EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

ESARR ADVISORY MATERIAL/GUIDANCE DOCUMENT
(EAM/GUI)

EAM 4 / GUI 2

ESARR 4 AND RELATED SAFETY OVERSIGHT

Edition	**:**	**4.0**
Edition Date	**:**	**21 March 2006**
Status	**:**	**Released Issue**
Distribution	**:**	**General Public**
Category	**:**	**ESARR Advisory Material**

F.2 DOCUMENT CHARACTERISTICS

TITLE		
EAM 4 / GUI 2 **ESARR 4 and Related Safety Oversight**		
Document Identifier	**Reference**	EAM 4 / GUI 2
eam4gui2_e40_ri_web	**Edition Number**	4.0
	Edition Date	21-03-2006

Abstract

The previous versions of EAM 4 / GUI 2 were produced before the approval of ESARR 1 and the entry into force of the SES Regulations. As such, their enactment has necessitated a full review of the document in order to ensure its consistency with this new regulatory material.

As a first step in this review process, the SRC has produced this version of EAM 4 / GUI 2 to include a new table with guidance on the criteria for the assessment of compliance with ESARR 4. This table replaces the former highlevel checklists included in previous versions of the document.

Apart from the new table, no other contents have currently been modified. However, it is intended to produce a fully revised version of EAM 4 / GUI 2 to provide NSAs with guidance on the safety oversight of ESARR 4-related requirements.

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 INFORMATION					
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	☐

COPIES OF SRC DELIVERABLES CAN BE OBTAINED FROM

Safety Regulation Unit
EUROCONTROL
Rue de la Fusée, 96
B-1130 Bruxelles

Tel: +32 2 729 51 38
Fax: +32 2 729 47 87
E-mail: sru@eurocontrol.int
Website: 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)	21.03.2006
Head Safety Regulation Unit (SRU)	***signed by Peter Stastny*** (Peter STASTNY)	21.03.2006
Chairman Safety Regulation Commission (SRC)	***signed by Ron Elder*** (Ron ELDER)	21.03.2006

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	01-Oct-01	New working draft including initial contents for all sections. Circulated to SRU for review and as an input to 1st progress meeting (08/10/01).	All
0.03	27-Nov-01	Draft version incorporating feed back from SRU (harmonisation with SRC POLICY DOC 3). All Sections updated. Circulated to SRU and RTF for comments.	All
0.04	25-Jul-02	New Draft incorporating comments received from SRU and RTF and SRC.	As noted by change marks
0.05	18-Oct-02	Update as a result of ICAO comments for RTF Working Group approval. New document format.	All
0.1	18-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
2.0	25-Jun-03	Terminology clarification and error correction in Appendix B.	As noted by comment marks
2.01	11-Aug-03	Update of document cross references**.** Expansion on guidance for minor and minor changes (2.2.3.1)	All
2.02	15-Sep-04	Update after RTF.27	As noted by comment marks
2.03	02-Nov-04	Update after RFC No. 0424.	
2.1	08-Nov-04	SRU quality check. Document status amended to draft issue and sent to SRC for formal consultation.	All

F.4 DOCUMENT CHANGE RECORD

EDITION NUMBER	EDITION DATE	REASON FOR CHANGE	PAGES AFFECTED
3.0	05-Jan-05	Minor changes as a result of SRC consultation (RFC No. 0434). Document formally released.	38, 50
3.1	06-Feb-06	Review to check consistency with Single European Sky and ESARR 1 requirements.	New Appendix B
3.2	03-Mar-06	New version produced after SRC consultation (RFC No. 602).	2, 7
4.0	21-Mar-06	Document formally released.	-

(Space Left Intentionally Blank)

F.5 CONTENTS

(Space Left Intentionally Blank)

F.6 EXECUTIVE SUMMARY

The previous versions of EAM 4 / GUI 2 were produced before the approval of ESARR 1 and the entry into force of the Single European Sky (SES) Regulations.

As such, their enactment has necessitated a full review of the document in order to ensure its consistency with this new regulatory material.

As a first step in this review process, the Safety Regulation Commission (SRC) has produced this version of EAM 4 / GUI 2 to include a new table (Appendix B) with guidance on the criteria for the assessment of compliance with ESARR 4. This table replaces the former highlevel checklists included in previous versions of the document.

The new table is primarily intended to provide National Supervisory Authorities (NSAs) with guidance to support the development of their strategy to verify the implementation of ESARR 4-related requirements in the context of the certification and on-going oversight of Air Navigation Service Providers (ANSPs) against the Common Requirements established in Commission Regulation (EC) 2096/2005. As such, the table is also referred to in EAM 1 / GUI 5 ‘ESARR 1 in the Certification and Designation of Service Providers’.

Apart from the new table, no other contents have currently been modified. However, it is intended to produce a fully revised version of EAM 4 / GUI 2 to provide NSAs with guidance on the safety oversight of ESARR 4-related requirements.

(Space Left Intentionally Blank)

1. GENERAL INTRODUCTION

1.1 Introduction

1.1.1 Purpose

The purpose of this document is to provide guidance to States in establishing safety oversight for assessing compliance with the provisions of ESARR 4 "Risk Assessment and Mitigation in ATM", Edition 1.0.

The establishment of safety oversight with regards to ESARR 4 is intended to ensure that the national ATM System is only allowed to be modified after a risk assessment and mitigation exercise has demonstrated that the ATM operations will remain within tolerable safety levels.

This document also allows emphasising the obligations and responsibilities of States for effective safety oversight in Air Traffic Management, at least in so far as ESARR 4 related regulations and safety oversight are concerned.

While still aiming at ensuring a harmonised implementation of ESARR 4 across ECAC States, this document does not intend to provide one exclusive model for ESARR 4 safety oversight:

- It includes a number of recommendations which are either generic or conversely, only valid in certain circumstances; and
- It depicts a number of safety regulatory tools which could be combined and tailored to specific needs, into unique solutions to suit a State's specific situation.

Note: As ESARR 4 strengthens the new provisions of Annex 11 in the area of safety assessment[1], this document could also be used by States to verify compliance with related ICAO standards (and recommended practices).

1.1.2 Scope

The scope of this document is confined to the safety regulatory aspects of ATM, inclusive of all its elements; people, procedures[2] and equipment[3]. It excludes the subjects of security, regularity and efficiency when those are not directly safety related.

It also excludes the regulatory aspects of issuing licenses to radio aeronautical station.

This document does not contain all necessary guidance on the provision of a safety oversight function. In particular, ESARR 1 and SRC Policy Document 1 should also be used as well as the other ESARR and guidance materials.

---

[1] *Refer to Amendment 40 to ICAO Annex 11*

[2] *Including airspace design and procedures*

[3] *Hardware, software and integration thereof*

In a safety regulatory regime, there are two major elements of regulations which need to be operated: 'Rule-making' and 'Safety Oversight'. This document only deals with the Safety Oversight[4] functions of the designated authority, even if some necessary statements refer to rule making.

If the prime focus of this document is the safety oversight of changes to the national ATM System against ESARR 4 and related approval process, some guidelines are also provided when such a national safety approval is expected to rely on an existing SRC harmonised view on the acceptability of a European programme.

1.1.3 Safety Oversight Functions

ESARR 4 safety oversight is applied in respect of proposed new ATM operations, up to the point of introduction into operational use, but also during its operational life, till "decommissioning". It is also applied to all types of proposed changes to an existing ATM operation, either in the form of new developments, enhancements or corrections.

In some cases, ESARR 4 safety oversight can be in the form of 'initial safety oversight', leading to 'safety regulatory approvals'. In other cases, ESARR 4 safety oversight can be in the form of 'on going safety oversight'. (Refer to SRC Policy Document 3 and ESARR 1).

Both 'initial safety oversight' and 'on going safety oversight' of ESARR 4 are addressed in this document.

1.2 Context

The implementation of ESARR 4 safety oversight at national level requires, in one form or another, the establishment of a specific function at national level.

This ESARR 4 safety oversight function will most probably be undertaken within a larger State-based organisation, of safety regulatory nature, called throughout this document "designated authority"[5].

The establishment of that designated authority, its roles, functions, safety regulations, resources and related ESARR 4 safety oversight processes may well differ significantly across States. In addition to a number of political, economical, legislative, and cultural factors, options to be selected when establishing the ESARR 4 safety oversight function will need to take into account a number of industry-related parameters such as;

- The national arrangements for ATM service provisions,
- The capacity of the service provider(s),
- The number and size of regulated service provider(s),
- Previous experience in Risk Assessment and Mitigation processes in service provider (s) and within the designated authority itself, and

[4] *Safety Oversight is "The function undertaken by a designated authority to verify that safety regulatory objectives and requirements are effectively met" (Refer to SRC POLICY DOC 3- Ed. 0.03)*

[5] *SRC POL DOC 3 uses the alternative term "ATM Safety Regulator". Both terms are equivalent.*

- The visibility/common past experience the designated authority has acquired over the years on/with the regulated service providers in Risk Assessment and Mitigation.

Some of these criteria are being developed further in subsequent sections.

1.2.1 International Obligations

It is recognised that the harmonisation of safety regulations and standards worldwide is not enough to ensure their uniform implementation across States.

It is the integration of such regulations and standards in the national regulation and practices of States and their timely implementation that will ultimately achieve safety of aircraft operations and Air Navigation provisions world-wide EUROCONTROL Member States will have to ensure that ATM service-providers meet the ESARR 4 safety requirements through appropriate safety regulation and safety oversight.

1.2.2 Designated Authority

A State entity, called 'designated authority' in this document[6] ought to exist and carry out, among other things, ESARR 4 safety oversight. In that process, the necessary legal and/or constitutional powers to ensure compliance with ESARR 4 compliant national regulations must be addressed and this authority ought to be vested with the necessary powers to ensure compliance with those regulations.

In the context of ESARR 4 and in addition to the generic ideas provided in SRC Policy Document 3, the national aviation legislation should also;

- Authorise the designated authority to develop and promulgate national safety minima for ATM which at least meet those specified in SRC Policy Document 1;
- Require the designated authority to be satisfied that all proposed changes to the ATM System can be implemented within at least approved tolerable safety minima for ATM.

1.2.3 Regulatory and Service Provision Context

1.2.3.1 Regulatory Culture

Requirements on how best to establish a designated authority in charge of safety regulatory oversight may vary from States to States.

In the development, adoption, enactment and promulgation of national safety regulations, a State can make a number of choices which govern the type, nature and level of prescription of ATM safety regulations.

ESARR 4 only represents a minimum set of safety regulatory requirements required at European level. If ESARR 4 can be considered as a good balance between objective driven and prescriptive regulation, one State may have decided to add complementary provisions in a more or less prescriptive manner. These potential choices will have an impact on related safety oversight activities.

[6] *Or 'ATM safety regulatory body', or 'Civil Aviation Authority' in other documents.*

In the establishment of the designated authority, the State has also the option of adopting solutions which will govern its role and daily safety oversight activities in the implementation of ESARR 4.

This may range;

- from a stringent regulatory involvement where for example, all potential changes to the ATM System are being systematically under regulatory review and acceptance/approval;
- to an extreme passive role, where for example the holder of an approved Safety Management System (SMS) would be audited once in a while for all SMS related processes, inclusive of the risk assessment and mitigation ones.

A designated authority adopting an extreme passive role is not recommended as it would imply that the service providers are self-regulated. Alternatively, the designated authority, by being over involved, could inhibit the service provider's control of its operations and its safety involvement.

It is recommended to establish at national level a balanced ESARR 4 safety oversight system with due consideration of the industry maturity in safety, and to both the aviation community and the public interest.

1.2.3.2 Institutional Arrangements for ATM Service Provision

The responsibility of ensuring safety within the national airspace rests with the State. The requirement for 'Risk Assessment and Mitigation in ATM' equally applies to government and to commercialised organisations providing ATM services.

Whenever the service provision of ATM is delegated to a commercialised organisation, it is of prime importance that the State retains its overseeing responsibilities and ensures that the service provider complies with ESARR 4.

Even if the service provision remains government-based, the best transparent and robust way of ensuring compliance with ESARR 4 would be to establish a separate function within the administration which would verify initial and on going compliance with ESARR 4, all along the life cycle of the ATM System and related components.

Note: This safety oversight function is different and complementary to the internal verification mechanisms (such as "safety surveys" as per ESARR 3) implemented within the Safety Management System itself.

Whatever the service provision arrangements implemented at national level, it is recommended to establish a separate safety oversight function and a well documented safety oversight system to ensure full compliance with ESARR 4.

(Space Left Intentionally Blank)

1.2.3.3 Capacity of ATM Service Provider

The level of ESARR 4 safety oversight should be dependent upon the capacity and maturity of the regulated service providers in risk assessment and mitigation.

Except in a limited number of States and service providers, we are still in the early days of implementing risk assessment and mitigation in ATM;

- Previous experience in Risk Assessment and Mitigation processes and more specifically in ESARR 4, both in service provider (s) and in designated authorities, is limited,
- Previous experience in implementing ESARR 4, both in service provider (s) and in the designated authorities, is almost nil, and
- Equally, common past experience in ESARR 4 type of implementation, related potential challenges and issues is low, or even non-existent. Designated authorities would therefore benefit from a direct feed back on the implementation of ESARR 4.

This implies that today, the level of maturity of the service provider(s) as well as of the designated authorities in that specialised area of risk assessment and mitigation may still be insufficient.

There is a need for a close interface between the designated authority and the regulated organisation(s) in order to build confidence across the two communities and also support a joint learning process in ESARR 4 type of implementation.

At the early days of ESARR 4 implementation, it is also recommended that designated authorities avoid at all costs adopting a passive safety oversight role and dedicate enough resources and expertise in verifying compliance with ESARR 4 requirements.

Note: When the regulated organisations and designated authorities have acquired enough experience in implementing ESARR 4, the designated authority will be in a position to adopt a less involved safety oversight attitude. This could be the right time to relax the typical criteria used in the past to determine if a safety regulatory oversight action/review is required for a change to the ATM System. Delegation of some safety regulatory approval competence to an approved representative of the service provider could also, at a later stage, be contemplated.

1.3 Regulatory Capacity

1.3.1 Organisation

As already stated, in all States, it will be necessary to establish some form of entity within the government, vested with the necessary authority to ensure that ESARR 4 safety requirements are met[7].

[7] *In Some States, it may be found that this function can be undertaken in a cost effective manner through co-operative arrangements with neighbouring States or regional arrangements.*

The implementation of ESARR 4 safety oversight at national level requires, in one form or another, the establishment of an appropriate organisation, with adequate processes, working procedures and resources. In establishing such an entity, one should give consideration to the recommendations made in previous sections.

However, as the safety oversight activities related to ESARR 4 are only part of a bigger set of safety regulatory functions within a specific national legislative context, no model or detailed recommendations for organisational arrangements are provided in this document.

1.3.2 Processes and Procedures

In section 1.2.3.2, it is recommended to "establish…a well documented safety oversight system to ensure full compliance with ESARR 4".

Such safety oversight system should establish and implement the interface between the designated authority and the ATM service provider(s) in the area of ESARR 4 safety oversight. Recommendations and guidelines for such processes are being developed further in Chapter 2.

In addition, it would be advisable to develop an internal manual within the designated authority, containing;

- instructions to undertake ESARR 4 safety oversight for safety oversight staff to do their task consistently; and
- standard forms and reports structure to be used to document the outcome of any ESARR 4 safety oversight activities.

All these processes and procedures will most probably drive the required budget and staff to perform the ESARR 4 related safety oversight function.

1.3.3 Budget

Refer to SRC Policy Document 3 and ESARR 1 for generic recommendations.

The implementation of an ESARR 4 safety oversight function will require the allocation of a budget, the size of it being dependent upon the volume of work to be handled, and more specifically the;

- number of ATM service providers under ESARR 4 safety oversight,
- frequency and scope of changes being submitted to safety regulatory approval,
- safety oversight processes and procedures in place for ESARR 4, and
- expected average travel length and time required for audits and inspections.

(Space Left Intentionally Blank)

1.3.4 Staff

1.3.4.1 General

Refer to SRC Policy Document 3 and ESARR 1 for generic principles.

The structuring and level of staffing involved in ESARR 4 safety oversight will obviously depend on the volume of work to be handled, and more specifically the;

- number of ATM service providers under ESARR 4 safety oversight,
- frequency and scope of changes being submitted to safety regulatory approval, and
- safety oversight processes and procedures in place for ESARR 4.

1.3.4.2 Recruitment

Refer to SRC Policy Document 3 and ESARR 1 for generic principles.

In addition, SRC Policy Document 3, ESARR 4 Safety Oversight staff should include a combination of safety specialists, as well operational and technical experts, who would over time share and combine their initial know how.

When recruiting, it seems essential to select staff with a wide aviation culture, a sound aviation background, willingness and an ability to keep learning about safety techniques as well as new operational concepts and techniques.

Those chosen to be in charge of any assessment of safety argument, related safety regulatory audit or inspection[8] must possess basic qualification appropriate to those tasks. In particular, they must possess relevant operational and technical expertise and understanding of relevance to the national ATM system.

1.3.4.3 Training

Refer to SRC Policy Document 3 and ESARR 1 for generic principles.

In addition, there should be specialist training for ESARR 4 Safety Oversight staff. Some areas that should be considered for more detailed training are;

- ESARR 4 based national regulation, and rationale;
- Applicable aircraft safety regulation, more specifically applying to CNS/ATM functions,
- Risk assessment and mitigation processes and techniques,
- Recognised Means Of Compliance to ESARR 4,
- New areas of change to the ATM system, and
- Safety occurrence reporting and analysis in ATM.

[8] *SRC POL DOC 3, Appendix 2, includes criteria for qualification of personnel performing safety regulatory audits and inspections.*

1.3.4.4 Harmonised Judgement

It is essential that ESARR 4 safety oversight activities be conducted to a common standard. The development of a manual containing instructions to safety oversight staff will promote standardisation. Standard forms and procedures should also be used to document the outcome of any ESARR 4 safety oversight activities as well as related follow up.

This is even more crucial when beginning the ESARR 4 safety oversight process, as it is essential that the judgement of the staff about the acceptability of specific risks and safety evidence/argument be harmonised. When faced with similar issues, ESARR 4 safety oversight staff should not develop a view completely different from a colleague.

It is therefore essential to implement appropriate mechanisms to share across the ESARR 4 safety oversight team the outcome of past oversight exercise in order to avoid inconsistent judgements being made about similar issues;

- A data base of hazards with allocated categorisation of severity of effect and accepted tolerable risk level (with associated assumptions and rationale) could be developed as a reference tool,
- Sessions with all the staff could be organised to discuss specific issues, such as those related to proposed means of compliance as well as to the risk assessment of new operational concepts and new technology,
- Depending on the size of the ESARR 4 safety oversight team, there could be a need for a focal point charged with the development of views and responses on specific issues, which could then be used by all involved in safety regulatory audits and inspections. The focal point would most probably need to liaise with the staff charged with the development and maintenance of national ESARR 4 compliant safety regulations, and
- Safety reports (from safety regulatory audits and inspections, etc.) could be circulated within the safety oversight team to allow for cross fertilisation and for standardising the regulatory responses

2. SAFETY OVERSIGHT

2.1 Introduction

2.1.1 General Considerations

For transparency and to ease the communication with the regulated service providers, it is recommended to document the safety regulatory procedures and related arrangements established to verify compliance with ESARR 4.

Under those circumstances, both the staff from the designated authority and the regulated organisations will have a common knowledge of what is expected from service providers, and what ESARR 4 safety oversight consists in and leads to.

2.1.2 Regulatory Procedures and Arrangements

Verification of compliance with ESARR4 by ATM Safety Regulators should be performed through regulatory procedures and arrangements established and documented to;

- Ensure **initial safety oversight** undertaken through **safety regulatory approvals** for those;
  - Constituent parts of the ATM System or,
  - Categories of changes to the ATM System,

whose acceptability requires a formal safety regulatory approval before being allowed to be operated.

- Ensure **ongoing safety oversight** undertaken to verify continuous compliance with ESARR 4 in the use of risk assessment and mitigation processes conducted by the ATM service-provider and the results of those processes; and
- Facilitate the use of safety regulatory audits and inspections in both, initial and ongoing, safety oversight processes.

The rights and duties of service providers with respect to audits and inspections carried out by the designated authority should also be documented (e.g. access of auditors to places, documents and evidence).

2.2 Practical Aspects

2.2.1 National Safety Minima[9]

The implementation of ESARR 4 at national level requires that national safety minima for ATM be developed according to the provisions of SRC Policy Document 1. EAM 4 / GUI 1 proposes some guidelines for States to develop those safety minima in a consistent manner.

[9] *In accordance with SRC POL DOC 3, the determination of national safety minima goes beyond safety oversight and forms part of the national safety regulatory responsibility that sets minimum acceptable levels of safety.*

These safety minima should be used to develop a national risk classification scheme according to ESARR 4. EAM 4 / GUI 1 also proposes some guidelines for States to develop their scheme in a consistent manner.

This national risk classification scheme is to be used by national service providers as an input to develop their own scheme, customised to the services they provide. This should, if needed, enable them to determine those safety objectives related to a specific change to the ATM system within their managerial control.

It is recommended to;

- Document the procedures used to derive national safety minima in ATM and associated national risk classification scheme,
- Document the procedures used to update those safety minima and associated national risk classification scheme over time,
- Promulgate the national ATM safety minima and make them available to the national aviation community, and
- Promulgate the national risk classification scheme in the ESARR 4 compliant national regulations.

2.2.2 Scope of Safety Oversight

2.2.2.1 General

Within a safety regulatory approach consistent with the implementation of ESARR 4, the designated authority should ensure that providers assess new systems and changes in ATM before their introduction into operational service.

ESARR 4 applies to <u>all changes</u> to the ATM System (Refer to EAM 4 / GUI 1).

"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"

Equally, it is expected that ESARR 4 safety oversight should apply **to all new systems and all changes** to the ATM System through initial or/and ongoing safety oversight.

2.2.2.2 Safety Oversight Options

A designated authority can not dedicate the same level of safety regulatory efforts to all changes to the ATM System, whatever their safety significance[10]. Some changes and operations/systems also may be subject to a specific approval, others not.

Criteria and conditions driving the level of safety oversight efforts and related procedures must be explicitly specified at national level. Elements/factors which might be taken into account include the level of implementation of ESARR 3 and the maturity of the regulated service provider(s), the resources available for ESARR 4 safety oversight in the designated authority as well as the scope, past experience in similar areas, or level of safety performance of the service provider under consideration.

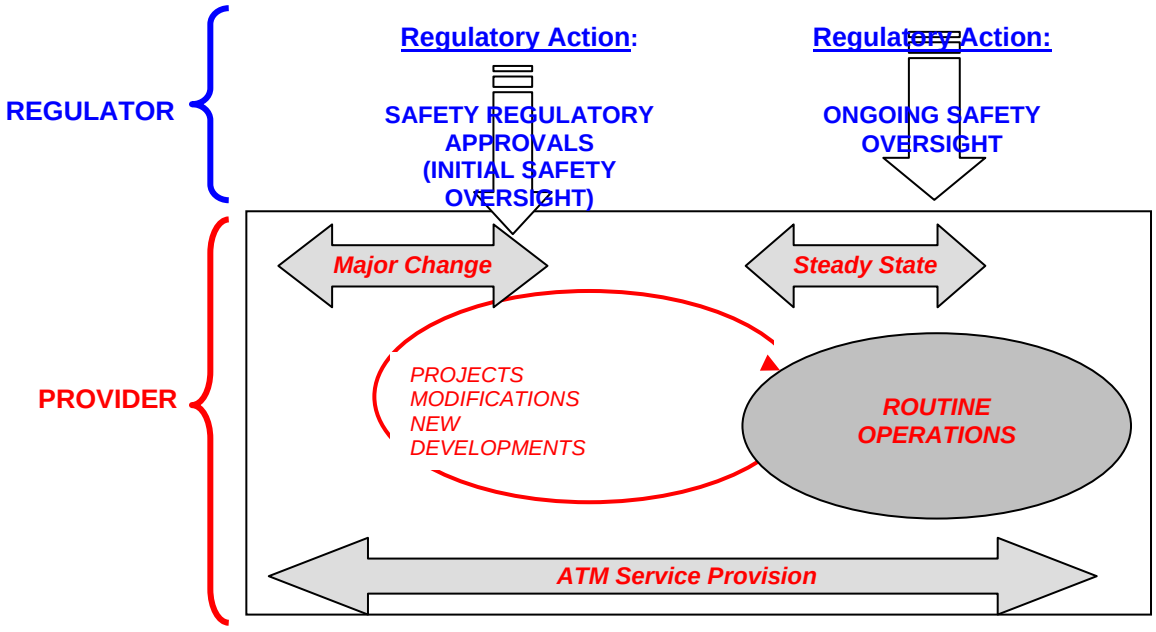
[10] *Refer to Chapter 1.*

Additional operational factors would include the potential for safety impact of the proposed change, as determined by a preliminary Functional Hazard Analysis, the complexity of the change, the existence of not of previous experience in the area covered by the change, and the existence or not of validated international standards.

Similarly, criteria and conditions driving both the issuance of a safety regulatory approval related to a change to the ATM System and its renewal, limitation or suspension must be explicitly specified at national level.

Obviously, different safety oversight options exist and will need to be selected at national level to optimise the benefit of ESARR 4 safety oversight in the national context. Section 2.2.3 describes some safety oversight tools and activities which could be used and combined when developing those options.

It is recommended, for the benefit of both the safety oversight staff and of the regulated industry, to document as much as possible, each of these safety oversight options, as well as the criteria and conditions to which they relate (i.e. criteria which will usually determine which safety regulatory oversight actions will be applied for a specific change to the ATM System).



(Figure 1 – ESARR 4 Safety Oversight Actions)

(Space Left Intentionally Blank)

2.2.3 Safety Oversight Tools and Activities

2.2.3.1 Initial and On-going Safety Oversight

Any specific safety regulatory procedure used to perform ESARR 4 safety oversight should be established in relation with the risk assessment and mitigation processes, and their related safety argument(s), conducted by the provider to meet the national requirements on *'Risk Assessment and Mitigation'* compliant with ESARR 4.

The assessment of compliance with ESARR 4 should be considered in two operational states of the national ATM System;

- The normal day to day operation, with non-major changes, and
- In any area or time of major change[11].

The designated authority needs to ensure that ESARR 4 is complied with before and during operational implementation, as well as on a continuous basis throughout the life cycle of the ATM System and of its constituent parts.

The **on-going safety oversight** would mainly concern the steady state of the operated ATM System; that is to say, the routine operation of already established systems, and possibly, the handling of non-major changes to the ATM System. On going safety oversight should primarily be performed through a regular programme of safety regulatory audits and inspections of the approved safety management system inclusive of associated risk assessment and mitigation processes and arguments, as the main provider's tools to ensure safety in ATM services.

On the other hand, there is a need to address new systems and major changes more thoroughly**. Initial Safety oversight, undertaken through safety regulatory approvals** will normally be conducted on particular system selected by virtue of their significance, as documented by the designated authority. Initial safety oversight will mainly deal with changes with major safety implications[12], with new technologies, new operational concepts, complex projects systems, and other big projects and developments. The introduction of new operational units, new equipment and operational procedures, or a new airspace structure design, are some clear examples of candidate major changes which may be subject to initial safety oversight actions, hence to safety regulatory approvals.

Both on going safety oversight and initial safety oversight can rely on programmes of safety regulatory audits and inspections.

Initial and ongoing safety oversight should be implemented to verify the adequacy of documented processes and safety arguments, of implemented processes and of the operated ATM system. They would concern verification that the;

- proposed risk assessment and mitigation method/process described in the SMS documentation of a specific ATM service provider meets the applicable national regulations;
- implemented risk assessment and mitigation processes are consistent with the documented organisation's risk assessment and mitigation processes,

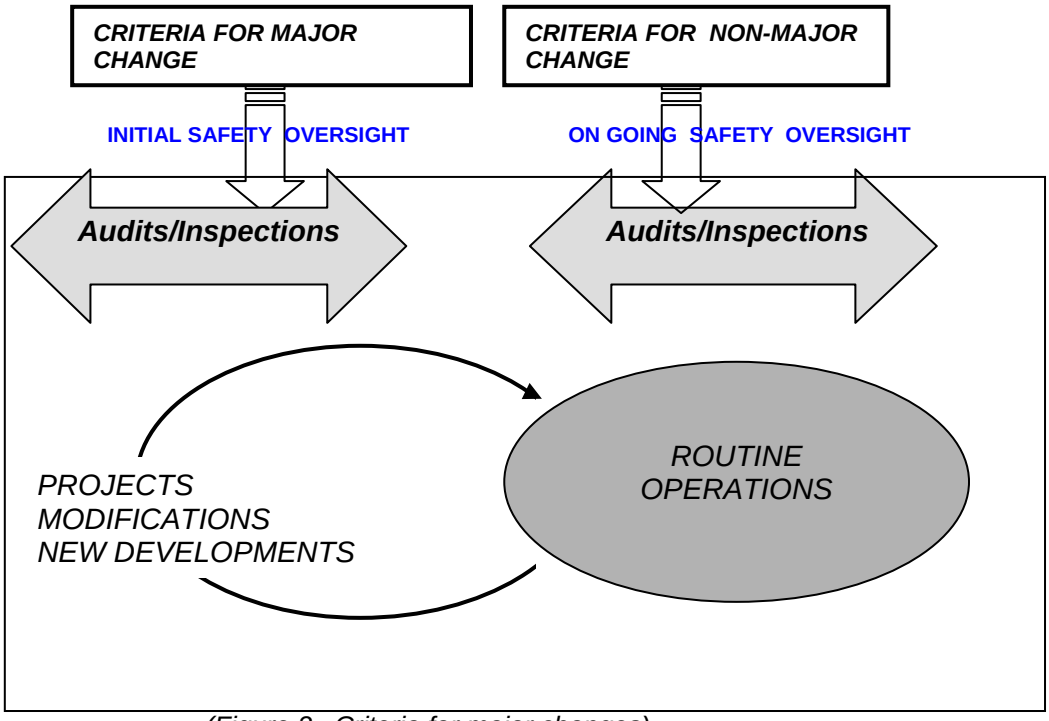
[11] *Refer to the need for defining what 'major' means in Chapter 1 and also in Chapter 2-section 2.2.2.2.*

[12] *As determined during a preliminary Functional Hazard Assessment, for example.*

- safety arguments (i.e. results of risk assessment and mitigation processes) demonstrate that proposed changes can be implemented within tolerable safety minima, in a manner compliant with ESARR 4 national regulations,
- ATM system and related elements are adequate and will meet allocated safety requirements (i.e. examination of man machine interface, of simulation of specific environmental conditions, of the operational documentation), and
- ATM System and related elements will meet applicable published safety related specifications and standards.

It is recommended to establish and publish a set of criteria to determine if a change to the ATM System should be submitted to initial safety regulatory oversight (hence to safety regulatory approval) or not, i.e. if the change is major[13] .

As a complement, it is recommended to establish a formal programme of safety regulatory audits and inspections as part of 'initial' or/and 'on going safety oversight', potentially combined with those related to SMS, to assess compliance with ESARR 4 related processes and to verify that the ATM System is operated within tolerable ATM safety minima.



(Figure 2– Criteria for major changes)

2.2.3.1.1 Defining Minor or Major Changes

Within ESARR 4 and ESARR 3, one of the key principles is to identify risks to the ATM service. Within ESARR 4 this is specifically related to the identification of hazards and risks. However, the intention of Safety Management is to allow the

[13] *Criteria to be determined and documented in the national safety oversight procedures (Refer to Chapter 2).*

Service Provider to conduct this Risk assessment with the appropriate amount of safety oversight.

Safety oversight is defined in this document in two levels, initial and ongoing. To determine whether initial or ongoing oversight is appropriate to a change, this document uses the principle of a major or a minor change. However there are many different ways of defining a change as minor or major.

To restate, the difference is that a major change is one that would require initial safety oversight (and on-going safety oversight) and a minor change would require only on-going safety oversight. This reduction in safety oversight by the regulator is balanced by the increased demonstrated safety management at the service provider.

The difference between them is meant to indicate that in the organisation with a mature risk assessment and mitigation regime, the regulator has sufficient confidence and experience of the risk assessment and mitigation regime. Consequently, the regulator has assurance that the organisation has demonstrated adequate competency to manage a minor change.

Furthermore, the terms are not strictly defined as a change that could be considered minor in an organisation with a well established, mature risk assessment and mitigation regime might be a major change in an organisation with a less established risk assessment and mitigation regime. Hence, it is not possible, taking into account all the possible regulatory regimes and levels of maturity of the Service Providers to define the difference between ‘major’ and ‘minor’. However, it is possible, based on the experience of certain countries, to provide some guidance on possible criteria to consider when defining the difference for particular national implementations.

At no point in this document are the terms minor or major meant to indicate any difference in the application of ESARR 4 that is required. ESARR 4 is to be applied to all changes to the ATM system.

The terms ‘major’ and ‘minor’ are not meant to be synonymous with ‘big’ and ‘small’ as there is no suggestion that ‘small’ changes are less safety critical than ‘big’ changes.

In all cases the introduction of the minor – major change in safety oversight should only take place after a period where the service provider demonstrates, through a number of safety assessments of changes, that they have a safety management system in place that ensures a competent and well managed safety assessment process.

2.2.3.1.1.1 Major/Minor Criteria Based on Severity of the Effect of the Hazard Caused by the System

One of the first steps of the ESARR 4 process is to determine the severity of the effect of the hazards introduced by that system. Therefore, the Regulator could use the highest severity determined from this step to determine the major – minor criteria. For example all system changes for which the Risk Assessment and Mitigation indicates a Hazard with an effect classified at 1 or 2 might be defined as major, and all others could be minor.

In such an example, to ensure that the Service Provider is correctly determining the Severity Classification, the on going Safety Oversight would need to specifically assess those system changes that had been determined by the Safety Provider as being 3, 4 or 5[14].

2.2.3.1.1.2 Major/Minor Criteria Based on Risk Acceptability

A subsequent step of the ESARR 4 process is to determine the required safety objectives of the system. If during the course of the system development, it is apparent that the safety objectives are difficult to achieve (for reasons of practicality or lack of verification), some countries are proposing to use a risk acceptability[15] matrix approach that allows the acceptance of risks that do not meet the safety objectives provided additional steps are carried out – principally management acceptance or endorsement[16]. Therefore, the Regulator could use these risk acceptability criteria to determine the major – minor criteria. For example all system changes for which the risk assessment and mitigation indicates a risk classified at 'a'[17] or 'b' might be defined as major, and all others could be minor. This assumes that risk class 'a' relates to unacceptable and risk class 'd' is acceptable.

In such an example, to ensure that the Service Provider was correctly determining the acceptable risk class, the on going Safety Oversight would need to specifically assess those system changes that had been determined by the Safety Provider as being class 'c' or 'd' .

The consideration of acceptable risk in this manner can be interpreted in that the system as designed is not tolerably safe as defined as ESARR 4. The acceptable risk method should only be used within very mature Safety Regulatory regimes where the consequences of allowing intolerable risks in one area of the ATM system can be fully explored and mitigated in other areas.

2.2.3.1.1.3 Major/Minor Criteria Based on Verification of Safety Requirements

Another of the parts of the ESARR 4 process is to allocate Safety Requirements to parts of the ATM system. However, certain parts of the ATM system have difficulty in providing validation that such requirements can be met. Examples of such areas could include where safety requirements are met by software, people or procedures. At present, safety requirements that are allocated to these system elements are likely to be validated by use of assurance levels.

An assurance level is a method of applying a set of tools or techniques (generally, but not exclusively a set of quality management processes) to the development of a piece of software, a procedure or a training element. There would generally be a number of assurance levels that correspond to the degree of safety criticality allocated to that system element.

---

[14] *Using the Severity Classes defined in ESARR 4.*

[15] *Risk acceptability is used here to differentiate from Risk Tolerability as used in ESARR 4. Risk Tolerability is the assessment of the required performance based on the severity of the effect of the hazard, risk acceptability is the assessment of the achieved performance of the designed system.*

[16] *The endorsement or acceptance of risk by management is meant to indicate that additional risk mitigation will be ensured by that management layer. It indicates that this mitigation will be provided outside of the system under consideration.*

[17] *Small letter 'a' and 'b' are used to ensure that there is no confusion with the severity classification scheme used in 2.2.3.1.1.*

Therefore, the Regulator could use the assurance level to define the major - minor classification. For example, the regulator could assess the assurance levels to be used by the service provider and then define that any system that requires assurance level A[18] or B is major and assurance level C, D and E is minor. This assumes that assurance level A and B are associated with the higher safety risks[19]. It is also likely that this criteria could only be used in conjunction with that in 2.2.3.1.1.2.

In such an example, to ensure that the Service Provider was correctly determining the assurance levels, the on going Safety Oversight would need to specifically assess those system changes that had been determined by the Safety Provider as being C, D or E.

2.2.3.1.1.4 Major/Minor Criteria Based on Novelty

Some changes conducted by a service provider can be considered routine. In other words, the change that is conducted is the same as a change that has previously been carried out and the methods for controlling and implementing the change have been shown by the previous change to achieve the safety requirements placed on the system.

Certain countries are considering that the ATM System can include all the procedures and standards used by the service provider to conduct changes to the ATM system. Therefore, if this procedures and standards have been shown to be adequate in prior application, then providing the same procedure and standard is applied for a new change, then the regulator can have high confidence that the change will meet the safety requirements.

Therefore, the Regulator could use the existing procedures or standards used by the service provider to define the major minor classification. For example, the regulator could assess (or make use of existing Compliance assessments conducted by the SRU) the procedures and standards to be used by the service provider and then define that any system change that uses these are minor changes. Any change not covered by these procedures or standards would be classified as major. To ensure that the Regulator can capture the procedures and standards that are considered appropriate, some countries require the inclusion of procedure or standards references within the Service Provider Safety Management System or within the rulemaking process.

In such an example, to ensure that the Service Provider was correctly applying the procedures and standards, the on going Safety Oversight would need to specifically assess those system changes that had been determined by the Safety Provider by these procedures or standards.

Changes that fall within this category are as follows.

---

[18] *Categories A, B etc are used to signify that these are not the same categories as used in 2.2.3.1.1.1 and 2.2.3.1.1.2.*

[19] *This example follows the ESARR 6 Software Assurance Level. In national regulatory systems, there may be any number of assurance levels associated with particular system elements.*

2.2.3.1.1.4.1 Major Minor Criteria Based on Changes Controlled by Procedures and Standards Already Validated at the Service Provider

In everyday life an ATM service provider faces all kinds of activities, procedures and events that could be considered as “changes”. Most of them are, however, well defined and documented as part of the existing system and could therefore not need to be considered as “changes” in the sense of ESARR 4. The concept is then to ensure that every plan or activity to alter the existing system is thoroughly examined and analysed by a risk assessment process to make sure that no unacceptable risks are induced by this alteration.

In order to use this concept it is necessary to:

a) define the “existing ATM system” by pointing out the definitions and documentation available (including laws, legal regulations, international and national standards, published official documents, company internal regulations that are endorsed by the regulator);

b) define a “change” as any activity or alteration that is NOT included in or described as being part of the “existing system”, defined in a).

This means, that activities and processes that are already regulated by law, covered by national or international standards or documented in internal documents endorsed by the regulator are considered part of the existing systems and are considered as minor changes.

It should be required, however, that the compliance of any process or activity with existing regulation or standards has to be documented unambiguously (“Proof of Compliance”) In order to use this concept, the system considered must have described safety objectives/safety levels. i.e. must have been subject to a baseline ESARR 4 compliant risk assessment

The procedures and standards that can be used by the service provider might be those that have been developed internally. For example, the following changes might have associated procedures;

- Updating of radar maps,
- Installation of a number of similar pieces of equipment i.e. a radar, VOR or ILS replacement programme,
- Reconfiguration of operational telephones.

2.2.3.1.1.4.2 Major Minor Criteria Based on Changes Controlled by Procedures and Standards Already Validated by Other Agencies

The procedures and standards that can be used by the service provider might be those that have been developed externally. For example ICAO standards and recommended practices, International Telecommunication Union standards, EUROCAE standards etc. The following examples are of changes that could be covered by such standards;

- Technical standards for equipment,
- Operational phraseology,
- Design of ATC procedures such as SIDs and STARs, etc.

The regulator will need to exercise caution with the approval of such external standards for the following reasons. These are particularly applicable if the nation has no previous experience of application of the standard.

The external standard being used might not be appropriate to the operational environment in the particular country. For example, the standard might have been developed making assumptions on traffic density, traffic capabilities, traffic equipage, ATM service provider equipage etc that are not met by the aircraft or the ATM provider in the country.

There may be no specific safety analysis conducted on a standard, i.e. many standards relate to the technical details of the interoperability of systems without consideration of the operational, procedural and people aspects of the use of the system.

2.2.3.1.1.5 Major Minor Criteria based on changes Made Within the Bounds of the Original Equipment Approval

When a new system has been installed and assessed as compliant with ESARR 4, it is necessary for the regulator to consider which types of changes can be carried out on this system that require a further approval. This is particularly true as regards modifications to the system that can be expected as part of maintenance.

2.2.3.1.1.5.1 Replacement Parts

A regulator could consider that any replacement part that is part of the original equipment and is as specified by the manufacturer could be fitted without requiring a change to the approval. However, the regulator could consider that the repair of a system with a component that is not as specified by the original manufacturer could require a new ESARR 4 assessment. Even in such circumstances, the regulator could consider that provided the service provider conducts an assessment to show that the part does not alter the function, the operating characteristics or performance characteristics of the system, then the change could be considered minor.

2.2.3.1.1.5.2 Modifications to Change System Performance

If the purpose of the system modification is to change the performance of the system or to change the function of the system, then this could indicate a change to the safety objectives of the system as a result of increased safety risk. Such a change could then require a new risk assessment and mitigation.

2.2.3.1.1.5.3 Alteration of Configuration Data

Within many systems, there are user configuration settings that effect the functionality. Although this is typically relevant to systems that use software components, the same re-configurability can occur within hardware systems.

The regulator should ensure that any such user configurable items should be accounted for in the risk mitigation process. This could be in the form of a defined configuration list that relates the approval to a given configuration.

Wherever possible, the regulator should attempt to define the restrictions in terms of the required performance of the system rather than by attempting to define the configuration of the equipment. For example, if it is necessary to control the power, pulse width, PRF, frequency, modulation depth etc for safety reasons, the limitations should be defined in terms of the actual emissions from the equipment rather than sub system limitations in terms of equipment specific codes or settings.

Therefore, the Regulator could use the existing configuration as assessed by the service provider to define the major minor classification. Any change outside this configuration would be classified as major. To ensure that the Regulator can capture the configuration(s) that are considered appropriate, some countries require the inclusion of the configuration to be recorded within the Service Provider Safety Management System or within the rulemaking process.

In such an example, to ensure that the Service Provider was correctly adhering to the configuration, the on going Safety Oversight would need to specifically assess any system changes that had been determined by the Safety Provider.

2.2.3.1.1.7 Major Minor Criteria Based on Complexity

Some systems require the allocation of safety requirements across several service providers. Data link systems, voice communication systems, radar systems etc require considerations between the ground ATM supplier, utility providers, communication service providers, satellite providers, aircraft manufactures and aircraft system providers. While the adequate and satisfactory justification of the safety of the externally provided services is the responsibility of the ATM service provider, the regulator could decide that the more organisations involved in a change, the more likely for these requirements to not be achieved.

Therefore, the Regulator could use the number of organisations required to coordinate safety requirements for a system to define the major minor classification. Any change requiring the coordination of more than three organisations could be classified as major.

In such an example, to ensure that the Service Provider was correctly adhering to the complexity criteria, the on going Safety Oversight would need to specifically assess any system changes that had been determined by the Safety Provider as non complex.

2.2.3.2 Use of the Analysis of ATM Safety Occurrences

The analysis of safety occurrences in ATM contributes to the monitoring of achieved ATM safety levels. As a general rule, its results should be used to support safety oversight activities. Particularly, these results may support the monitoring of specific assumptions and of the effectiveness of risk mitigation means as included in a specific safety argument.

It is recommended to document the type of safety data which must be made available to the designated authority, both on a generic basis, along the lines of the safety indicators developed in ESARR 2, and on a case by case, for safety occurrences related to a specific change to the ATM System

Note: In the case of an extremely passive ESARR 4 safety oversight which solely relies on the service provider's competence and on its level of commitment to safety, safety performance monitoring becomes the only element of ESARR 4 Safety Oversight. Indeed, the only visibility the designated authority would have on the achieved ATM safety levels and acceptability of past changes would be through feed back from accident investigation and ESARR 2 implementation[20].

2.2.4 Grant of a Safety Regulatory Approval

2.2.4.1 Need for a Safety Regulatory Approval

After completion of ESARR 4 initial safety oversight, it seems necessary to indicate one way or another acceptance of the safety argument, hence of the ATM System, or system elements, or proposed changes being considered for operational service.

Accordingly, safety regulations and related ESARR 4 safety oversight procedures should lead ATM service providers to follow some sort of acceptance/approval process at least for new systems or major[21] changes before going into operational service.

Two main approaches could be conceived depending upon specific situations and related proposed changes;

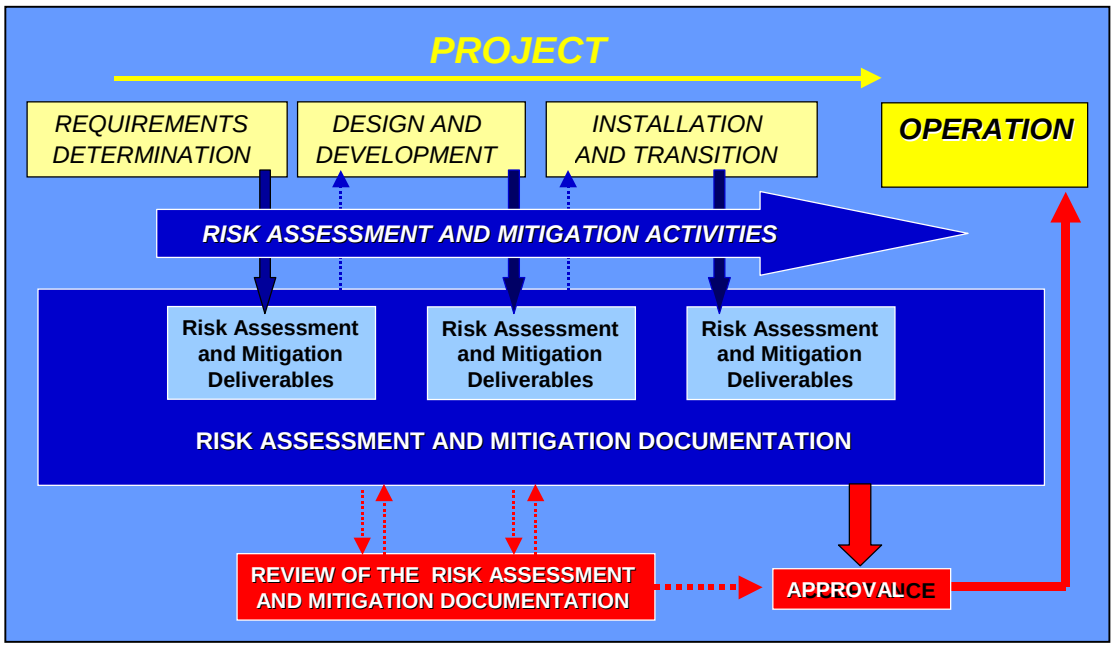
- In some cases, the provider may carry out internal acceptance processes, as part of its SMS and may use risk assessment and mitigation to ensure appropriate internal decision making. In such a context, no immediate direct regulatory involvement would be needed throughout those processes. Compliance with ESARR 4 would be assessed as part of a regular programme of ESARR 4 or ESARR 3 safety regulatory audits and inspections. However, this would only be possible if those SMS processes have demonstrated to be effective, and enough on going regulatory oversight is focused on them; and
- In other cases, designated authorities may decide that new systems and major changes need to be directly accepted by the designated authority through a formal initial safety oversight process in which the designated authority is expected to make the final decision on the acceptability of the system, in addition to the internal acceptance process of the service provider. ESARR 4 type of risk assessment and mitigation processes would provide assurance and demonstration to support those decisions.

[20] *The risk being that a passive role may also have been adopted in the case of ESARR 2, jeopardising the reliability of the reporting system.*

[21] *As defined in Chapter 1 and Chapter 2 Section 2.2.2.2.*

It should be noted that the establishment of such initial safety oversight processes, leading to the issuance of safety regulatory approvals, would be consistent with other aviation practices applied in respect of aircraft manufacturers, operators and airports[22].

Different intermediate options can be adopted depending upon several factors. The main tool for customising and harmonising the initial safety oversight processes across States but also over time, when more experience is gained, is the set of options/criteria determining the significance of a change, as introduced in section 2.2.2.2.



(Figure 3 – Initial Safety Oversight and Safety Regulatory Approval)

2.2.4.2 Life of a Safety Regulatory Approval

The designated authority needs to ensure that ESARR 4 is complied with and minimum safety minima in ATM met before any issuance of a safety regulatory approval, and on a continuous basis throughout the duration of that approval.

- The 'initial safety oversight' process should normally lead to the issuance of a safety regulatory approval for operations of the ATM System/introduction of a major change into operations, and
- The 'on-going safety oversight' process', combined with feed back from Reporting and Analysis of ATM Safety Occurrences, should provide the necessary mechanism for renewing periodically the approval, or limiting, modifying or suspending it.

As specified in SRC POLICY DOCUMENT 3, "the form of approval is a matter of national choice and must indicate as a minimum the precise scope, applicability and duration of the approval".

[22] *If we consider recent amendment 14 to Annex 14 and related aerodrome certification manual.*

It is recommended to document the conditions of issuance of such safety regulatory approvals, as well as conditions of suspension, cancellation, renewal, limitation and modification of that approval.

2.2.4.3 Scope of the Safety Regulatory Approval

SRC Policy Document 3 and ESARR 1 introduce the need for the designated authorities to define its approval approach with regard to the approval of the ATM System and of its elements. In particular, SRC Policy Document 3 states that, having regard of the significance of the different system elements of the ATM system, the designated authority will further need to identify the "constituent parts of the ATM System which would require a formal safety regulatory approval before being allowed to be operated".

Various views can be expressed regarding the scope/level of the safety regulatory approval and related safety argument;

- Should safety regulators issue an approval for a piece of equipment, a function, a service?
- Should safety regulator issue an approval for personnel?
- Should safety regulator issue an approval for specific ATM operations?
- Should safety regulator issue an approval for each operational unit (i.e. ACC, TWR)
- Should safety regulator issue a unique approval for the overall ATM operations of an organisation, including all associated privileges?

This is a matter for national choice as it depends upon a number of criteria, such as the number of services provided, their size and related services provided. However, in order to initiate a harmonisation of practices, here are some recommendations to be considered;

- The introduction of a new or modified operational capability into service should be subject to a form of safety regulatory approval (e.g. RVSM, new RNAV procedures, dynamic re-routing),
- The introduction of new types of functions, brand new technology and technical concepts into operations should also be subject to a safety regulatory approval even if the operational capabilities and services being offered are similar than previously approved operations (e.g. use of GNSS for specific operations, introduction of a new radar processing system),
- The modification of existing functions, of existing equipment (replacement of Navaids, installation of a new radar sensor, modification to software in flight plan processing system) may not be subject to a specific safety regulatory approval except if it is highly critical for safety (ILS Cat 3) and for a specific safety critical operations,

(Space Left Intentionally Blank)

Other modifications of lower safety significance could not be subject to any form of safety regulatory approval and be dealt with as part of on going safety oversight[23].

A general principle would be to avoid issuing a safety regulatory approval for an element of the ATM System which does not have a direct safety impact alone but which can be considered as part of a more global system in a specific operational environment.

Approval activities could ultimately and primarily be focused on system levels where all the elements[24] , functions and services are actually integrated to provide a complete operational service; that is to say, on operational units.

According to SRC Policy Document 3, as a minimum those constituent parts where all the elements and functions are integrated into a final operational service (such as Area Control Centres (ACC) or Towers (TWR)) should be formally approved before going into operational service. It could indeed be expected that the operations of operational units (TWR, ACC) would represent the minimum level requiring initial safety oversight as well as the issuance by the designated Authority of a an approval. Related safety arguments could refer to more specific safety arguments developed for particular operational capabilities such as RNAV or technical equipment such as FDPS.

Note: Requirements against which to issue such a safety regulatory approval would go beyond ESARR 4 and most probably include at least the implementation of some requirements of ESARR 2, 3 and 5.

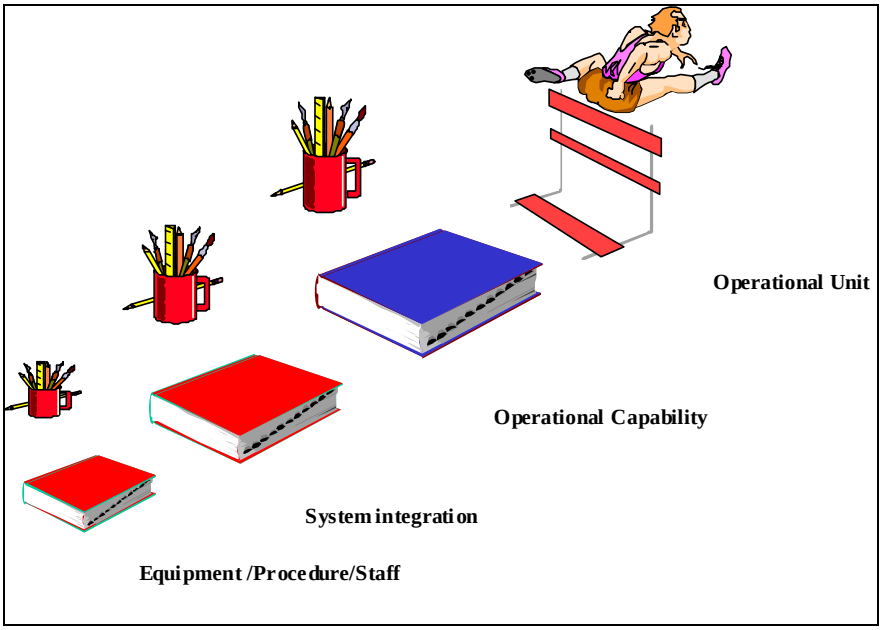
As depicted in Fig. 2, intermediate forms of safety regulatory acceptance could co-exist in order to progressively acquire a safety credit at lower levels. This progressive approach would also lead to the issuance of a formal safety regulatory approval(s) for an operational unit and /or for the national ATM System.

The objective of initial safety oversight is therefore to consider arguments and evidence to decide and state whether an ATM System or part of an ATM System, is safe to be introduced into operational service. The introduction into operational service of TWR, ACC etc. is what should ultimately be the minimum to be approved. However, intermediate approvals could be implemented as well.

(Space Left Intentionally Blank)

[23] *In addition to the internal acceptance process of the service provide organisation.*

[24] *People, equipment, procedures.*



(Figure 4 – Safety Credit)

Successive steps in the initial safety oversight process could be identified, each being granted a certain credit as demonstration and justification of compliance to well identified sets of safety requirements (of safety standards/published safety related specifications) have been carried out.

However, as ESARR 4 focuses on safety requirements determined in a specific environment of operations, it may seem difficult and even counter-productive to grant an approval to parts of the ATM System whose safety impact is largely determined by the technical and operational environment in which it operates. It would therefore be recommended to avoid granting a safety regulatory approval to a part of an ATM System whose safety impact may vary according to its technical and operational environment.

2.2.4.4 Safety Regulatory Aspects in Small Organisations

ESARR 4 does not contain any provisions that require a different application of Risk Mitigation and Assurance between large and small organisations. However, the SSAP has identified that certain small organisations, particularly airports, in consideration of their operational capabilities should be regulated in a different manner to larger organisations.

These considerations are not made on the basis of any allowable reduction in safety processes but are to reflect the fact that certain organisations exhibit lower safety risk by their operational capabilities and their development style.

The first consideration relates to the type of operational tasks conducted by the small organisations. In general, small organisations do not formulate new approaches to the provision of ATM. They use methods inherited from other organisations or standard methods that are derived from long standing standard practices, whether these standard practices are internationally derived or nationally derived. Safety oversight should therefore be focused on the aspects of ensuring that experience from these other organisations is sufficiently carried over to the small organisation. This can be accomplished by safety oversight using auditors with a sufficient breadth of understanding of current operational methods.

The second consideration is that small organisations are not usually original in their equipment purchases. Equipment is generally based on equipments previously purchased by larger organisations and supplied by external suppliers. These larger organisations will normally have already proven the safety requirements of such systems through a priori assessment and through in service monitoring. Safety oversight – as already identified in EAM 3 / GUI 2 - can therefore be focused on how the SMS deals with these external services and on the Safety Argument supplied by the manufacturer. Safety oversight should consider the use of interfaces to other National Safety Regulators where the systems are already in use in other countries. It is even possible that safety oversight might make use of 'approved equipments' within its national framework.

The third consideration is that the ATM equipment at small organisations tends to be of a simpler architecture than in larger ATM organisations. It is less complex and therefore more understandable to the operators. It is therefore possible to allow more of the safety argument to be made from in-service monitoring than a priori assessment. Safety oversight could therefore be focused on the safety monitoring and safety occurrence parts of ESARR 3 (Paragraph 5.3.3 and 5.2.7 respectively).

The fourth consideration is that the ESARR 4 requirements for risk assessment and mitigation already allow for the fact that the depth and scope of the risk assessment and mitigation evidence supplied is in relation to the types of function performed, the severity of the effect of the hazard and the complexity of the constituent part of the ATM system being considered (see ESARR 4 footnote 8 on page 10 – also enclosed at Enclosure 2). ESSAR 4 identifies a process which should be followed, and the elements in that process. It does not indicate that the risk assessment and mitigation documentation should be built to a certain structure, or even that certain sections within such documentation are obligatory. Safety oversight should therefore recognise that the contents of such documentation can be less formal when addressing lower risks.

The fifth consideration is the development of a risk classification scheme in small ATM organisations. It is unlikely to be efficient to request multiple similar operators to determine independent risk classification schemes as required by Appendix A-2 of ESARR 4. Such risk classification matrixes should be constructed by groups of such operators, or set by the national regulator. For certain categories of risks, the safety objectives may be defined quantitatively or based on the use of existing standards, regulations, practices or procedures. For certain risk categories it is possible that no a priori risk assessment and mitigation is necessary.

The sixth consideration is the use of Acceptable Means of Compliance (AMC). There are many methods, tools and techniques to the construction of a risk assessment and mitigation document. Safety oversight should make use of the AMC process to evaluate these techniques and make them available for use across small organisations.

2.2.5 Proposed Means of Compliance

ATM service providers may refer to acceptable means of compliance in their risk assessment and mitigation procedures.

ESARR 4 Safety Oversight staff should therefore be ware of those AMC to ESARR 4.

Two documents have been assessed by SRC to establish to which extent they may be declared as acceptable means of compliance with the provisions of ESARR 4;

- EATMP Air Navigation System Safety Assessment Methodology (FHA)- Ed 1.0; and
- EUROCAE ED78A/RTCA DO 204 'Guidelines for the approval of ATS supported by data communications"

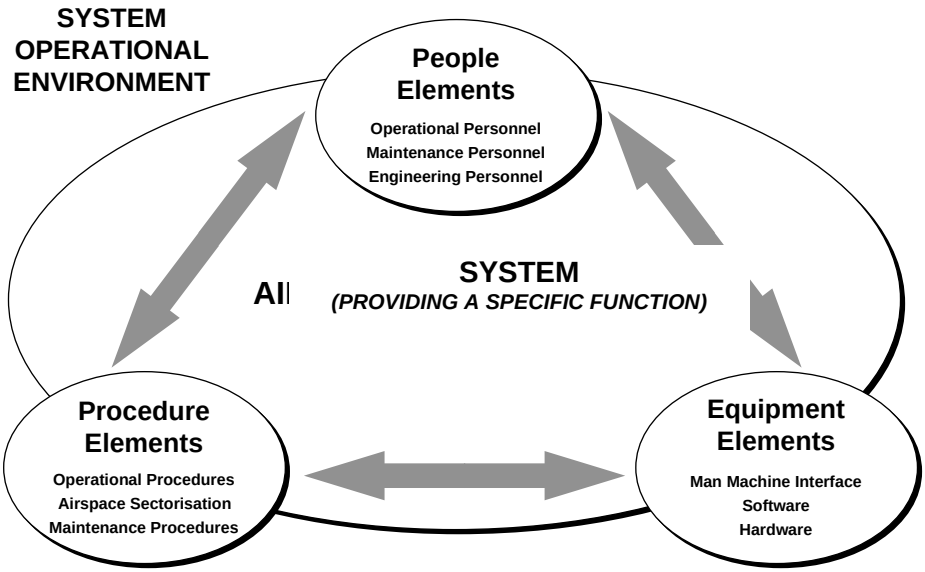
2.2.6 External Interfaces

The designated authority in charge of ESARR 4 safety oversight ought to maintain a number of interfaces, some of those on a daily basis, for the performance of initial and on going safety oversight.

It is recommended to develop and promulgate those procedures of interfaces.

2.2.6.1 Adopting a System Approach

Each sub-system of the ATM System combines one or more system elements, which interface to fulfil a specific function. The system elements are equipment, people and procedure. The generic composition of an ATM system is illustrated in the next figure.



In the light of this concept, the designated authority should identify the scope and boundaries of the system to be dealt with, as well as the interactions of the system under consideration with the operational environment and external factors.

This should enable the designated authority to identify the interfaces it itself needs to establish in the course of its ESARR 4 safety oversight.

Examples of typical interfaces to be established include the Aeronautical Information Services (AIS) and the MET authorities.

2.2.6.2 Co-ordination with Other Safety Regulatory Authorities

A typical interface to be established includes the airport safety regulatory authority.

In addition, ESARR 4 requires a total system approach to be adopted in the risk assessment and mitigation of ATM. Indeed, airborne and spatial components of the ATM System might be required to implement a specific ATM operational capability. Consequently, those components involved in ATM would be subject to ESARR 4.

The legal powers for enforcing safety requirements bearing on aircraft design and operations is usually vested in a specific authority, called in this document 'aircraft certification authority'. When developing safety requirements for new airborne systems, it is essential that due account is given to the safety constraints coming from ATM, in addition to traditional airworthiness and flight operations requirements.

Co-ordination with those safety regulatory bodies dealing with aircraft certification, at national level and world-wide, is therefore essential, both when deriving safety objectives and safety requirements, and developing related international standards, for changes to the ATM System, but also when verifying compliance with those.

Note: At European level, a specific forum exists within the Joint Aviation Authority, called the JAA CNS/ATM, which establishes Temporary Guidance Leaflet for new airborne CNS/ATM systems, and triggers related safety regulatory actions in JAA. This group implements at European level one of those interfaces between the ATM safety regulatory community and the aircraft certification authority community.

2.2.6.3 Co-ordination with ICAO

In the framework of its Universal Safety Oversight Programme, ICAO will develop some audits protocols for verifying compliance with Annex 11 and more specifically with risk assessment and mitigation related requirements. It would be beneficial if the safety regulatory audit protocols developed by the designated authority be developed giving full consideration of the ICAO standards and recommended practices and related ICAO safety oversight audit protocols; it would also be beneficial if the designated authority was to contribute ESARR 4 safety oversight experts to the ICAO Safety Oversight audits.

2.2.6.4 Co-ordination with the SRC

The EUROCONTROL Agency co-ordinates with Member States for the definition and implementation of a number of changes to the European ATM system.

As such, a number of core safety activities are also co-ordinated at European level, within the EUROCONTROL Agency. Those safety activities essentially aim at contributing that the proposed operational concepts are demonstrated to be within tolerable safety minima.

The SRC is tasked with the development of a harmonised safety regulatory view in the acceptability of the proposed change (Refer to SRC Document 6), which is provided to the EUROCONTROL Permanent Commission;

- The SRC will assess the risk assessment and mitigation processes proposed by the Agency against ESARR 4 and state their acceptability,
- The SRC will assess related safety policy, safety plan and other safety deliverables against ESARR 4 and state their acceptability,

- The SRC will develop specific safety regulatory requirements in a Requirement Application Document (RAD) when applying relevant ESARRs to the proposed change (Refer to SRC Document 6),
- The SRC will co-ordinate with aircraft safety regulatory authorities the acceptability of safety requirements bearing on the aircraft segment,
- The SRC may also assess some national safety deliverables, should issues in that area impact the overall safety of the proposed European change, hence of other ECAC States.

Therefore, co-ordination with the Safety Regulation Commission for changes to the European ATM System is also necessary;

- Indeed, the SRC exists to ensure the harmonised development and uniform implementation of safety objectives, requirements and safety standards across ECAC; and
- This implies contributing to the SRC the national views on the acceptability of related safety deliverables and ultimately, of the proposed change;
- This implies making use of the SRC harmonised view in the national safety oversight process when times come for the national implementation; and
- This implies providing feed back to SRC on different national views and on related potential issues.

Note: In addition, the uniform implementation of ESARR 4 implies recognising a number of Means of Compliance to ESARR 4.

2.2.6.5 Feed back from the reporting and analysis of ATM safety occurrences

As already mentioned, the analysis of ATM safety occurrences allows to increase the visibility on the risks induced by the ATM System and its constituent elements. Feedback on key risk areas in ATM also enables to verify over time the validity of assumptions made in safety arguments as well as the effectiveness of safety mitigation measures.

This feedback would allow a risk model to be developed based on feedback from experience, supporting the anticipation and control of risks induced by changes to the ATM System.

Essential sources of information include the outcomes of;

- accident and serious incident investigations. Therefore, a close working interface should be established with the national Accident Investigation Authority, while still preserving their necessary level of independence, and
- the analysis of incidents in ATM and other ATM related accident precursors. Therefore, a close working interface should be established with the organisations responsible for determining the facts, causes and recommendations of incidents and other precursors in ATM.

(Space Left Intentionally Blank)

3. INITIAL SAFETY OVERSIGHT

3.1 Introduction

3.1.1 General Considerations

The 'initial safety oversight' of ATM service providers involves activities far beyond the assessment and acceptance of documentation.

Although the importance of the latter elements should not be overlooked, 'initial safety oversight' also includes safety regulatory audits and inspections of processes, examination of evidence and final products.

3.1.2 Scope of Initial Safety Oversight

As already stated in Chapter 2, from a safety oversight perspective, there is a need to address major changes more thoroughly.

Initial safety oversight will mainly deal with major changes, according to those criteria defined by the designated authority (refer to section 2.2.2.2), the ATM service provider ought to;

- establish evidence of ESARR 4 requirement compliance and satisfy itself that safety will be kept, as a minimum, within safety minima,
- document as early as possible when defining the proposed change, the rational for the significance classification of that proposed change. This should be made available to the designated authority at any time.

If, according to the procedures and criteria promulgated by the designated authority, the change is classified by the service provider as 'major', the designated authority ought to be involved in the related project as early as possible, to facilitate its initial safety oversight and related issuance of safety regulatory approvals.

Initial safety oversight may also be decided and applied by the designated authority on an ad hoc basis.

3.1.3 Initial Safety Oversight Procedures

3.1.3.1 General

The ATM service provider risk assessment and mitigation procedures, as documented in its Safety Management System should ensure full compliance with ESARR 4.

The ATM service provider risk assessment and mitigation procedures, as implemented on a daily basis, should ensure full compliance with ESARR 4.

The results of any risk assessment and mitigation process should be documented in a safety argument. The safety argument must be acceptable i.e. should meet the provision of ESARR 4 and should demonstrate that the proposed change can be implemented and operated within tolerable safety levels. Related proofs and evidences should be available for examination.

The ATM system under its managerial control should also meet agreed ATM safety minima, allocated safety objectives and requirements as well as any mandatory safety standards or specifications published by the designated authority. This would also be subject to verification.

3.1.3.2 Initial Safety Oversight Activities

During the definition and implementation of a change to the ATM system, some 'initial safety oversight' activities will take place;

- assessment of the documented risk assessment and mitigation procedures and arrangements that the service provider intends to use;
- assessment of the safety policy;
- assessment of safety plan or equivalent;
- development of safety regulatory criteria, standing as a specific implementation/interpretation of ESARR 4 for that particular application[25];
- safety regulatory audits of implemented risk assessment and mitigation procedures;
- assessment of safety argument;
- examination related evidence;
- examination of the modified ATM System as well as constituent parts;
- inspection that the modified ATM system meets mandatory safety standards and published specifications;
- monitoring of safety performance; and
- issuance of a safety regulatory approval.

3.2 Assessment of Safety Documentation

3.2.1 Risk Assessment and Mitigation Procedures

The ATM service providers should have documented, within its own safety management system, its internal procedures for risk assessment and mitigation of changes to the ATM System under its managerial control.

These internal risk assessment and mitigation should be have been assessed already in the course of "on-going safety oversight" and recognised as meeting ESARR 4 compliant national regulations.

If the documented risk assessment and mitigation processes are communicated for the first time to the designated authority in the context of a major change, it is obviously recommended that such preliminary assessment of documentation be undertaken before the actual safety regulatory audit against ESARR 4 compliant regulations takes place as this will facilitate the preparation of the safety regulatory audit protocols.

Also refer to Section 4.2.1 below.

[25] *This regulatory activity could be undertaken in conjunction with the entity having developed the ESARR 4 compliant national safety regulations, to facilitate a harmonised implementation of ESARR4.*

3.2.2 Safety Policy

The safety oversight staff will determine if the safety policy contains an overview of the proposed change, with description of operational concept, identification of applicable safety regulatory requirements, statements of proposed means of compliance as well as of project safety policy and project safety management principles.

Of specific importance for safety oversight would be the policy to be adopted for the proposed change project when determining the quantified risk classification scheme to be used when setting safety objectives.

3.2.3 Safety Plan

The safety oversight staff will determine if the safety plan documents the activities to be undertaken to be in a position to demonstrate and produce evidence that the proposed change will be implemented within tolerable safety minima, from transition, transfer to operations, operations and maintenance, upgrades, to decommissioning.

The safety oversight staff will also determine if the safety plan was developed in close interaction with the Project Management Plan.

The safety oversight staff will determine if enough co-ordination is anticipated between all stakeholders involved in the proposed changes and with their designated authorities.

3.2.4 Safety Argument

3.2.4.1 Objectives

The safety oversight staff will determine if the documented risk assessment and mitigation procedures used for that specific change is compliant with ESARR 4 compliant national regulations. In particular, the assessment should verify that the service provider has considered any interrelationships in its risk assessment and mitigation and that assumptions placed on elements of the aviation system outside its managerial control have been validated.

It is also essential to verify that the documented outcome of the risk assessment and mitigation process is acceptable, i.e. that the implementation of the change as per the safety argument is shown to meet tolerable safety minima. In particular, the assessment should verify;

- Completeness and correctness of the list of hazards,
- Consistency and credibility of the rationale leading to the allocation of severity classes,
- Validity of safety objectives, ensuring that tolerable safety minima will continue to be met; (this will require an acceptance of the apportionment process by which the risk classification scheme used for the project has been derived from the ATM National Safety Minima),
- Validity, effectiveness and feasibility of safety requirements, ensuring that if implemented, safety objectives will be met, and
- References to clear evidence that safety requirements are and will continue to be met.

The Safety Argument will not only address the hazards associated with the new system, but also those hazards associated with transition.

Transition – the act of bringing an operational system into operational service. It relates to hazards associated with the;

- installation of the new system and how it effects existing systems,
- modifications necessary to existing systems to interface with the new system,
- removal of existing systems replaced by the new system,
- temporary loss of functionality during the removal and replacement of systems,
- reversionary procedures in case new systems prove unreliable or lack performance ,
- maintenance of older systems for an adequate time period to prove the adequacy of the new systems.

3.2.4.2 Scope and Level of Assessment

The scope and depth of the assessment will depend on the safety significance of the change. The focus of the assessment will be largely dependent upon severity of the effect of hazards and related criticality of functions. Focus should be placed on hazards of higher severity of effect.

The scope and depth of the initial safety oversight should also consider the level of assurance/evidence required when verifying safety requirements are implemented.

In addition, the assessment should address specifically the consistency between the safety argument specific to the change and the operational documentation reflecting the actual operations of the ATM system (such as operational manual, AIP, etc.).

3.2.4.3 Standardisation of Assessment

The assessment of the acceptability of safety arguments is subjective, but that subjectivity should be reduced to a minimum.

A database of ATM related hazards with associated severity of effect and rationale could be maintained by the designated authority. It could be used as a reference of past statements of acceptability.

3.2.5 Use of SRC Assessment

In some cases, the change under oversight at national level will consist in a local implementation of a wider European programme.

The safety oversight staff will determine if the national safety policy clearly distinguishes, when describing the proposed change, the scope of the programme which is common to many States from the national variations. It should also determine if the policy clearly indicates the additional safety objectives and principles to be applied nationally.

The safety oversight staff will determine if the national safety plan clearly indicates those tasks which would be undertaken at national level, from those which would be undertaken at European level (a*lso refer to SRC POL DOC 4)*.

The European programme should be subject to SRC safety oversight:

- Ideally, the safety oversight staff in charge of the national initial safety oversight of the national project should also contribute related national inputs to the SRC assessment of related European safety arguments,
- The SRC should co-ordinate with the JAA and other aircraft certification authorities the enactment and enforcement of safety requirements bearing on the aircraft segment as a result of the European risk assessment and mitigation process,
- The final assessment of acceptability of the national safety argument should refer to and make the best use of the outcome of the SRC assessment on related European safety arguments, and
- The designated authority should report back to the SRC any differences in the national view on the acceptability of the proposed change.

3.2.6 RAD or National Equivalent

A National document, equivalent to the SRC Requirement Application Document (RAD), could be developed for a specific project/change at national level.

Such document would specify a number of safety requirements derived as an application of safety regulatory requirements relevant to the change under consideration, and customised to the change under oversight.

Such document would facilitate the common interpretation of applicable safety regulatory requirements to the change under consideration and contribute to a constructive interface between safety oversight staff and service provider personnel staff.

In some cases, the change under oversight consists in a local implementation of a wider European programme. The development of national safety requirements for a national change should contribute to and then refer to the SRC developed Requirement Application Document (RAD).

3.3 Assessment of Procedures

3.3.1 Objectives

The ATM service provider risk assessment and mitigation procedures, as documented in its Safety Management System, and implemented in this specific programme, should ensure full compliance with ESARR 4 compliant national regulations.

This assessment aims at verifying compliance of implemented risk assessment and mitigation procedures with ESARR 4 (and with documented processes, if shown to meet the provisions of ESARR 4 compliant national regulations).

3.3.2 Preparation

SRC Policy Document 3 includes a number of generic recommendations related to the preparation of safety regulatory audits.

A specific importance is the development of audit organisation and protocols/check lists prior to going on site.

The oversight staff should audit against the risk assessment and mitigation procedures and documentation used in the project, as documented in the SMS, as well as against ESARR 4 safety requirements.

Typical ESARR 4 audit protocol/check list is proposed in Appendix C. It would need to be developed further to be customised to the ESARR 4 compliant national safety regulations as well as to the internal risk assessment and mitigation procedures being proposed by the service provider.

One safety regulatory audit could be organised for each major milestone identified in the safety plan, when a safety regulatory view is expected on a safety deliverable, but this should be tailored to the specific situation.

3.4 Assessment of the ATM System

3.4.1 Objectives

The ultimate objective of that assessment is to verify that the ATM System is operated within tolerable safety minima.

It aims at verifying that the end product and constituent parts meet;

- allocated safety objectives and requirements derived from the application of risk assessment and mitigation (this will include examining the evidence claimed in the safety argument), and
- any mandatory safety standards or published specifications.

3.4.2 Activities

The safety oversight staff ought to verify the correctness of the final implementation of the ATM System, so that it is convinced that it meets, with an adequate level of assurance, all safety requirements and objectives resulting for the application of the risk assessment and mitigation process, as well as all requirements included in applicable safety standards and published specifications.

Depending on the scope and nature of the proposed change, the examination of the final ATM system and constituent parts could include:

- Verification that claimed performances for a system are met (i.e. reliability, availability),
- Verification that all safety objectives and requirements are met,
- Verification that the designed Human Machine Interface is acceptable,
- Examination of a prototype or trial implementation against allocated safety requirements, and
- Inspection that requirements derived from safety standards/published specifications are met.

Depending on the scope and nature of the proposed change, evidence that safety requirements are met could include;

- Examination of evidence that assumptions made are and will remain valid,
- Examination that the operational documentation reflects the outcome of the safety argument (i.e. AIP, Operational, maintenance, engineering and training manuals updated according to outcome of safety argument),
- Examination of letters of agreement between FIRs,
- Examination of the test coverage for a software,
- Examination of results of simulation,
- Examination of training manual,
- Verification that Head of Operations and Head of Maintenance are committed to implementing documented safety requirements,
- Verification that the safety requirements bearing on the airborne segment are indeed reflected in up to date airborne standards and that compliance with these is being verified by appropriate authorities,
- Verification that the safety requirements bearing on the airborne segment are promulgated via AIS, and
- Examination of the “Reporting Manual” or equivalent to determine to verify the requirements for safety performance monitoring have been included into the internal safety occurrence reporting and analysis process.

3.5 Reporting and Follow-Up

3.5.1 Reporting

For generic recommendations on the reporting of an audit of procedures in safety oversight, refer to SRC Policy Document 3.

In general, a report should be completed at the end of each ‘initial safety oversight’ activity; documentation assessment, assessment of procedures, assessment of the final product/system).

3.5.2 Follow-up

For generic recommendations on the follow up of an audit of procedures in safety oversight, refer to SRC Policy Document 3.

All discrepancies and non-compliance items should be corrected to the satisfaction of the designated authority prior to the commencement of any operational service involving the proposed change.

The designated authority may also decide to accept a limited operations if the non-compliance items are assessed as being minor and are being corrected within a specified time.

‘Initial safety oversight’ does not allow an ATM system to be operational once forever. It is being followed by on going safety oversight.

'Initial safety oversight' will transfer to 'on going safety oversight' the responsibility of;

- Verifying continuing validity of assumptions,
- Verification of continuous implementations of safety requirements,
- Verification of effectiveness of implemented mitigation measures, and
- Verification that minimum tolerable safety minima are met.

3.6 Safety Regulatory Approval

3.6.1 General

'Initial safety oversight' provides the basis for the issuance of a safety regulatory approval. The approval represents the outcome of the initial safety oversight process.

3.6.2 Delegation of ESARR 4 Initial Safety Oversight

In some instances, where a sound and mature risk assessment and mitigation process is in place, it could be agreed by the designated authority that the approval of a number of major changes be delegated to the ATM Service Provider under specified conditions.

Care should however be recommended as States should not discharge its responsibility upon the industry and should maintain its overall control of its safety oversight functions.

In the case of total or partial delegation to the ATM service provider, safety oversight would then rely more heavily on "on going safety oversight".

3.6.3 Third Party ESARR 4 Initial Safety Oversight

It is considered that the initial safety oversight of major changes should never be delegated to a third party even if "accredited to perform such functions for non-major changes".

(Space Left Intentionally Blank)

4. ON-GOING SAFETY OVERSIGHT

4.1 Introduction

4.1.1 General Considerations

A State's obligation and responsibility for a safe ATM System does not end with the issuance of a safety regulatory approval.

A State shall ensure that all privileges granted by such an approval are not exercised unless the holder maintains compliance with ESARR 4 compliant national regulations.

Maintenance of continued compliance with ESARR 4 demands that a State therefore establishes a system of continued control and supervision, in order to ensure continuing validity of safety regulatory approvals.

This system is called in this Document "on going safety oversight".

The continued validity of a safety regulatory approval is dependent on the ATM service provider maintaining compliance with the safety requirements established for its issuance. The designated authority should therefore be given the authority to conduct safety regulatory audits and inspections, and to grant, modify, renew, suspend, revoke, or terminate a safety regulatory approval.

Additionally, the designated authority should have the responsibility for exercising continuing surveillance over the ATM provider's operations, to ensure that acceptable risk assessment and mitigation practices are maintained and to verify that tolerable safety levels are met.

4.1.2 On-going Safety Oversight Procedures

4.1.2.1 Scope of On-going Safety Oversight Activities

Throughout all phases, the surveillance programme, the standards and service provider's capabilities in risk assessment and mitigation should be equal to or exceed those required at the time of initial approval.

Safety regulatory audits and inspection against ESARR 4 compliant national regulations should contribute to determining if the ATM service provider meets the provisions of ESARR 4 national regulations on a continuous basis and if risk assessment and mitigation processes are conducted as documented.

On going safety oversight should also determine the capacity of the service provider to conduct those risk assessment and mitigation processes as documented, and in a manner compliant with ESARR 4 national regulations.

This includes determining the adequacy of resources, of allocation of responsibilities, existence and adequacy of internal instructions, information dissemination process and of all other means necessary to conduct risk assessment and procedures.

In addition, on going safety oversight should determine if that all changes in the applicable national regulations are reflected in the documented risk assessment and mitigation procedures of the ATM service provider.

On going safety oversight also caters for those changes to the ATM System, which were classified as “non-major”.

Furthermore, on going safety oversight has to be able to evaluate the individual parts of the ATM system as well as the integration of such part;

- The safety regulatory audits and inspections should verify the overall consistency of a multitude of safety arguments and their consistent implementation in a single ATM system;
- Equally, on going safety oversight has to be able to evaluate the interface of the ATM System under the managerial control of service provider with other external systems with which it interfaces (such as MET systems, AIS, aircraft systems, externally supplied systems). It is indeed important to conduct safety regulatory audits and inspection in sufficient depth and scope to be satisfied that the organisation has considered any interrelationships in its risk assessment and mitigation.

Finally, the scope of the safety regulatory audits and inspections should be determined taking into account the outcome of past safety regulatory audits and identified issues.

In view of increasing complexity of the ATM System as well as of the institutional changes taking place in the ATM industry, it is also recommended to review periodically the scope and depth of the safety regulatory audits and inspections.

4.1.2.3 Programmed and Random On-going Safety Oversight

Required on going safety oversight activities should be planned and conducted by the designated authority.

On going safety oversight should be accomplished on a continuing basis, performed at specified times or intervals, or conducted in conjunction with the renewal of a safety regulatory approval.

Scheduled safety regulatory audits and inspections must be augmented by a periodic random audit and inspection of all facets of the operations related to risk assessment and mitigation.

In view of increasing complexity of the ATM System as well as of the institutional changes taking place in the ATM industry, it is also recommended to review periodically the periodicity of safety regulatory audits and inspections.

The designated authority should also be able to initiate ad-hoc actions in the event of an urgent safety problem.

4.1.2.4 Existence of Safety Management System

This document assumes a national implementation of Safety Management Systems in service providers, in a manner consistent with ESARR 3. Obviously, the on going safety oversight activities related to ESARR 3 would serve as a sound basis for some of the ESARR 4 on going safety oversight activities. (Refer to EAM 3 / GUI 3 ‘ESARR 3 and related Safety Oversight’).

In particular, ESARR 3 on going safety oversight could be used as a baseline for some planned ESARR 4 on going safety oversight activities, and more specifically when;

- assessing the acceptability of the proposed risk assessment and mitigation processes (initial acceptance and acceptance of changes to the processes),
- verifying compliance of the implemented processes with ESARR 4 required processes.

The degree to which SMS is being implemented in one service provider obviously would drive the level of additional on going safety oversight required to verify compliance with the requirements for risk assessment and mitigation.

4.2 Assessment of Safety Documentation

4.2.1 Risk Assessment and Mitigation Procedures

The ATM service providers should have documented, within its own safety management system, its internal procedures for risk assessment and mitigation of changes to the ATM System under its managerial control.

These internal risk assessment and mitigation processes should be assessed by safety oversight staff to verify compliance of declared procedures with ESARR 4 compliant national regulations.

It is recommended that such preliminary assessment be undertaken before the actual safety regulatory audits against ESARR 4 compliant regulations takes place as this will facilitate the preparation of the audit protocols. Indeed, the more thoroughly the preliminary assessment is conducted, the less likelihood there will be of having serious problems in the course of safety regulatory audits and inspections.

This assessment should provide the ESARR 4 safety oversight staff with a determination on the adequacy of those procedures (and potential modifications) and with an appreciation of the potential ability of the service provider to conduct risk assessment and mitigation in accordance with ESARR 4 compliant national regulations;

- If the assessment indicates major non-compliance and deficiencies, the safety oversight staff should require rectification before initiating a safety regulatory audit or an inspection;
- If the assessment indicates only minor deficiencies, the safety oversight staff may decide to conduct a safety regulatory audit and or inspection in order to determine the service provider capability to effectively carry out the procedures as documented.

(Space Left Intentionally Blank)

4.3 Assessment of Procedures

4.3.1 Objectives

The ATM service provider risk assessment and mitigation procedures, as documented in its Safety Management System, and implemented on a daily basis, should ensure full compliance with ESARR 4 compliant national regulations.

The safety regulatory audit aims at verifying compliance of implemented risk assessment and mitigation procedures with ESARR 4 compliant national regulations. It should also confirm that risk assessment and mitigation procedures, as documented in the Safety Management System are being followed and are effective regarding their compliance with ESARR 4 national regulations.

In addition, the regulatory audits should determine if all changes in the applicable ESARR 4 compliant national regulations are being implemented.

4.3.2 General Principles

Refer to Section 3.3.2.

While the scope of national regulations will need to be extensive enough, it is not feasible or desirable to attempt to cover every conceivable operational detail.

Of specific interest to safety regulatory audits performed as part of 'on going safety oversight' is the verification that an adequate management process is in place to handle;

- potential various levels of safety arguments (e.g. for operational units, major systems or operational capabilities),
- their overall consistency, and
- the modifications of safety arguments.

The safety regulatory audits should also confirm the capacity of the service provider to conduct those processes as documented, i.e. if associated resources, responsibilities and internal instructions, information dissemination necessary to conduct risk assessment and procedures are being effectively implemented.

4.4 Assessment of the ATM System

4.4.1 Objectives

This assessment usually forms part of a safety regulatory audit and aims at verifying the ATM System and constituent parts against allocated safety requirements and applicable safety standards/published specifications as well as national ATM safety minima.

4.4.2 General Principles

Such assessment should allow verification of all records related to risk assessment and mitigation processes and analysis of ATM safety occurrences.

The assessments would focus on;

- Verifying the continuous validity of assumptions made in various safety arguments with examination of evidence,
- Verification of continuous implementations of safety requirements, with examination of evidence,
- Verification of effectiveness of implemented mitigation measures, with examination of evidence, and
- Verification that minimum tolerable safety minima are met, with examination of evidence (Refer to Section 4.3.7).

4.4.3 Non-Major Changes

There must be a system in place to ensure that changes do not adversely effect safety. The system must ensure that the significance of changes is assessed against clear criteria and associated rationale documented. The ATM service provider ought to;

- establish evidence of ESARR 4 requirement compliance and satisfy itself that safety will be kept, as a minimum, within safety minima,
- document as early as possible when defining the proposed change, the rational for the significance classification of that proposed change. This should be made available to the designated authority at any time.

If, according to the procedures promulgated by the designated authority (refer to section 2.1.2), the change is classified as ‘non-major’ the designated authority may only be provided with;

- a short description of the change,
- the rationale for the classification ‘non-major’ at the time of the change.

The designated authority should have every right to disagree with the proposed classification.

Note: An alternative would be that the designated authority is not informed immediately and gets its first sight of the list of “non major” changes during agreed routine reporting intervals or during programmed ESARR 4 or ESARR 3 types of safety regulatory audits and inspections.

The regulatory assessment will enable the designated authority to assess the effective implementation of those criteria and related procedures on a number of “non-major changes” to verify in particular, that some changes have not been under-estimated. Evidence of the “non major” classification of a number of changes should be requested during an audit and examined.

4.4.4 Operational Documentation

There must be a system in place to ensure that the impact of changes is adequately reflected in the operational documentation.

An examination of documents such as the following, as well as the determination of their overall consistency with the outcome of all safety arguments would be essential;

- The Aeronautical Information Service is key to airspace users and reflect what is required of operators to ensure the safety of the airspace,
- The operational Manual is also a key document as ATCO will base their daily work on its contents; it should also reflect all relevant safety requirements as determined in the course of current[26] safety arguments,
- Similarly, the Maintenance Manual should also reflect all relevant safety requirements determined in the course of current[27] safety arguments,
- The engineering Manual should also reflect all relevant safety requirements determined in the course of current[28] safety arguments, and
- The training Manual should also reflects the existence of current safety requirements.

4.4.5 Interfaces

Safety oversight staff have to be able to evaluate the interface of the ATM System under managerial control of one service provider with external stakeholders (MET authority, AIS, aircraft manufacturers, operators, external suppliers other ATM service providers).

The regulatory assessment would enable the examination of proofs that such internal and external co-ordination mechanisms are in place as well as the necessary promulgation of safety objectives and requirements to organisations or units responsible for their implementation.

Examination of all key documents tracking the status of the interfaces being maintained with stakeholders should be undertaken during regulatory assessments (e.g. letters of agreement).

In particular, evidence of that a Total System Approach is being adopted should be examined.

4.4.6 Use of Analysis of ATM Safety Occurrences

ATM service providers should use safety performance indicators to help them assess the effectiveness of their Safety Management Systems, including their risk assessment and mitigation processes.

The validity of safety assumptions made in the course of risk assessment and mitigation and the effectiveness of safety mitigation measures adopted could also be monitored.

---

[26] *Current means "valid", i.e. still in force.*

[27] *Current means "valid", i.e. still in force.*

[28] *Current means "valid", i.e. still in force.*

The ATM service providers could maintain a database of hazards, associated severity of effect and rationale and mitigation means, the contents of which could be assessed against the results of the monitoring process.

Such indicators could help the providers in being pro active but also could be audited by the designated authority, when verifying the validity of safety objectives and requirements as well as the overall performance of the ATM System against agreed tolerable ATM safety minima.

4.4.7 Safety Oversight of the human element in the Safety Assessment

The first part of the safety assessment is to assess the safety functional requirements. The safety assessment should address the functional requirements falling on the human element of the system and are associated with what the human should do when presented with a given situation. This includes consideration of human behavior in various emergency situations and new system fault and reduced functionality modes. The most obvious is training in unusual circumstances and emergency procedures. These would normally be captured in operational and training documentation. It would then be the role of Safety Oversight with ESARR 5 to ensure that such training has been given.

The second part of the safety assessment is to assess the ability (or inability) of the human to react in a given manner. This relates to the safety performance requirements. Such requirements should be considered in terms of workload and competence. While the issue of human reliability is too detailed to address here, certain brief guidelines can be given. Human reliability relates to how many tasks the human has to undertake, the complexity of these tasks, the novelty of these tasks, the time allocated to undertake the tasks, the degree of information to assimilate to undertake the tasks. Etc.

4.5 Reporting and Follow-Up

4.5.1 Reporting

Refer to SRC Policy Document 3, Annex 2.

4.5.2 Follow up

Refer to SRC Policy Document 3, Annex 2.

Should the ATM service provider fail to take adequate remedial actions, the designated authority could limit the scope of the holder’s approval. In particular, it could be prevented to undertake any major changes the ATM System under its managerial control.

(Space Left Intentionally Blank)

4.6 Safety Regulatory Approval

4.6.1 General

On going safety oversight can provide the basis for suspension, modification, limitation or renewal of an initial approval.

4.6.2 Delegation of On-going Safety Oversight Responsibilities

In some instances, where a sound and mature risk assessment and mitigation process is in place, it could be agreed that the approval of a number of non-major changes be delegated to the ATM Service Provider.

States should however maintain its overall control of its safety oversight functions and should implement a reliable “on going safety oversight” programme.

4.6.3 Third Party ESARR 4 On-going Safety Oversight

In some instances, where the designated authority is poorly resourced, it could be agreed that the approval of a number of non-major changes be delegated to a third party organisation, accredited to perform such functions by the designated authority.

This could present an advantage if such a third party was to be accredited European-wide as the workload of accrediting and overseeing a third party organisation would also require some resources.

(Space Left Intentionally Blank)

APPENDIX A – TERMS AND DEFINITIONS

TERM	DEFINITION
Accident	As per ICAO Annex 13
Assessment	An evaluation based on engineering, operational judgement and/or analysis methods. *(An appraisal of procedures or operations based largely on Experience and professional judgement* *(ICAO DOC 9735))*
ATM	The aggregation of ground based (comprising variously ATS, ASM, ATFM) and airborne functions required to ensure the safe and efficient movement of aircraft during all appropriate phases of operations.
ATM Service-Provider	An organisation responsible and authorised to provide ATM service(s)
AMC	Acceptable Means Of Compliance
ESARR	EUROCONTROL Safety Regulatory Requirement (see Safety Regulatory Requirement)
External Services	All material and non-material supplies and services, which are delivered by any organisation not covered by the ATM Service-Provider's Safety Management System.
Incident	An occurrence, other than an accident, associated with the operation of an aircraft, which affects or could affect the safety of operation.
Level of Safety	A level of how far safety is to be pursued in a given context, assessed with reference to an acceptable or tolerable risk.
PMC	Proposed Means Of Compliance
Regulation	The adoption, enactment and implementation of rules for the achievement of stated objectives by those to whom the regulatory process applies.
Safety Management System (SMS)	A systematic and explicit approach defining the activities by which safety management is undertaken by an organisation in order to achieve acceptable or tolerable safety

TERM	DEFINITION
Safety Oversight	The function undertaken by a designated authority to verify that safety regulatory objectives and requirements are effectively met.
Safety Performance	The measurement of achieved safety within the overall ATM system performance measurement.
Safety Regulatory Requirement	The formal stipulation by the regulator of a safety related specification which, if complied with, will lead to acknowledgement of safety competence in that respect.
Safety Regulatory Audit	Verify Written procedures and arrangements against required procedures and arrangements; And/or actual processes and their results against written procedures and arrangements[29].
Safety Regulatory Inspection	Verify products, services or specified parts of the ATM System against specifications required and previously published by the Safety Regulator.
SRC	Safety Regulation Commission
System	A combination of physical components, procedures and human resources organised to perform a function.

Note: Not all definitions included in ESARR 4 are listed in this Appendix.

(Space Left Intentionally Blank)

[29] *This also includes verification of compliance with allocated objectives, mitigation measures and any other arrangement identified as a result of the procedures carried out by the ATM service-provider.*

APPENDIX B – GUIDANCE ON THE CRITERIA FOR THE ASSESSMENT OF COMPLIANCE WITH ESARR 4

This table has been produced to provide NSAs with guidance to support the development of criteria for the assessment of compliance with ESARR 4.

This material is of particular interest when developing a strategy to verify the implementation of ESARR 4-related requirements in the context of the certification and ongoing oversight of ANSPs against the Common Requirements established in Commission Regulation (EC) 2096/2005. As such, the table is referenced to in EAM 1 / GUI 5 'ESARR 1 in the Certification and Designation of Service Providers'.

This table also contains indications about the possible use of its contents by NSAs. In particular, it should be noted that this material only provides guidance on possible evidences and possible ways to evaluate them. The range of contents from this table that may support the NSA in a specific situation will normally depend upon the case. In particular, different approaches will be needed for initial and ongoing safety oversight. NSAs are expected to define their strategy regarding the necessary actions and level of verification consistently with the recommendations of EAM 1 / GUI 3 and EAM 1 / GUI 5. The evidences and ways to assess them will also depend on the implementing arrangements put in place by the ANSP to meet the requirement.

(Space Left Intentionally Blank)

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes

NOTES ABOUT THE USE OF THIS TABLE

a) The table provides indications about evidences that can be expected to be found to show compliance with the requirement. These evidences illustrate a means, but not necessarily the only possible means, by which a requirement can be met. Evidences to be looked at will depend on how ANSP intends to implement safety requirement in its SMS procedures.

b) Guidance is also included about some possible ways to assess these evidences. Depending upon the case only a limited set of the actions proposed, or other alternative or additional actions, may be needed to assess the evidences under consideration. NSAs are expected to define their strategy regarding the necessary actions and level of verification in a manner consistent with the recommendations of EAM 1 / GUI 3 and EAM 1 / GUI 5. In particular, different approaches will be needed for initial and ongoing safety oversight.

c) Indications of possible evidences are given not only regarding the existence of written arrangements/procedures but also in relation to their effective implementation. This latter aspect is normally demonstrated by means of evidences which exist after allowing a period for the effective operation of the written arrangements/procedures.

d) Sampling is proposed to assess the effective implementation of various arrangements. As a general rule, it is recommended that samples include at least 10% of the units relevant to the case under consideration over a specific period of time. Wherever sampling is proposed, the comments/notes normally include an indication of the sampling unit.

5.1	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:	*Common Requirements* *Annex 2, 3.2.1* Within the operation of the SMS, a provider of air traffic services shall ensure that hazard identification as well as risk assessment and mitigation are systematically conducted for any changes to those parts of the ATM functional system and supporting arrangements within his managerial control, in a manner which addresses: [...]	Risk assessment and mitigation procedure(s): • Elements showing that procedures are in place (e.g. status, approval signatures applicability date, etc.), • Elements describing the process, its applicability and scope. • Allocation of responsibilities throughout the process	Check that documented procedure(s) are in place for hazard identification and risk assessment and mitigation. Check that the scope of the process is identified and documented: • The process described applies to any changes to those parts of the ATM system within the managerial control of the ANSP. • In particular, check that the process applies to any change to supporting services within the managerial control of the ANSP. • Coordination actions are foreseen when a change is outside the managerial control of the ANSP • The ‘changes’ to the ‘ATM system’ are qualified and an analysis of their impact within the ATM system exists Check the existence of means by which the changes to the system are controlled (configuration management) Check that responsibilities are allocated in the process	The term ‘change’ should be understood as a new system or a change to an existing system. ‘Functional system’ in Common Requirements is equivalent to ‘system’ in ESARRs. The “managerial control” of the ANSP should be identified and covered The “systematic” nature of the action should be demonstrated.

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
			Records documenting the identification of changes subject to the process.	First of all, request a presentation of the operational and technical changes within the ATM system. Secondly, in order to assess the evidences related to the effective implementation of all the provisions contained in 5.1, consider a sample of changes. The sample should be selected by the NSA and include enough changes to cover: • Changes to supporting services within the managerial control of the ANSP. • Changes at different stages of their lifecycle. • Changes which concern airborne and ground components. • Changes which concern human, procedures, airspace and equipment. • Changes which concern different ATM operational units and different types of ATM services provided by the ANSP. Review the application of the relevant procedure(s) to this sample in order to check: • That all changes were addressed, or are being addressed, through the application of the procedure(s).	To note that it is proposed to use the same sample in relation to all ESARR 4 provisions under Section 5.1. Depending upon the case, this sample could be same one used in relation to 5.2 and/or 5.3. (sampling unit = change to a part of the ATM system and the supporting services under the ANSP's managerial control). The sampling may take place after considering a list of the new systems and changes to existing systems within the managerial control of the ANSP. To note that ESARR 1 contains provisions on the safety oversight of changes. To note that Articles 5(2) and 5(3) of the CRs establish that a certified air navigation service provider shall notify the national supervisory authority of: • Planned changes to its provision of services which may affect its compliance with the applicable common requirements or with the conditions attached to the certificate. • Planned safety related changes to the provision of air traffic services

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
5.1.1 a)	addresses the 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;	*Common Requirements* *Annex 2, 3.2.1* [...] the complete life-cycle of the constituent part of the ATM functional system under consideration, from initial planning and definition to post-implementation operations, maintenance and de-commissioning; [...]	Risk assessment and mitigation procedure(s): • Elements describing the process, its applicability and scope and the responsibilities for the actions.	Check that the process described in the procedure(s) address(es) the: • 'initial planning' phase; • 'definition' phase'; • 'operations' phase; • 'post implementation' phase; • 'maintenance phase; • 'de-commissioning' phase; of the constituent part of the ATM system under consideration.	
			Records documenting the conduct of risk assessment and mitigation and its results	Within the sample of changes selected in 5.1 above, check that all the life-cycles phases were addressed, or are planned to be addressed, for each change.	
5.1.1 b)	addresses the airborne and ground[30] components of the ATM System, through co-operation with responsible parties; and;	*Common Requirements* *Annex 2, 3.2.1* [...] the airborne, ground and, if appropriate, spatial components of the ATM functional system, through co-operation with responsible parties; and [...]	Risk assessment and mitigation procedure(s): • Elements describing the process, its applicability and scope and the responsibilities for the actions.	Check that the process described in the procedure(s) address(es) the airborne, spatial and ground components of the ATM system concerned by the change. Check that the process includes steps for cooperation with responsible parties wherever a change concerns components (airborne and/or ground) of the ATM system outside the managerial control of the ANSP.	
			Cooperation arrangements with relevant responsible parties.	Check the existence of co-operation arrangements agreed with relevant responsible parties as regards changes concerning components (airborne and/or ground) of the ATM system outside the managerial control of the ANSP.	To note that the nature, context and scope of co-operation arrangements may vary depending upon the case.

[30] *Including spatial components.*

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
			Records documenting the: • Determination of scope, boundaries and interfaces • Co-operation with responsible parties • Results from these actions • Configuration control and change management (how the changes are controlled)	Within the sample of changes selected in 5.1 above, check that for each change: • The assessment of the impact on airborne of spatial component is performed , • It has been identified whether the change concerns components (airborne, spatial and/or ground) of the ATM system outside the managerial control of the ANSP, • The components concerned are identified, • The parties responsible for these components are identified, • Co-operation has taken place or is planned, Wherever cooperation was completed, results from that cooperation can be shown in terms of appropriate measures related to the implementation of the change by all the parties involved and AIS (notifying required to equipage or to given airspace block).	

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
5.1.1.c)	addresses the 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.	*Common Requirements* *Annex 2, 3.2.1* [...] the equipment, procedures and human resources of the ATM functional system, the interactions between these elements and the interactions between the constituent part under consideration and the remainder of the ATM functional System.	Risk assessment and mitigation procedure(s): • Elements describing the process, its applicability and scope and the responsibilities for the actions.	Check the capability to perform an analysis of the impact of the change. Check that the process described in the procedure(s) address(es) the: • Human; • Procedures; and • Equipment. concerned by the changed as well as the: • Interactions between them; • Interactions between the constituent part under consideration and the remainder of the ATM system. And propose ways to address them in detail : • Software black o white boxes • Man-machine interfaces, etc.	An “impact analysis of changes” is a means to identify all the possible components of the system which are impacted by the change
			Records documenting the conduct of risk assessment and mitigation and its results.	Within the sample of changes selected in 5.1 above, check that for each change: • Human, procedure and equipment elements are considered if they are concerned, • Interactions between them are identified and subsequently addressed according to the procedures, • Interactions between the part under consideration and the remainder of the ATM system are identified and subsequently addressed according to the procedures.	

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
5.2	The hazard identification, risk assessment and mitigation processes shall include:	*Common Requirements* *Annex 2, 3.2.2* The hazard identification, risk assessment and mitigation processes shall include: [...]	All evidences related to the 5.2. Sub-sections below.	In order to assess the evidences related to the effective implementation of the provisions contained in 5.2, consider a sample of changes. The sample should be selected by the NSA and include enough changes to cover: • Changes to supporting services within the managerial control of the ANSP. • Changes at different stages of their lifecycle. • Changes which concern airborne, spatial and ground components. • Changes which concern human, procedures and equipment. • Changes which concern different ATM operational units and different types of ATM services provided by the ANSP.	The existence of documented procedure(s) for hazard identification and risk assessment and mitigation should have been verified in relation to 5.1. The following sections elaborate further the specific elements to be contained in the process. To note that it is proposed to use the same sample in relation to all ESARR 4 provisions under Section 5.1. Depending upon the case, this sample could be same one used in relation to 5.1 and/or 5.3. (sampling unit = change to a part of the ATM system and the supporting services under the ANSP's managerial control).

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
5.2 a	A determination of the 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;	*Common Requirements* *Annex 2, 3.2.2* [...] (a) A determination of the 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; [...]	Risk assessment and mitigation procedure(s): Elements describing: • Determination of scope, boundaries and interfaces, • Identification of functions of the constituent part under consideration, • Environment of operations, • Results expected in regard to these points. • Plan of actions for the agreement and implementation of safety requirements	Check that the procedures(s) define(s) actions to provide guidance and how to determine: • The scope, • Boundaries, and • Interfaces. of the constituent part being considered, as well as the: • functions that the constituent part is to perform, • environment of operations in which it is intended to operate. Check that the procedure(s) include(s) appropriate cooperation with parties responsible for developing/implementation of safety requirements. Check that the procedures(s) define(s) means to collate the results from these actions.	To note that the "safety requirements" are aiming at the safety improvement of the system. They can be defined by the specification of the change, as safety constraints. They can be the result of the application of the regulation or the result of an approved safety assessment and mitigation process.
			Records documenting the: • determination of scope, boundaries and interfaces; • identification of functions of the constituent part under consideration; • identification of its environment of operations; and • results from these actions • Plan of actions for the agreement and implementation of safety requirements.	Within the sample of changes selected in 5.2 above, check that for each change the: • actions conducted conformed with the relevant procedure(s), • scope, boundaries, interfaces, functions and environment of operations were determined for the constituent part under consideration, • results from that determination were collated, • applicable regulatory requirements were identified and referenced, • activities depicted in 5.2 a) are fully coordinated between those parties responsible for developing and/or implementing the safety requirements bearing on the constituent part under consideration or on other parts of the ATM system or the environment of operations.	

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
5.2 b	A determination of the safety objectives to be placed on the constituent part, incorporating	*Common Requirements* *Annex 2, 3.2.2* [...] A determination of the safety objectives to be placed on the constituent part, incorporating: [...]	All evidences related to the bullets of 5.2 b) below.	Check the implementation of 5.2 b i) ii) iii). When checking these points, consider the articulation of 5.2 b i) ii) iii) into an overall process to determine safety objectives to be placed on the constituent part. Check also that the activities depicted in 5.2 b are fully coordinated between those parties responsible for developing and/or implementing the safety requirements bearing on the constituent part under consideration, or on other parts of the ATM system or the environment of operations.	
5.2 b i)	an identification of ATM-related credible hazards and failure conditions, together with their combined effects	*Common Requirements* *Annex 2, 3.2.2* [...] An identification of ATM-related credible hazards and failure conditions, together with their combined effects; [...]	Risk assessment and mitigation procedure(s): Elements describing: • Hazard identification, • Results expected in regard to these points.	Check that the procedures(s) define(s) a systematic process to identify: • ATM-related credible hazards, • ATM-related credible failure conditions, • Combined effects of ATM-related credible hazards and failure conditions. In addition, when checking these points consider the provisions mentioned on this table regarding paragraph 1 of Appendix A-1 (i.e. identification of hazards takes place prior to assessing the risk). Check that the procedures(s) define(s) means to collate the results. Check the update of the hazard log if subsequent steps or processes confirm the need to add or modify the list.	Depending upon the case the activities to be conducted when performing the procedure(s) actions may include: • Functional hazard assessment (FHA). • Trials, simulations, experts' brainstorming, etc. • Review of operational data, databases, etc. • Hazard log See 5.2 b) above. See Appendix 1, Para 1, below.

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
			Records documenting the hazard identification process and its results.	Within the sample of changes selected in 5.2 above, check that for each change: • The actions conducted conformed with the relevant procedure(s), • ATM-related credible hazards and failure conditions and their combined effects were determined, • The results from that determination were collated and updated, if needed. In addition, when checking these points, consider the provisions mentioned on this table regarding paragraph 1 of Appendix A-1 (i.e. identification of hazards takes place prior to assessing the risk). Check that the procedures(s) define(s) means to collate the results.	See 5.2 b) above. See Appendix 1, Para 1, below.
			Qualification of operational personnel involved in the hazard identification process.	Check that criteria exist to define the people qualified to contribute to an identification of hazards when implementing the procedure. Review the criteria to assess whether that operational staff involved, or other stakeholders, if coordination is needed, have qualifications which are relevant to the operations under consideration. Review the application of the criteria to a specific sample selected by the NSA. More specifically, check that people involved met the relevant criteria at the time the hazard identification was conducted.	FHA techniques need the involvement of personnel qualified to contribute to the identification of hazards. This is an essential component to obtain 'credible' hazards as required in ESARR 4. (sampling unit = operational expert, such as ATCO or aircrew, involved in the identification of hazards through FHA techniques).

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
5.2 b 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,	*Common Requirements* *Annex 2, 3.2.2* [...] 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 Section 4 [...]	Risk assessment and mitigation procedure(s): Elements describing: • Assessment of the effects of hazards on aircraft safety, • Assessment of the severity of those effects, • Severity classification scheme used, • Results expected in regard to these points.	Check that the procedures(s) define(s) a systematic process to: • Address all hazards identified, • Assess the effects on operations that need to be considered including: o Effects on the ability to provide or maintain safe services, o Effects on the functional capabilities of the airborne and ground parts of the ATM system, o Effects on ATCO and/or aircrew, o Effects on the environmental mitigation measures (which are not part of the constituent par under consideration). • Assign a severity to each effect identified, • Use the severity classification scheme required in ESARR 4 Figure A-1 when assigning the severity. In addition, when checking these points, consider the provisions mentioned on this table regarding Appendix A. Check that the procedures(s) define(s) means to collate the results. Check the rationale described or the procedure used to qualify the “probable effect under the worst case scenario” to assess if statistically sound.	See 5.2 b) above. See Appendix 1 below.

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
			Records documenting the assessment of effects of hazards and their severity and the results from this action.	Within the sample of changes selected in 5.2 above, check that for each change: • The actions conducted conformed with the relevant procedure(s), • All the hazards resulting from the identification of hazards were considered, • All potential effects on operations have been considered, • Each effect has been assigned a severity on a sound basis 5credible effect under the worst case scenario) • The severity was assigned by using the severity classification scheme of ESARR 4 Figure A-1, • A rationale for the severity assignment is stated for each effect, • The results were properly collated with their justification. In addition, when checking these points, consider the provisions mentioned on this table regarding Appendix A.	See 5.2 b) above. See Appendix 1 below.

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
5.2 b 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.	*Common Requirements* *Annex 2, 3.2.2* [...] 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 Section 4 [...]	Risk assessment and mitigation procedure(s): Elements describing: • Determination of tolerability of hazards in terms of maximum rate of occurrence, • Risk classification scheme, • Results expected in regard to these points.	Check that a risk classification scheme has been developed / included in procedures and that the derivation of maximum probability for classes 2 to 5 is sound and justified. More specifically, check that the procedures(s) define(s) a systematic process which: • Addresses all the hazards identified, • Obtains safety objectives expressing the tolerability of the hazards in terms of maximum rate of occurrence, • Derives the hazard's tolerability from the severity of the effect of the hazard and the maximum rate of the occurrence of the hazard, • Derives the hazard's tolerability by using a risk classification scheme consistent with ESARR 4 Appendix A. In addition, when checking these points, consider the provisions mentioned on this table regarding Appendix A. Check that the procedures(s) define(s) means to collate the results.	The term *'severity'* should be understood as *'severity of the effect of the hazard'.* See 5.2 b) above. See Appendix 2 below. To note that no equivalent to the ESARR 4 Figure A-2, exists in the CRs.

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
			Records documenting the assessment of effects of hazards and their severity and the results from this action.	Within the sample of changes selected in 5.2 above, check that for each change the: • Actions conducted conformed with the relevant procedure(s), • Output of these actions is a set of safety objectives, • Safety objectives specify the hazards tolerability in terms of the hazards maximum rate of occurrence, • Risk classification scheme is clearly referenced and has been used, • Risk classification scheme used is consistent with ESARR 4 Appendix A, • Safety objectives are traceable to identified hazards, • Results were properly collated and justified. In addition, when checking these points, consider the provisions mentioned on this table regarding Appendix A.	See 5.2 b) above. See Appendix 2 below.
5.2 c	the derivation, as appropriate, of a risk mitigation strategy which:	*Common Requirements* *Annex 2, 3.2.1* [...] (c) The derivation, as appropriate, of a risk mitigation strategy which: [...]	All evidences related to the bullets of 5.2 c) below.	Check the implementation of 5.2 c i) ii) iii). When checking these points, consider the articulation of 5.2 c i) ii) iii) into an overall process to determine safety requirements bearing (as appropriate) on: • The constituent part under consideration, • Other parts of the ATM system, • The environment of operations. Check also that the activities depicted in 5.2 c) are fully coordinated between those parties responsible for developing and/or implementing the safety requirements bearing on the constituent part under consideration or on other parts of the ATM system or the environment of operations.	

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
5.2 c i)	specifies the defences to be implemented to protect against the risk-bearing hazards[31],	*Common Requirements* *Annex 2, 3.2.1* [...] (i) specifies the defences to be implemented to protect against the risk-bearing hazards, [...]	Risk assessment and mitigation procedure(s): Elements describing: • Determination of risk mitigation strategy, • Results expected in regard to this point.	Check that the procedures(s) define(s) a systematic process to produce a risk mitigation strategy which: • Addresses all the safety objectives, • Specifies the defences to be implemented, and • These defences are intended to meet the safety objectives obtained from the application of 5.2 b) and, consequently, reduce and/or eliminate the risks induced by the identified hazards. Check that the procedures(s) define(s) means to collate the results.	See 5.2 c) above.
			Records documenting the determination of risk mitigation strategy and the results from this action. • Documenting the validation and agreement of the implementation of safety requirements	Within the sample of changes selected in 5.2 above, check that for each change: • The actions conducted conformed with the relevant procedure(s) • Defences were defined • The defences are traceable to the safety objectives obtained from the application of 5.2 b) and, consequently, to the identified hazards • The results were properly collated and justified, • The responsibilities for the implementation of the defences are allocated	See 5.2 c) above.

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

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
5.2 c ii)	includes, as necessary, the development of safety requirements[32] potentially bearing on the constituent part under consideration, or other parts of the ATM System, or environment of operations, and	*Common Requirements* *Annex 2, 3.2.1* [...] (ii) includes, as necessary, the development of safety requirements potentially bearing on the constituent part under consideration, or other parts of the ATM System, or environment of operations, and [...]	Risk assessment and mitigation procedure(s): Elements describing: • Determination of risk mitigation strategy, • Results expected in regard to this point.	Check that the procedures(s) define(s) actions forming a systematic process which: • Addresses the safety objectives as necessary; • Includes the development, as necessary, of safety requirements; • Includes appropriate cooperation with parties responsible for developing/implementation of safety requirements; and • These safety requirements bear, as necessary; on: o The constituent part under consideration; o Other parts of the ATM system; o The environment of operations. Check that the procedures(s) define(s) means to collate the results. Check that the procedure(s) allocate responsibilities with regard to the implementation of safety requirements.	Checking cooperation with other parties is mentioned with regard to 5.2 c. However it should be noted that this aspect is particularly important regarding 5.2 c ii). See 5.2 c) above.

[32] *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.*

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
			Records documenting the determination of risk mitigation strategy and the results from this action. • Documenting the validation and agreement of the implementation of safety requirements	Within the sample of changes selected in 5.2 above, check that for each change: • The actions conducted conformed with the relevant procedure(s), • The development of safety requirements was addressed as necessary in cooperation with parties responsible, • As a result, safety requirements were defined as necessary, • The safety requirements are traceable to the safety objectives obtained from the application of 5.2 b) and, consequently, to the identified hazards, • The results were properly collated with the allocation of responsibilities	See 5.2 c) above.
5.2 c iii)	presents an assurance of its feasibility and effectiveness[33];	*Common Requirements* *Annex 2, 3.2.1* [...] (iii) presents an assurance of its feasibility and effectiveness ; [...]	Risk assessment and mitigation procedure(s): Elements describing: • Determination of risk mitigation strategy, • Results expected in regard to this point.	Check that the procedures(s) define(s) a systematic process to produce a risk mitigation strategy which: • Includes assurances of its feasibility and effectiveness, by showing that it is: o Comprehensive (addressing both potential causes and potential consequences of identified hazards), o Able to reduce the risk to a tolerable level in an environment assumed, o Testable when implemented. o Feasible Check that the procedures(s) define(s) means to collate the results.	To note that 'assurances' will normally be based on analysis whose 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. See 5.2 c) above. Possible use of simulation and modelling.

[33] *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.*

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
			Records documenting the determination of risk mitigation strategy and the results from this action.	Within the sample of changes selected in 5.2 above, check that for each change the: • Actions conducted conformed with the relevant procedure(s), • Risk mitigation strategy includes assurance of its feasibility and effectiveness based on an analysis and detailed arguments, at the appropriate level, • Risk mitigation strategy is: o Comprehensive (addressing both potential causes and potential consequences of identified hazards), o Able to reduce the risk (includes arguments to show that it reduces or controls the risk, o Credible (this can be proven, for example, by stakeholder endorsement of the process and conclusions), o Testable when implemented (this is typically an expert judgement that may, for example, be supported through peer review or other means). • Assurances of feasibility and effectiveness cover all the identified hazards, • Results were properly collated.	See 5.2 c) above. Possible use of simulation and modelling.

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
5.2 d	Verification that all identified safety objectives and safety requirements have been met:	*Common Requirements* *Annex 2, 3.2.1* [...] (d) Verification that all identified safety objectives and safety requirements have been met [...]	All evidences related to the bullets of 5.2 d) below. In addition, it should exist a description of the overall verification and validation processes with regard to the implementation of changes	Check the implementation of 5.2 d i) ii) iii). When checking these points, consider the articulation of 5.2 d i) ii) iii) into an overall process to verify that all identified safety objectives and safety requirements have been met. Check also that the activities depicted in 5.2 d) are fully coordinated between those parties responsible for developing and/or implementing the safety requirements bearing on the constituent part under consideration or on other parts of the ATM system or the environment of operations. In addition, when checking these points, consider the provisions mentioned on this table regarding Appendix A-2, paragraph 2 (i.e. application of additional safety management considerations whenever reasonable).	The testing process should include the safety management principles with regard to the verification and validation process.
5.2 d i)	prior to its implementation of the change	*Common Requirements* *Annex 2, 3.2.1* [...] • Prior to its implementation of the change, [...]	Risk assessment and mitigation procedure(s): Elements describing: • Verification that safety objectives and safety requirements are met, • Results expected in regard to this point. • Links between the safety verification and the overall verification and validation process with regard to the change	Check that the procedures(s) define(s) a systematic process to take appropriate measures, prior to the implementation of the change, to provide assurance that: • Assumptions are satisfied, • Safety objectives are satisfied, • Safety requirements are satisfied as planned. Check that the procedures(s) define(s) means to collate the results.	The impact on contracts, training records, operational manuals, AIS, etc should be documented and updated as required to implement the change.

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
			Records documenting the verification of safety objectives and safety requirements and the results from this action. • Documenting the testing, verification and validation process.	Within the sample of changes selected in 5.2 above, check that for each change the: • actions conducted conformed with the relevant procedure(s), • evidence shows that the: o verification measures for pre-implementation have been implemented, o assumptions have been verified, o safety objectives have been satisfied, o safety requirements have been met, • results were properly collated.	
5.2 d ii)	during any transition phase into operational service,	*Common Requirements* *Annex 2, 3.2.1* [...] • During any transition phase into operational service, [...]	Risk assessment and mitigation procedure(s): Elements describing: • Verification that safety objectives and safety requirements are met, • Results expected in regard to this point. • Links between the safety verification and the overall verification and validation process with regard to the change	Check that the procedures(s) define(s) a systematic process to take appropriate measures, during any transition phase into operational service, to provide assurance that: • Assumptions are satisfied, • Safety objectives are satisfied, • Safety requirements are satisfied as planned, • Hazards specific to transition are identified, • Specific back up plans exist. Check that the procedures(s) define(s) means to collate the results.	

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
			Records documenting the verification of safety objectives and safety requirements and the results from this action. • Documenting the testing, verification and validation process.	Within the sample of changes selected in 5.2 above, check that for each change the: • Actions conducted conformed with the relevant procedure(s), • Evidence shows that the: o verification measures for any transition phase into operational service have been implemented, o assumptions are verified, o safety objectives are satisfied, o safety requirements are met. • Results have been properly collated. More specifically check that: • Arrangements have been made to ensure that safety performance is verified in the operational environment, • New safety problems raised during the transition have been addressed. • List of hazard to be updated	

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
5.2 d iii)	during its operational life, and	*Common Requirements* *Annex 2, 3.2.1* [...] During its operational life, and [...]	Risk assessment and mitigation procedure(s): Elements describing: • Verification that safety objectives and safety requirements are met, • Results expected in regard to this point. • Links between the safety verification and the overall verification and validation process with regard to the change	Check that the procedures(s) define(s) a systematic process to take appropriate measures during operational life, including safety monitoring, to provide assurance that: • Assumptions are satisfied, • Safety objectives are satisfied, • Safety requirements are satisfied as planned. Check that these measures form a "post implementation" monitoring of assumptions and safety performance and follow-up incidents in order to verify compliance to safety requirements Check that the procedures(s) define(s) means to collate the results.	
			Records documenting the verification of safety objectives and safety requirements and the results from this action. • Documenting the testing, verification and validation process.	Within the sample of changes selected in 5.2 above, check that for each change the: • actions conducted conformed with the relevant procedure(s), • evidence shows that the: o verification measures for operational life have been implemented including: o assumptions have been verified, o safety objectives have been satisfied, o safety requirements have been met. • results have been properly collated. More specifically check that the verification measures implemented included, as appropriate. • Continuous safety monitoring, • Continuous safety occurrences reporting and assessment.	

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
5.2 d iv)	during any transition phase till decommissioning.	*Common Requirements* *Annex 2, 3.2.1* [...] During any transition phase till decommissioning. [...]	Risk assessment and mitigation procedure(s): Elements describing: • Verification that safety objectives and safety requirements are met, • Results expected in regard to this point. • Links between the safety verification and the overall verification and validation process with regard to the change	Check that the procedures(s) define(s) a systematic process to take appropriate measures, during any transition till decommissioning, to provide assurance that: • Assumptions are satisfied, • Safety objectives are satisfied, • Safety requirements are satisfied as planned. Check that the procedures(s) define(s) means to collate the results	
			Records documenting the verification of safety objectives and safety requirements and the results from this action. • Documenting the testing, verification and validation process.	Within the sample of changes selected in 5.2 above, check that for each change the: • Actions conducted conformed with the relevant procedure(s) • Evidence shows that the: o verification measures for any transition phase till decommissioning have been implemented, o assumptions have been verified, o safety objectives have been satisfied, o safety requirements have been met. • The results have been properly collated. More specifically check that: • The safety impact on ATM operations due to withdrawing from operations has been assessed. • Within the ”post implementation” there was sufficient monitoring of assumptions and safety performance, and follow-up of incidents	

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
5.3	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:	*Common Requirements* *Annex 2, 3.2.3* 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: [...]	Risk assessment and mitigation procedure(s): Elements describing: • Risk assessment and mitigation documentation, • Process to collate and document the results, rationales and evidence of risk assessment and mitigation.	Check that the procedure(s) establish(es) the means to collate and document the results, associated rationales and evidence from the: • Determination of scope, boundaries and interfaces required in 5.2 a), • Identification of hazards required in 5.2 a) i), • Determination of severities required in 5.2 a) ii), • Determination of hazards tolerability required in 5.2 a) iii), • Derivation of a risk mitigation strategy as required in 5.2 c), • Verification that all identified safety objectives and safety requirements have been met as required in 5.2 d. Check that an appropriate set of risk assessment and mitigation documentation is defined in the procedure(s).	The notion of 'risk assessment and mitigation documentation' was introduced in ESARR 3 as regards the means to collect and document the results from risk assessment and mitigation. Isolated results are normally documented in records. The risk assessment and mitigation documentation refers to the whole set of documents related to the process and its results, from records to the document presenting the safety argument.

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
			Records documenting the collation and documentation of results, associated rationales and evidence.	In order to assess the evidences related to the effective implementation of the provisions contained in 5.3, consider a sample of changes. The sample should be selected by the NSA and include enough changes to cover: • Changes to supporting services within the managerial control of the ANSP. • Changes at different stages of their lifecycle. • Changes which concern airborne and ground components. • Changes which concern human, procedures and equipment. • Changes which concern different ATM operational units and different types of ATM services provided by the ANSP. Review the application of the relevant procedure(s) to check that they have been applied to each change in the sample.	To note that it is proposed to use the same sample in relation to all ESARR 4 provisions under Section 5.3. Depending upon the case, this sample could be same one used in relation to 5.1 and/or 5.3. (sampling unit = change to a part of the ATM system and the supporting services under the ANSP's managerial control).

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
5.3 a	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[34] including, as appropriate, specifications of any predictive, monitoring or survey techniques being used;	*Common Requirements* *Annex 2, 3.2.3* [...] complete arguments are established to demonstrate that the constituent part under consideration, as well as the overall ATM functional system are, and will remain tolerably safe by meeting allocated safety objectives and requirements. This shall include, as appropriate, specifications of any predictive, monitoring or survey techniques being used; [...]	Risk assessment and mitigation procedure(s): Elements describing: • Articulation of results, associated rationales and evidence from risk assessment and mitigation in a safety argument.	Check that the procedure(s) establish the means to articulate the results, associated rationales and evidences into a safety argument (sometimes known as 'safety case') for each change considered.	'Safety argument' means the demonstration and evidence that a proposed change can be implemented within the applicable tolerable levels of safety.
			Safety arguments resulting from the risk assessment and mitigation process.	Within the sample of changes selected in 5.3 above, check that for each change the: • Safety argument exists, • Development of the safety argument conformed with the relevant procedures, • Safety argument presents a demonstration that the constituent part under consideration, as well as the overall ATM system, are and will continue to be safe, • Safety argument includes, as appropriate, specifications of any predictive, monitoring or survey techniques used. Within the same sample, review the safety arguments in order to check their completeness and correctness.	The review of safety arguments should normally be conducted by means of the process established to implement ESARR 1 Section 7. Several actions proposed in this table with regard to the results of various processes can be part of that review. EAM 1 / GUI 4 is being developed to provide NSAs with comprehensive guidance on the review of safety arguments.

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

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
5.3 b	That all safety requirements related to the implementation of a change are traceable to the intended operations / functions.	*Common Requirements* *Annex 2, 3.2.3* [...] all safety requirements related to the implementation of a change are traceable to the intended operations / functions.	Risk assessment and mitigation procedure(s): Elements describing: • Means to ensure traceability of safety requirements to intended operations/functions.	Check that the procedure(s) establish the means to keep traceability of all safety requirements to the intended operations/functions. Notably when: • The safety requirements are defined as a result of 5.2 c) ii), • Assurance is provided to show that safety requirements in the context of 5.2 d).	
			Records documenting the traceability of safety requirements to intended operations/functions.	Within the sample of changes selected in 5.3 above, check that for each change: • Each safety requirements is traceable to the intended operations/functions.	
Appendix A A-1 Paragraph 1	Before the risks associated with introduction of a change to the ATM System in a given environment of operations can be assessed, a systematic identification of the hazards shall be conducted.	*Common Requirements* *Annex 2, 3.2.4* [...] A systematic identification of the hazards shall be conducted. [...]	Evidences related to 5.2 b) i).	Preferably check these provisions when considering the evidences showing compliance with 5.2 b i). Check specifically the identification of hazards is conducted before risks are assessed.	5.2 b) i) required identification of hazards.

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
Appendix A A-1 Paragraph 2 & Figure A-1	The severity of the effects of hazards in that environment of operations shall be determined using the classification scheme shown in Figure A-1.	*Common Requirements* *Annex 2, 3.2.4* [...] The severity of the effects of hazards in a given environment of operations shall be determined using the classification scheme shown in the following table, [...]	Severity classification scheme used Other evidences related to 5.2 b) ii).	Preferably check these provisions when considering the evidences showing compliance with 5.2 b ii). Check that the severity classification scheme conforms with the one included in ESARR 4 Appendix 1.	5.2 b) ii) requires severity classification. To note that: • The table of Figure A-1 makes clear that although the severity classification of effects proposed is common to that in ESARR 2, the examples chosen relate to *a priori* assessment. • On the other hand, the table included in the CRs uses definitions which may be reflected in the ESARR 4 examples except for the fact that it is not made clear that the definitions relate to *a priori* assessment.
Appendix A A-1 Paragraph 3	As there is no such scheme today as an accident/incident causation model, the severity classification shall rely on a specific argument demonstrating the most probable effect of hazards, under the worst case scenario.	*Common Requirements* *Annex 2, 3.2.4* [...] while the severity classification shall rely on a specific argument demonstrating the most probable effect of hazards, under the worst-case scenario. [...]	Severity classification scheme used. Other evidences related to 5.2 b) ii), specifically those related to the assignment of severity classes.	Preferably check these provisions when considering the evidences showing compliance with 5.2 b ii). Check that severity classification relies on a specific argument demonstrating that most probable effect of hazards, under the worst case scenario.	5.2 b) ii) requires severity classification. To note that on the table of Figure A-1, the worst credible effect in the environment of operations determines the severity class.

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
Appendix A A-1 Paragraph 4	In order to deduce the effect of a hazard on operations and to determine its severity, the systematic approach/process shall include (but not be restricted to) the effects of hazards on the various elements of the ATM System, such as: • Effect of hazards on air crew (e.g. workload, ability to perform his/her functions), • Effect of hazard on the ATCOs (e.g. workload, ability to perform his/her functions), • Effect of hazard on the aircraft functional capabilities, • Effect of the hazard on the functional capabilities of the ground part of the ATM system, Effect on the ability to provide safe ATM services (e.g. magnitude of loss or corruption of ATM services / functions).	*Common Requirements* *Annex 2, 3.2.4* In order to deduce the effect of a hazard on operations and to determine its severity, the systematic approach/process shall include the effects of hazards on the various elements of the ATM functional system, such as the air crew, the air traffic controllers, the aircraft functional capabilities, the functional capabilities of the ground part of the ATM functional system, and the ability to provide safe air traffic services.	Severity classification scheme used. Other evidences related to 5.2 b) ii), specifically those related to the assignment of severity classes.	Preferably check these provisions when considering the evidences showing compliance with 5.2 b ii). Check that when deducing the effect of a hazard on operations and to determine its severity, consideration is given to, but not restricted to, the effects of hazards on: • Aircrew, • ATCOs, • aircraft functional capabilities, • the functional capabilities of the ground part of the ATM system, • the ability to provide safe ATM services.	5.2 b) ii) requires severity classification.

ESARR 4 Reference	ESARR 4 provision	EC provisions intended to transpose the ESARR provision	Evidence(s)	How could the evidence be assessed	Comments/Notes
Appendix A A-2 Paragraph 1 & Figure A-2	Safety objectives based on risk shall be established *(1)* in terms of the hazards maximum probability of occurrence, derived both from the severity of its effect, according to Figure A-1 and from the maximum probability occurrence of the hazard's effect, according to Figure A-2.	*Common Requirements* *Annex 2, 3.2.4* Safety objectives based on risk shall be established in terms of the hazards maximum probability of occurrence, derived both from the severity of its effect, and from the maximum probability of the hazard's effect.	Risk classification scheme used. Other evidences related to 5.2 b) iii).	Preferably check these provisions when considering the evidences showing compliance with 5.2 b iii). Check that: • Safety objectives based on risk are established, • They are established in terms of the hazards maximum rate of occurrence, • The hazards maximum rate of occurrence is derived both from: • The severity of its effect according to Figure A-1, and • The maximum rate of occurrence of the hazards effect according to Figure A-2.	5.2 b) iii) requires determination of safety objectives in terms of hazards maximum rate of occurrence. To note that no equivalent to the ESARR 4 Figure A-2 exists in the CRs.
Appendix A A-2 Paragraph 2	As a necessary complement to the demonstration that these quantitative objectives are met, additional safety management considerations shall be applied so that more safety is added to the ATM system whenever reasonable.	*Common Requirements* *Annex 2, 3.2.4* As a necessary complement to the demonstration that established quantitative objectives are met, additional safety management considerations shall be applied so that more safety is added to the ATM system whenever reasonable.	Evidences related to 5.2 d).	Preferably check these provisions when considering the evidences showing compliance with 5.2 d). Check specifically that, whenever reasonable, additional safety management considerations are applied to add more safety beyond the levels achieved through the implementation of 5.2.	5.2 d) requires verification that safety objectives and safety requirements are met. This refers to further safety measures added to those resulting from applying the risk assessment and mitigation process.

(***)