comparing both schemes, the most severe class of ESARR 4 would be equivalent to “catastrophic accident”, as ESARR 4 assumes the worst case scenario for elements outside of its control.

At a lower level, secondary criteria to be used include the potential for collision between aircraft and aircraft/ground/something else, and the degree of ability to recover from such hazardous situation.

The rationale is that the physical proximity of an ATM induced accident whether distance or time based) alone does not determine the level of risk. The geometry of the situation and other factors equally contribute to the level of risk.

This implies that there can not but be some subjective judgement in any assessment of severity, hence advocating for putting together the rationale for a severity class.

In addition, elements to be considered in the severity assessment would include a number of indicators, such as ATCO and crew workload, exposure time to the hazard etc. but these should not be seen as the final severity criteria.

The rationale is that this approach of assessing in a structured manner the various impacts of a hazard will help develop the necessary rational/justifications for the severity classification against impact on aircraft operations. This approach will also help to keep track of those rationales and provide a good basis for any regression analysis should any modification in the environment of operations occurs.

This implies a level of subjectivity of lesser degree in the assessment of severity. Furthermore, it will enable collation of useful data for future work, hence paving the way to a more and more standardised method for assessing severity.

[23] *Such accidents would include mid air collision between two aircraft, collision with the ground, collision on the ground, but also loss of flight control due to ATC.*

Elements to be considered in the severity assessment could include those mitigating means that the safety regulator would a priori consider as acceptable or unacceptable.

An example could be the use of safety nets as mitigation means or not, for which the national regulator may have issued a policy, or for which the regulator may make a statement at the beginning of the project.

Worst case scenario

The severity of hazards will be determined by the credible consequences on the managed aircraft, when the outcome of all the safeguards which may exist in the other parts of the ATM System have been taken into consideration.

For example, the most severe class will only be chosen in such cases when the total ATM System has exhausted its possibilities to affect what continues to happen and only chance determines if the consequence will be a collision or not.

Equally, the severity of hazards will be determined by the credible consequences on the managed aircraft, when the outcome of all the weaknesses and potential failures which may exist in the other parts of the ATM System have been taken into consideration.

This implies that applying the worst case scenario means that one can not assume rely solely on chance to avoid an accident.

Tolerability of effects

The rationale for the calculation of ESARR 4 quantified elements can be found in SRC POLICY DOC 1 "ECAC Safety Minima in ATM". Quantitative targets were developed at ECAC level, taking into account both the ECAC ATM 2000+ Strategy and JSSI safety objectives.

Notes;

1) A difficulty experienced in interpreting the absolute targets of ATM 2000+ was the expected variation, mainly growth, of traffic over the years; this traffic increase was addressed by establishing an assumption on the anticipated traffic growth over the years of operations of the ATM system and by deriving from the absolute safety targets the relative safety targets expressed in terms of 'per Flight Hour'[24].

2) Professional judgement was used to determine the maximum acceptable ATM direct contribution to accidents; an historical baseline over a time-span of 20 years was selected to confirm the credibility of the expert judgement on past identified ATM direct contribution to accidents and future acceptable targets.

[24] *Other units can be used such as 'per movement' or 'per operational units'.*

In this first release of ESARR 4 and its Appendix A;

- the quantified elements may not necessarily apply to airspace where there is no commercial transport aviation,
- only the maximum tolerable ATM direct contribution to accidents is being included in the risk classification scheme, and
- the quantified targets are applicable to the global ATM system (human/procedure/equipment).

The rationale is that;

- targets for ATM indirect contribution to accidents,
- targets for ATM incidents, and
- targets for ATM specific occurrences …

… could not be developed for ECAC as no reliable statistical data on those occurrences could be collected at ECAC level to provide a good enough level of assurance that related targets would be realistic. It would have been unreasonnable to mandate those lower level targets at regulatory level.

This implies that the quantitative definitions for the safety objectives associated with the maximum tolerable probabilities of ATM contributing to incidents of severity class 2, 3, 4 and 5 in the ECAC region remain to be determined at national regulatory level, due to a lack of consistent and reliable safety data on ATM past occurrences at European level

This implies that the ATM risk classification scheme of Appendix A should be refined at State level;

- with targets for all classes of incidents, based among other things[25] on national statistics, if available (if not, and pending their availability when ESARR 2 has been fully implemented, documented and reasonable assumptions may need to be made when deriving such targets),
- for general aviation; and as necessary, and
- for various phases of flight.

Note: SRC DOC TBD documents mechanisms for States to develop their national safety minima in ATM and related risk classification scheme.

An ATM service provider, in order to deal with specific constituent parts of the ATM system (e.g., modification of displays) may also not use directly the top level national ATM risk classification scheme to assess the severity of hazards related to such a change. It may need to develop a scheme consistent with the top level one that it adequately reflects the operational environment of the system under consideration (e.g. interfaces with other systems, phases of flight and classes of airspace).

The rationale for ESARR 4 not providing guidance to do so is that there is a need to analyse the entire ATM System, and understand how the specific system is going to be used and in which context, to be able to determine how it will affect overall safety.

[25] *Complementary means may include using professional judgement, or adopting an order of magnitude between classes equivalent to those of another States, with more reliable statistics.*

This potentially implies for the ATM service provider,

- the redefinition of the severity categories such that they are meaningful in the context of the system under consideration, and

- the accommodation of mitigation in other sub-systems for events in the system under consideration which may lead to a hazard.

This implies for the ATM safety regulator;

- to assess the acceptability of the scheme proposed by the provider and its consistency with the ATM risk classification scheme applicable nationally, and

- to verify that traceability of requirements across systems is well maintained throughout the life cycle of the ATM System and of its constituent parts.

Apportionment of ATM Safety Minima and derivation of safety objectives

The text and quantitative levels given in ESARR 4 (and in equivalent national safety regulatory requirement) only refer to the classification of the overall ATM safety performance ECAC-wide and are not directly applicable to the classification of individual risks.

This implies that the overall target (of minimum) level of safety has to be allocated among/apportioned to all the top-level risks identified in the realm of the state's responsibility. Thus, the maximum probability of a single hazard will usually be much smaller than the maximum probability derived from the overall minimum level of safety.

There is indeed a practical difficulty with the ESARR 4 scheme in determining safety objectives for the constituent parts of the ATM system as required under 5.2 (b). While the scheme in Appendix A sets safety objectives for ATM induced accidents and incidents, it does not lead to an approach for determining the quantitative relationship between these and ATM hazards and failure conditions.

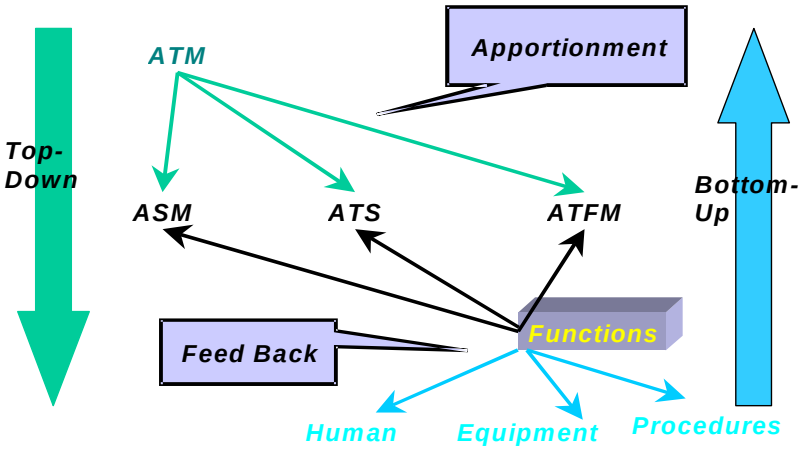
The rationale is that ESARR 4 remains at a high level and, being a regulatory requirement does not mandate a specific architecture for the ATM System. Additionally, ESARR 4 can not mandate a specific approach to deriving safety objectives and requirements as there may be more than one solution. Finally, there is no such thing today as an identified reliable causality model for accident which would help determine such relationship, at least at regulatory level.

The pros of this approach is that ESARR 4 remains ”objective” driven, and leaves full flexibility to those demonstrating compliance with its intent. *(Note: The con of this approach, however, is that ESARR 4 does not provide explanations on **how** it can be implemented).*

This implies that, to set safety objectives to specific hazards, a method of apportionment of the overall probability and /or a derivation of the top level quantified target down to the lower levels such as functions or elements of the ATM System (equipment, people, procedure) has to be developed. The development of such method falls within the remit of the ATM System designer(s). It will be left to the ATM service provider to give a robust argument for any particular application of ESARR 4.

This apportionment may be done in different ways, per phase of flight, per type of risks/accident, per ATM service/function, assuming a maximum of hazards in ATM which will have the potential to lead an ATM accident[26], or a combination thereof.

Related detailed approach will need to be assessed and accepted by the safety regulatory authority.



(Fig 2:- Apportionment of total ATM Risk)

Units

The rationale for using the units 'Flight /Hour' and 'per movement' in ESARR 4 is that these are the most commonly used units when both aircraft and ATM are considered.

Additionally, these units are used within ICAO for specific ATM related risks.

It is recognised that other units would need to be defined depending on the ATM system and sub-system under consideration.

This implies that ESARR 4 does not mandate any units, leaving the ATM provider to propose one, depending on the scope and purpose of the ATM system or sub-system under consideration.

It is expected that apportionment of safety objectives and related allocation of safety requirements to the ground part of the ATM system also requires further work to determine the appropriate units, depending on context. In doing so, care should be taken to the fact that one flight may cross more than one unit, sector or ACC in one hour.

[26] *With adequate justifications and means to verify over time that assumptions are correct.*

Safety Management Considerations

One should not oppose implementing ESARR 4 and the use of safety management considerations (such as ALARP[27]). Indeed such SMS practices and tools are considered to be a safety management activity to be carried out within **safety regulatory minima.**

Indeed, once the safety regulatory minima are demonstrated, ESARR 4 also requires that additional safety improvements be implemented in some risks areas following some kind of safety benefit analysis. This aims at focusing on safety areas where there may be additional safety benefits to be gained.

Aviation harmonisation

There are a number of safety targets across the aviation industry, most of them addressing specific purposes and specific risks (refer to SRC DOC 1, Edition 1.0).

The main conclusion of SRC DOC 1 is that when comparing different safety targets/minima, it is absolutely necessary to identify their respective scopes and assumptions;

- ICAO for example addresses specific risks and does not specify any airspace TLS which would be valid worldwide or on a regional basis. ICAO Target Levels of Safety (TLS) are often based on historical baseline which are world-wide, not European based, and rely on a lot of assumptions, which are not always documented, nor valid everywhere;
- Harmonisation of ESARR 4, Appendix A-2 with the quantitative targets of FAR/ JAR 25[28] is difficult and may be irrelevant as the scope and applicability of the two risk matrices are different. (Refer to SRC DOC 1 "Safety Minima Study", Ed 1.0, which identifies the rationale for JAA/FAA quantification levels and related scope of application[29]);
- Some requirements in JAA AMJ[30] 25.11 have been developed based on past experience and assuming a "traditional ATC environment". JAA AMJ 25.11 may need to be revisited in the light of new ATM System and environment as well as on the increasing reliance of ATM on airborne components. The assessment of ATM related risks are complementary to that of JAA's assessments of aircraft design, operations and maintenance's risks.

(Space Left Intentionally Blank)

[27] *As Low As Reasonably Practicable.*

[28] *AC/AMJ 25.1309*

[29] *AMJ 25. 1309 deals with the design requirement for aircraft equipment only (which is considered to cover 10% of the causes of catastrophic accidents) assuming the aircraft is isolated. AMJ 25. 1309 deals with the design requirement for aircraft equipment only (which is considered to cover 10% of the causes of catastrophic accidents) assuming the aircraft is isolated.*

[30] *Advisory Material Joint.*

6.3.4. Future Development

Once a limited number of categories of environment of operations have been identified across ECAC (or even world-wide) together with practical experience in the assessment of effects of typical ATM hazards/Failure Conditions and related severity, more guidance to regulators may be developed for them to develop a more refined view on the acceptability of the proposed severity and associated rationale[31].

The risk classification scheme of ESARR 4 will be populated with quantified definitions for classes 2, 3, 4 and 5. These will be included in a revised version of ESARR 4 once enough and consistent safety data have been collected by EUROCONTROL, which are compliant with the requirements outlined in ESARR 2. (*Note: Meanwhile, these quantitative definitions must be determined at national level based on past and reliable evidence on numbers of ATM related incidents, unless national statistics are not reliable).*

EUROCAE is revisiting its standard ED78A[32] and developing air-ground safety requirements related to specific operational concepts and environment of operations. The SRC has assessed to which extent ED78A can be recognised as a means of compliance with ESARR 4 (see EAM 4 / AMC 2 and SRC Document 20).

Co-ordination work is also necessary between EUROCONTROL SRC and the JAA to take into account ATM and ESARR 4 in the development of future versions of JAA.AMJ 25.11 as well as deliverables of JAA CNS/ATM.

Once enough hazards have been analysed and associated rational or severity classification well documented and collated in a structured manner, once national safety reporting schemes compliant with ESARR 2 have allowed for consistent safety data to be collected and analysed, it should become feasible to initiate a study to develop an approach for determining the quantitative relationship between the scheme in Appendix A (which sets safety objectives for ATM induced accidents and incidents) and ATM hazards and failure conditions.

6.4 Section 5.2.1 C

6.4.1 General

It requires the implementation of a risk assessment and mitigation process which includes;

- determination of a risk mitigation strategy for risk bearing hazards;
- determination and validation of safety requirements;

(Space Left Intentionally Blank)

[31] *A database of hazards, severity classes and associated rationale could be developed.*

[32] *Guidelines for the approval of ATS supported by data communications.*

6.4.2 Requirement

The requirement states that "*the hazard identification, risk assessment and mitigation processes shall include;*

c. the derivation, as appropriate, of a risk mitigation strategy which;

(i) specifies the defences to be implemented to protect against the risk-bearing hazards[33]*,*

(ii) includes, as necessary, the development of safety requirements[34] *potentially bearing on the constituent part under consideration, or other parts of the ATM System, or environment of operations, and*

(iii) presents an assurance of its feasibility and effectiveness[35]*.*

(Note: It is considered as essential that the activities depicted in a), b), c) and d) are fully co-ordinated between those parties responsible for developing and implementing the safety requirements bearing on the constituent parts of the ATM System). See 5.1 (b) above.

(Note: It is recognised that a combination of quantitative (e.g. mathematical model, statistical analysis) and qualitative (e.g. good working processes, professional judgement) arguments may be used to provide a good enough level of assurance that all identified safety objectives and requirements have been met).

6.4.3 Rationale and Implications

Risk bearing hazards

The rationale is that there is no regulatory obligation to add defences in the ATM System for risks which are already within the allocated safety objectives or for hazards which were not classified in classes 1, 2, 3 or 4. Indeed, too much efforts or focus of those non risk bearing hazards may distract from areas and risks where they is an immediate regulatory and safety need to act.

This implies that priority will be given to higher risks when implementing defences in the ATM System.

Safety requirements[36]

The rationale is that the intended system design, as initially thought, may not meet allocated safety objectives. The initial design and related probabilities of hazards/failure conditions need to be assessed against allocated safety objectives and this may lead to the introduction of changes to the initial design if the actual probabilities of specific hazards/failure conditions can not be shown to meet the defined safety objectives, and/or if additional safety management considerations apply.

---

[33] *To meet the safety objectives, and potentially to reduce and/or eliminate the risks induced by identified hazards.*

[34] *These safety requirements would be identified by the user of the system within the relevant standards and would need to be assessed, accepted and implemented prior to any operational use of the constituent part of the ATM system under consideration.*

[35] *The depth and scope of the analysis may depend on the types of functions performed, the severity of the effects of the hazards, and the complexity of the constituent part of the ATM system under consideration.*

[36] *As defined as per ESARR 4 "A risk mitigation means, defined from the risk mitigation strategy, that achieves a particular safety objective. Safety requirements may take various forms, including organisational, operational, procedural, functional, performance, and interoperability requirements or environment characteristics."*

Safety requirements will then have to be determined to either suppress some risks, reduce their probability of occurrence and/or mitigate their effect. This risk mitigation strategy will be derived after a detailed analysis of the potential failure modes inherent to the proposed design and should ultimately enable the revised design and related operating modes to meet the defined safety objectives.

Safety requirements may bear on the part under consideration but also on other parts of the ATM system. Similarly, assumptions placed on the environment of operations and used in the assessment of severity and related allocation of severity class becomes safety requirements.

An appropriate specification of safety requirements expressed either in a quantitative[37] or qualitative[38] way is essential.

This implies that safety requirements will result from the apportionment of safety objectives to the various system elements in order to enable the proposed design and operating modes to meet the defined safety objectives, hence to operate within tolerable safety minima.

Feasibility and effectiveness

The rationale is that various options may be eligible as safety requirements. The selection of the best options should take as a minimum account of their feasibility and effectiveness as well as of their relative added safety value. Indeed, there may be a tendency at the early days of implementing ESARR 4, to propose the implementation of procedures to control hazards occurring in equipment for example. However, such procedure can be accepted by the ATM safety regulator as a mitigation means only it is has been shown to be feasible and effective in the environment of operations assumed, under the worst credible case.

This implies that the ATM safety regulator should verify that safety requirements are validated to show that they are feasible and effective. Simulations, performance measurements etc are tools which can be used in that validation exercise.

6.5 Section 5.2.1 D

6.5.1 General

It requires the implementation of a risk assessment and mitigation process which includes;

- demonstrate that implemented system meets (and will continue to meet) safety objectives and requirements.

(Space Left Intentionally Blank)

[37] *Traditional measures have included the specification of reliability, availability, continuity, maintainability, recoverability, accuracy etc.*

[38] *In many areas, where people, procedures and software are involved, qualitative values or codes of practices/processes will need to be established.*

6.5.2 Requirement

The requirement states that "*the hazard identification, risk assessment and mitigation processes shall include;*

d. verification that all identified safety objectives and safety requirements have been met:

(i) prior to its implementation of the change,

(ii) during any transition phase into operational service,

(iii) during its operational life, and

(iv) during any transition phase till decommissioning.

(Note: It is considered as essential that the activities depicted in a), b), c) and d) are fully co-ordinated between those parties responsible for developing and implementing the safety requirements bearing on the constituent parts of the ATM System). See 5.1 (b) above.

(Note: It is recognised that a combination of quantitative (e.g., mathematical model, statistical analysis) and qualitative (e.g. good working processes, professional judgement) arguments may be used to provide a good enough level of assurance that all identified safety objectives and requirements have been met)."

6.5.3 Rationale and Implications

Verification of objectives and requirements

The rationale is that safety cannot be demonstrated if there is no verification that the ATM System and system elements, as implemented meet all identified safety objectives and safety requirements, with an adequate level of assurance.

This implies that the ATM safety regulator must check that implementation of all safety requirements and objectives have been be verified with an acceptable level of assurance/confidence and that related assurance/evidence exist.

Complete life cycle

Refer to section 2.2.3.

This implies that verification of compliance with safety objectives and requirements is an on going process, conducted throughout the implementation of system elements, their integration, the transition to operations, operations and maintenance phases. It ends at decommissioning/replacement of the system. Therefore, the ATM safety regulator should check that those responsible for operations and maintenance of the system have committed one way or another and before transfer to operations, to the continuing implementation and verification of the safety requirements they are responsible for.

(Space Left Intentionally Blank)

Quantified and qualitative evidence

ATM service providers do not have to demonstrate compliance to safety objectives and requirements by using only mathematical evidence. It is recognised that a combination of quantitative (e.g. mathematical model, statistical analysis) and qualitative (e.g. good working processes, professional judgement) arguments may be used to provide a good enough level of assurance that all identified safety objectives and requirements have been met

Obviously, ATM safety regulator can aceept both qualitative and quantitative evidence.

The rationale is that for procedures, personnel and software, it may not be feasible to demonstrate in a quantified manner compliance with quantified objectives.

This implies that ATM safety regulators may have to state at one stage that specific standards (such as software related standards, or competency schemes) are recognised as achieving a certain level of safety, and to implement a scheme whereby they can verify this over time and be in a position to have those standards modified and improved in the light of experience.

Various levels of demonstration

ESARR 4 note 8 states that;

"*The depth and scope of the analysis may depend on the types of functions performed, the severity of the effects of the hazards, and the complexity of the constituent part of the ATM system under consideration*".

Indeed, even if ESARR 4 is applicable to all changes, it is certainly not intended to require an extensive risk assessment (and extensive safety argument) for every single minor modification of parts of the system (like applying a minor software patch or changing a published radio frequency-the only way to determine that a soft patch is minor is by doing a safety assessment, but related workload and documentation should remain limited). Equally, it is certainly not intended to require an extensive analysis to demonstrate compliance with safety objectives and requirements for lower risks. Obviously, the contents of the safety argument may be limited in certain cases, and well developed in other cases.

This implies that it will be up to the safety regulator to progressively, and according to its safety oversight principles and procedures, to develop criteria for requiring a certain level of verification per category of changes and per category of risks (refer to EAM 4 / GUI 2 "ESARR 4 Safety Oversight").

6.5.4 Future Developments

In the future, once practical experience in the implementation of ESARR 4 has been gained, more guidance to regulators may be provided for them to develop a more refined view on the acceptability of proposed evidence and related safety regulatory effort.

Also refer to EAM 4 / GUI 2 dealing with ESARR 4 Safety Oversight.

6.6 Section 5.3

6.6.1 General

It requires the collection and collation of all safety demonstration and evidence and its documentation.

This document shall include;

- Results of risk assessment and mitigation;
- Evidence of risk assessment and mitigation;
  - To demonstrate that ATM system will remain tolerable safe
  - With traceability

6.6.2 Requirement

The requirement states that;

"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 correct and complete arguments are established to demonstrate that the constituent part under consideration, as well as the overall ATM System are, and will remain, tolerably safe[39] including, as appropriate, specifications of any predictive, monitoring or survey techniques being used, and*
- *that all safety requirements related to the implementation of a change are traceable to the intended operations/functions. "*

6.6.3 Rationale and Implications

ESARR 3 requires "safety records" to be maintained. Risk assessment and mitigation was seen as so essential that a specific set of documentation is required for that process.

The purpose of such a documented safety argument is to provide assurance that each system element as implemented meets its safety requirements with an adequate level of assurance/confidence and that the system as implemented will meet its safety objectives throughout its operational life time.

The rationale is that proper documentation of results and evidence, with traceability to intended functions/environment of operations will enable the ATM service provider;

- to check the overall consistency of the safety approach adopted and of the final outcomes, and
- to assess more easily any future modifications to the system under consideration.

[39] *i.e. meeting allocated safety objectives and requirements.*

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 imbrication 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.

What is essential to the safety regulator is to verify;

- the clear traceability between the analysis and outcome of each risk assessment and mitigation process (i.e. list of hazards, safety objectives and requirements, associated rationale and evidence of implementation),
- the consistency between all the outcome/assumptions in all the set of safety arguments maintained by the service provider, and
- the clear traceability and consistency between the safety argument documentation and the documents reflecting the actual implementation and operation of the ATM System (i.e. system specifications, training manual, operational documentation).

7. SECTION 6 – IMPLEMENTATION

7.1 General

ESARR 4, Section 5 '*Implementation'*, specifies the date by which ESARR 4 shall be implemented at national level.

7.2 Contents

Section 6.1 states that;

"The provisions of this requirement are to become effective within three years from the date of adoption by the EUROCONTROL Commission".

7.3 Rationale and Implications

The rationale is that State will need enough time to implement ESARR 4 at national level. At the same time, significant changes are being considered for the ECAC airspace and it is essential that they are subject to a formal risk assessment and mitigation process.

In other words, ATM safety regulators are given three years to;

- Have their national legislative arrangements modified as required,
- Develop, promulgate and enforce ESARR 4 in their national safety regulations,
- Develop fully an ESARR 4 safety oversight function,

ATM service providers are given three years to;

- Develop and document in their SMS documentation risk assessment and mitigation procedures, compliant with the national regulations;
- Implement those procedures fully for any changes to the ATM System under their managerial control.

Note: More detailed tasks and related milestones are provided in ECIP 2001.

8. SECTION 7 – EXEMPTION

8.1 General

It specifies the rules for exemptions.

8.2 Contents

The requirement states that no exemption is allowed.

8.3 Rationale and Implications

The rationale is that no change to the ATM System can be implemented without a clear indication that safety won't be jeopardised. Indeed, if only some changes to the ATM system were to be subject to ESARR 4, there would be no other mechanism which would allow to rule out a change on the ground that it has no safety impact.

However, even if ESARR 4 is applicable to all changes, it is certainly not intended to require an extensive risk assessment for every single minor modification of parts of the system (like applying a minor software patch or changing a published radio frequency-the only way to determine that a soft patch is minor is by doing a safety assessment, but related workload and documentation should remain limited).

This implies that if all changes to the ATM System are subject to ESARR 4, obviously, the level of analysis and demonstration of evidence will be adjusted to the significance of the changes and the severity of the risks.

Similarly, the safety regulator won't enforce the same level of safety oversight to all changes (refer to EAM 4 / GUI 2 'ESARR 4 Safety Oversight').

(Space Left Intentionally Blank)

9. SECTION 8 – ADDITIONAL MATERIAL

9.1 Overview

Section 5 '*Implementation'* of ESARR 4 includes advisory material and is formed by three sub-sections and one appendix;

- 8.1
- 8.2
- 8.3
- Appendix B - Terms and Definitions-Glossary

9.2 Section 8.1

9.2.1 General

It deals with existing parts of the ATM System and mentions evidence that those meet tolerable safety levels can be demonstrated based on feed back from experience.

9.2.2 Contents

Section 8.1 states that;

"For existing parts of the ATM System, an analysis based on available historical data, such as safety occurrence (i.e. accident, incident, ATM specific occurrence) statistics, human errors, equipment faults, mostly based on system safety monitoring and occurrence reporting schemes may contribute evidence to the safety assurance process, hence complementing the safety analysis depicted in section 5 of this requirement."

9.2.3 Rationale and Implications

The rationale is that it is not economically realistic or feasible to require all existing ATM system to be formally assessed by 2004 according to ESARR 4. However, this means that alternative means to show that safety is acceptable exists, such as feed back from past operations.

Additionally, this has also been the approach adopted in the past in aircraft certification.

This however implies that the existing reporting scheme provides for enough reliable data to make such a judgement.

9.3 Section 8.2

9.3.1 General

It provides some general guidance and ideas on how to show compliance with some parts of ESARR 4.

9.3.2 Contents

Section 8.2 states that;

"*EATMP SAM SAF ET1.ST03.1000-MAN- (Ed 1.0) is considered as a useful guidance when implementing this safety regulatory requirement*[40]*. The applicability of the methodology would need to be specified at the beginning of any risk assessment and mitigation process*. "

(Note: Future revisions of that document are also to be foreseen, to encompass assessment of the human, equipment and procedures elements and develop further the system safety assessment process beyond the Functional Hazard Assessment).

Link with software qualification

The safety objectives allocated to each hazard drive the determination of specific means to attain the proper level of confidence in the success of implementing the mitigation strategies and related safety requirements.

These means may include a set of different levels of constraints being set on specific software elements of the ATM System.

Safety monitoring and data collection

Safety monitoring and data collection mechanisms could be specifically developed as an enabling tool to the validation of the safety assumptions and requirements as identified during the risk assessment and mitigation processes, including hazard identification, as well as the assessment of the safety added value of the programme. For example, such mechanisms could be used for the validation of theoretical data such as Mean Time Between Failures) and models (such as fault tree, reliability flow charts) used in the safety assessment and safety assurance processes.

In addition, safety monitoring and data collection mechanisms consistent with the provisions of ESARR 2[41]*, could also be developed as enabling tools to define global safety indicators in order to control and monitor the safety levels reached in operation by the ATM System.*

Safety monitoring should therefore be seen as a complementary means of qualification before and during operational use."

9.3.3 Rationale and Implications

EATMP Air Navigation Safety Assessment Methodology

The EUROCONTROL Safety Regulation Commission (SRC) has the task of ensuring the uniform implementation of ESARR 4 across Europe, hence the need for SRC to recognise a number of acceptable Means of Compliance to help this uniform implementation of ESARR 4.

[40] *WARNING: The terminology used in that guidance is not fully consistent with that used by the Safety Regulation Commission. The compliance of this guidance with ESARR 4 still needs to be assessed by SRC.*

[41] *ESARR 2 'Reporting and Analysis of Safety Occurrences in ATM'.*

The EATMP Safety Assessment Methodology is a useful harmonised set of working practices for ANS providers to undertake a safety assessment of proposed changes to their System.

The EATMP Safety Assessment Methodology has been assessed by the SRC as a potential means of compliance to all or part of ESARR 4.

The EATMP Safety Assessment Methodology currently addresses only part of what is required within the scope of ESARR 4 as it only enables to set up a list of safety objectives. Further releases of the document should cover the whole life cycle of a project.

ESARR 4 and the EATMP methodology also differ in terms of scope as the EATMP methodology does not require a total system approach.

This implies that for providers of ATM services to use this EATMP methodology as one means to meet part (or all) of the requirements contained in ESARR 4, the methodology needs to be adjusted and complemented (refer to EAM 4 / AMC 2 and SRC Document 12).

Link with software qualification

The rationale is that for software, there is no mechanism which would allow to demonstrate in a quantified manner that quantified safety objectives are being met by software in a specific environment.

The SRC is finalising the development of ESARR 6.

In addition, the ATM safety regulatory community will have to recognise a number of specific standards or practices as acceptable to attain the proper level of confidence in the success of implementing software according to different quantified safety objectives (refer to what was done by the FAA and the JAA with DO178C/ED12C).

This implies an equivalent recognition for specific processes/working practices whenever no quantified demonstration is feasible (e.g. training standards, procedure development, etc.).

Safety monitoring and data collection

The rationale is that any model (e.g. Collision Risk Model) used in risk assessment and mitigation must be validated one way or another, and real data could contribute significant validation.

Additionally, some safety assumptions also need to be validated with real data. Examples include level of aircraft equipage, density of traffic per sector, probability of aircraft deviating from their Flight Level etc.

This implies that safety data monitoring will most of the time form part of the processes to be put in place for changes to the ATM System, but also permanently, according to ESARR 2.

This finally implies that safety monitoring and data collection compliant with ESARR 2 (and HEIDI taxonomy) should form part of any safety argument.

9.4 Section 8.3

9.4.1 General

It refers to Appendix B.

9.4.2 Contents

It refers to the ESARR 4 glossary of terms and definitions.

9.4.3 Rationale and Implications

The rationale is that ESARR 4 can not be read consistently without a set of terms and definitions.

Additionally, across the industry, there are many ways of defining and understanding a number of safety related terms, such as ‘hazard’ or ‘risk’. These terms have not yet been fully standardised in aviation.

Furthermore, specific terms may need to be defined and used in a specific manner in a safety regulatory context. This is why some terms used in SRC may not all match with definitions used in other documents.

Note: SRC DOC 4 includes a set of terms and definitions used throughout the ESARRs. However, as ESARR 4 was approved before SRC DOC 4, some definitions in ESARR 4 may differ. It is however intended that all definitions across ESARRs be ultimately made consistent.

(End of Document)