EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

ESARR ADVISORY MATERIAL/GUIDANCE MATERIAL
(EAM/GUI)

EAM 6/GUI 1

ESARR 6 GUIDANCE TO ATM SAFETY REGULATORS

Explanatory Material on ESARR 6 Requirements

Edition	**:**	**0.06**
Edition Date	**:**	**30 January 2007**
Status	**:**	**Working Draft**
Intended for	**:**	**Restricted SRU**
Category	**:**	**Guidance Document**

SAFETY REGULATION COMMISSION

F.2 DOCUMENT CHARACTERISTICS

TITLE		
EAM 6/GUI 1 **ESSAR 6 Guidance to ATM Safety Regulators – Explanatory Material on ESARR 6 Requirements**		
Document Identifier :	**Reference :**	EAM 6/GUI 1
filename	**Edition Number :**	0.06
	Edition Date :	30-1-2007

Abstract :

This guidance material has been prepared by the Safety Regulation Commission to provide guidance for ATM safety regulators and support the implementation of ESARR 6 – Software in ATM Systems.

The main purpose of this document is to provide guidance about the provisions established in ESARR 6, Obligatory Provisions. Each requirement is illustrated by giving explanatory material that includes a rationale, the most significant implications for both Regulator and Provider, and information about further development.

This is the first deliverable of a series of guidance documents to be developed by SRC relevant for ESARR 6.

Keywords :

ESARR 6	ATM Software	Software requirements
Safety Assurance	Configuration Management	Verification

Contact Person(s) :	**Tel :**	**Unit :**
Antonio Licu	+32 2 729 34 80	DGOF/SRU

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

SOFTCOPIES OF SRC DELIVERABLES CAN BE DOWNLOADED FROM :

www.eurocontrol.int/src

F.3 DOCUMENT APPROVAL

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

AUTHORITY	NAME AND SIGNATURE	DATE
Quality Control (SRU)	(Daniel HARTIN)	
Head Safety Regulation Unit (SRU)	(Peter STASTNY)	
Chairman Safety Regulation Commission (SRC)	(Philip S. GRIFFITH)	

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	04-Jun-02	Creation – First working draft 0.01 from SRU. Using available material following ASW 4 meeting (May 2002).	All
0.02	05-Jul-02	Revisions after ASW 5 meeting to capture the changes in ESARR 6 (ref. ESARR 6 ed. 0.10).	All
0.03	02-Sep-02	Revisions following Norway comments on edition 0.02.	5.1 & 6
0.04	25-Oct-02	Revisions following ASW 6 meeting and consultation thereafter. Main changes due to new edition ESARR 6 WD 0.12 and ESARR 6 Draft Issue 0.1. Document format also updated.	All
0.05	21-Dec-06	Revisions to all sections as part of a project to extend the level of guidance provided for ESARR 6.	All
0.06	30-Jan-07	Revisions following meeting of ESARR 6 Guidance project team. Focussing on regulatory concerns and integrating material in other sources.	All

F.5 CONTENTS

F.6 EXECUTIVE SUMMARY

This guidance material has been prepared by the Safety Regulation Commission to provide guidance for ATM Safety Regulators and support the implementation of ESARR 6.

Within the overall management of their ATM services, ATM service-providers shall operate safety management systems (SMS) in accordance with ESARR 3. Additional safety assurances are required in order to deal with the deployment of software systems. These assurances ensure that the risks associated with operating ATM software have been reduced to a tolerable level.

ESARR 6 requires the Designated Authority to ensure adequate and appropriate safety regulatory oversight. This guidance material explains the specific steps that ATM safety regulators may take when dealing with the approval of service provider operations supported by software functions.

The main purpose of this document is to provide guidance on the obligatory provisions in ESARR 6. Each requirement is illustrated by giving explanatory material that includes a rationale, the most significant implications for both Regulator and Provider, and information about further development.

[This space is intentionally left blank]

1. INTRODUCTION

1.1 Scope of the Document

The main purpose of this document is to illustrate the *Obligatory Provisions* laid down in ESARR 6 and facilitate their interpretation. Non obligatory provisions have been also included to better explain the rationale and the Safety Objective of this safety regulatory requirement

1.2 Interpreting the Document

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

The document includes a Section 6 to provide guidance considered necessary to achieve the stated safety objectives. This section includes all applicable mandatory requirements (expressed using the word “shall”), including those relating to implementation.

To ease the reading of the document the following editorial decoding needs to be used:

- whenever a text is highlighted in boxes as in the below example it represents a copy of text as was agreed in ESARR 6

Example:

i) ESARR 6 concerns the use of software in safety related ground-based ATM (Air Traffic Management) systems.

- The rest of text and pictures are used to interpret the requirements of ESARR 6 and to give additional guidance material to the ATM Safety Regulators in respect of usage and applicability of Safety Regulatory Requirements “Software in ATM systems”.

1.3 Context and High-Level Rationale

The implementation of ESARR 6 safety oversight at national level requires, in one form or another, the establishment of a specific function at national level. This ESARR 6 safety oversight function will typically be undertaken within a larger State-based organization, of a safety regulatory nature. For convenience, this organization will be referred to as the ‘designated authority’ throughout this document.

The establishment of that designated authority, its roles, functions, safety regulations, resources and related ESARR 6 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 6 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 the development of safety related software systems and risk assessment both within the service provider(s) and within the designated authority itself, and

Visibility of past experience the designated authority has acquired over the years with the regulated service providers in software development and risk assessment.

1.3.1 International Obligations

It is recognized that the harmonization 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 6 requirements through appropriate safety regulation and safety oversight.

1.3.2 Designated Authority

The 'designated authority' ought to exist and carry out, among other things, ESARR 6 safety oversight. This body must have recourse to the necessary legal and/or constitutional powers to ensure compliance with ESARR 6 national regulations.

In the context of ESARR 6 and in addition to the generic ideas provided in SRC Policy Document 3, the national aviation legislation should also;

Authorize 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, including any related changes to safety related software systems.

1.3.3 Regulatory and Service Provision Context

1.3.3.1 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. These choices will influence the precise mechanisms that are used to regulate the development of ATM safety related software. ESARR 6 provides minimum requirements that must be satisfied by these regulatory mechanisms. ESARR 6, therefore, only represents a minimum set of safety regulatory requirements specified at a European level.

In establishing a designated authority, the State also has the option of adopting solutions which will govern its role and daily safety oversight activities. These options also influence the implementation of ESARR 6. They 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 less frequently for all SMS related processes, including those that relate to the development of safety related software applications.

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 6 safety oversight system with due consideration of the industry maturity in safety, and to both the aviation community and the public interest.

1.3.3.2 Institutional Arrangements for ATM Service Provision

The responsibility of ensuring safety within the national airspace rests with the State. The requirement for a well documented and systematic approach to safety of 'Software in ATM Systems' equally applies to government and to commercialized organizations providing ATM services. Whenever the service provision of ATM is delegated to a commercialized organization, it is of prime importance that the State retains its overseeing responsibilities and ensures that the service provider complies with ESARR 6. Even if the service provision remains government-based, the best transparent and robust way of ensuring compliance with ESARR 6 would be to establish a separate function within the administration which would verify initial and on-going compliance with ESARR 6 during the software and systems lifecycle.

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 ESARRs 3, 4 and 6.

1.3.3.3 Capacity of ATM Service Provider

The level of ESARR 6 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. This has important consequences for the risk based approach to software safety that is advocated in ESARR 6. Designated authorities therefore often require additional guidance on the implementation of ESARR 6;

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. This has strong implications for the implementation of ESARR 6, which advocates a risk based approach to software development.

Previous experience in implementing ESARR 6, both in service provider (s) and in the designated authorities, is almost nil.

There is a need for a close interface between the designated authority and the regulated organization(s) in order to build confidence across the two communities. This collaboration should also support a joint learning process in the implementation of ESARR 6. During the initial implementation of this regulatory requirement, designated authorities should avoid adopting a passive approach to safety oversight. Resources and expertise must be devoted to verify compliance with ESARR 6 requirements.

When the regulated organizations and designated authorities have acquired enough experience in implementing ESARR 6, the designated authority will be in a position to adopt a less involved approach to safety oversight. Delegation of some safety regulatory approval competence to an approved representative of the service provider could also be contemplated at a later stage.

1.4 Regulatory Capacity

1.4.1 Organization

The implementation of ESARR 6 safety oversight at national level requires, in one form or another, the establishment of an appropriate organization, with adequate processes, working procedures and resources. The safety oversight activities related to ESARR 6 are, however, only part of a bigger set of safety regulatory functions. These functions are determined by the specific national legislative framework and so there is no single model for detailed organizational arrangements that can be recommended in this document.

1.4.2 Processes and Procedures

Section 1.3.3.2 recommends the creation of "…a well documented safety oversight system to ensure full compliance with ESARRs 3, 4 and 6". Safety oversight systems implement the interface between the designated authority and ATM service provider(s) as they work on ESARR 6 safety oversight. In addition, it would be advisable to develop an internal manual within the designated authority, containing;

Instructions for ESARR 6 safety oversight activities. These instructions can help to ensure the consistent performance of safety oversight functions by different members of staff; and

Standard forms and reports to be used to document the outcome of any ESARR 6 software safety oversight activities.

These processes and procedures help to determine the budget and staff that are required by ESARR 6 related software safety oversight functions.

1.4.3 Budget

The implementation of an ESARR 6 software safety oversight function will require the allocation of a budget. SRC Policy Document 3 and ESARR 1 provide generic recommendations for this funding requirement. However, the size of the budget will depend upon the volume of work to be handled, and more specifically;

The number of ATM service providers under ESARR 6 software safety oversight,

The frequency and scope of changes being submitted to safety regulatory approval,

The safety oversight processes and procedures in place for ESARR 6, and

The expected average travel length and time required for audits and inspections.

1.4.4 Staff

1.4.4.1 General

SRC Policy Document 3 and ESARR 1 provide further generic guidance on human resource requirements for safety oversight functions. The structuring and level of staffing involved in ESARR 6 safety oversight will also depend on the volume of work to be handled, and more specifically;

The number of ATM service providers under ESARR 6 safety oversight,

The frequency and scope of changes being submitted to safety regulatory approval, and

The safety oversight processes and procedures in place for ESARR 6.

1.4.4.2 Recruitment

As before, ESARR 1 and SRC Policy Document 3 provide high-level guidance for recruitment. ESARR 6 safety oversight staff should include technical specialists in software development as well as safety specialists and operational experts. These multi-skilled teams can help the exchange of information and expertise over time. The leaders of any safety assessment, audit or inspection must possess qualifications that are appropriate to these tasks. In particular, they must have relevant operational and technical expertise and an understanding of the relevance of their oversight to the national ATM system.

1.4.4.3 Training

SRC Policy Document 3 and ESARR 1 provide generic principles for the training of safety oversight staff. In addition, there should be specialist training for ESARR 6 Safety Oversight staff. Some areas that should be considered for more detailed training are;

ESARR 6 based national regulations and the rationale for those regulations;

Applicable aircraft safety regulations, more specifically applying to CNS/ATM functions,

Risk assessment and mitigation processes and techniques,

Recognized means of compliance with ESARR 6,

Limits of professional competence and when to seek additional expertise.

New areas of change to the ATM system, especially focusing on innovations involving software systems, and

Safety occurrence reporting and analysis in ATM with particular emphasis on software related incidents and accidents.

1.4.4.4 Harmonized Judgment

It is essential that ESARR 6 safety oversight activities be conducted to a common standard. The development of a manual containing instructions to safety oversight staff will promote standardization. Common forms and procedures should also be used to document the outcome of any ESARR 6 safety oversight activities and any associated follow-up activities. Standard tools and techniques are particularly important during the start-up phase for ESARR 6 safety oversight activities. It can be extremely difficult to harmonize the judgment of regulators during the initial assessments when there will be limited experience in performing many tasks associated with the oversight of software safety. When faced with similar issues, ESARR 6 safety oversight staff should reach broadly similar judgments to those of their co-workers.

It is essential to share tools and techniques across the ESARR 6 safety oversight team in order to avoid inconsistent judgments. It is also important to ensure that assessors meet to consider the feedback from the inspections and audits that have been conducted by other oversight teams. Information exchange between software safety oversight teams can be promoted by;

A database of previous software failure modes with analysis of system level consequences in terms of severity of effect and accepted tolerable risk level (with associated assumptions and rationale),

Sessions with all the staff to discuss specific issues, such as those related to proposed means of compliance as well as to the risk assessment of new software technology,

Depending on the size of the ESARR 6 safety oversight team, key individuals can be asked to collate views and responses on specific issues. These might then be documented and used by all involved in safety regulatory audits and inspections. This individual could provide feedback to the staff involved in the development and maintenance of national ESARR 6 compliant safety regulations, and

Software safety reports (from safety regulatory audits and inspections, etc.). These could be circulated within the safety oversight team to allow for cross fertilization and for standardizing the regulatory responses

1.5 Safety Objectives

The designated authority should establish objective safety goals that do not remove the ATM service provider's freedom in selecting appropriate means of compliance with the ESARR6 objectives. The principle aim behind ESARR 6 is to ensure that the risks associated with any software used in safety-related Air Traffic Management systems have been reduced to a tolerable level. This implies that the ATM service-provider must anticipate the execution of safety-related software and ensure that it only behaves in the manner intended.

The tolerability of risks associated with safety related software is identified as part of a systems level safety assessment. Software development activities ensure that programs meet system requirements and ensure that there are no other adverse side-effects from the execution of safety-related software. From this it follows that ATM service-providers must:

(1) Establish that requirements are necessary and sufficient to achieve a tolerable level of risk.

(2) Ensure that requirements are implemented completely and correctly

(3) Ensure that the implementation contains no functions which have an adverse impact on the safety of the system.

ATM service-providers must also document the arguments and evidence that help to demonstrate they have satisfied these three higher level goals. This creates an additional set of process requirements for ATM service-providers to demonstrate to the designated authority. The documentary evidence mentioned above must:

a) Be shown to stem from the processes and products to which it relates;

b) Not have been altered in any way without a clear justification being provided for those changes;

c) Be available for inspection;

d) Be clearly associated with a particular configuration, including a known executable version of the software and any associated data or descriptions.

In addition, it is important for ATM service-providers to demonstrate to the designated authority that they have well established procedures for the maintenance of safety arguments and evidence over the lifecycle of safety critical software. Functions are often introduced after initial development and these need to be assessed to determine whether or not any changes will have introduce new safety requirements or will undermine existing requirements.

To summarize, from a regulatory perspective the ATM service-providers must:

- Provide documentary evidence and arguments to show that software requirements identify the necessary and sufficient conditions for tolerable safety of ATM systems within particular operational contexts.

- Provide documentary evidence and arguments to demonstrate that software satisfies its requirements.

- Provide documentary evidence and arguments to show that software-related requirements can be traced to the point at which they are satisfied within a design.

- Provide documentary evidence and arguments that provide assurance that other software functions do not interfere with any of the functionality that is intended to satisfy system safety requirements.

- Provide documentary evidence and arguments which establishes system safety for a particular operational context referring to a specific executable version of the software as well as the particular data and documentation that is associated with this version of the software.

[This space is intentionally left blank]

2. SECTION A – SCOPE

(*Introductory Material – The provisions of this section in ESARR 6 are not obligatory)*

i) ESARR 6 concerns the use of software in safety related ground-based ATM (Air Traffic Management) systems used for the provisions of ATM services to civil air traffic, including the periods of cutover (hot swapping).

ii) The scope of ESARR 6 is confined to the ground component of ATM and as such, its applicability cannot be claimed, unless modified and adequately assessed, for the airborne or spatial component of ATM systems. Nevertheless, ESARR 6 applies to the supporting services, including Communications, Navigation and Surveillance (CNS) systems, under the managerial control of the ATM service-provider.

The scope of ESARR 6 is restricted to the ground component of Air Traffic Management. It does not apply to the airborne or spatial component of ATM services unless its provisions are appropriately modified. However, ESARR 6 does apply to the systems that supporting Communications, Navigation and Surveillance (CNS) services in a manner similar to the provisions of ESARR 3.

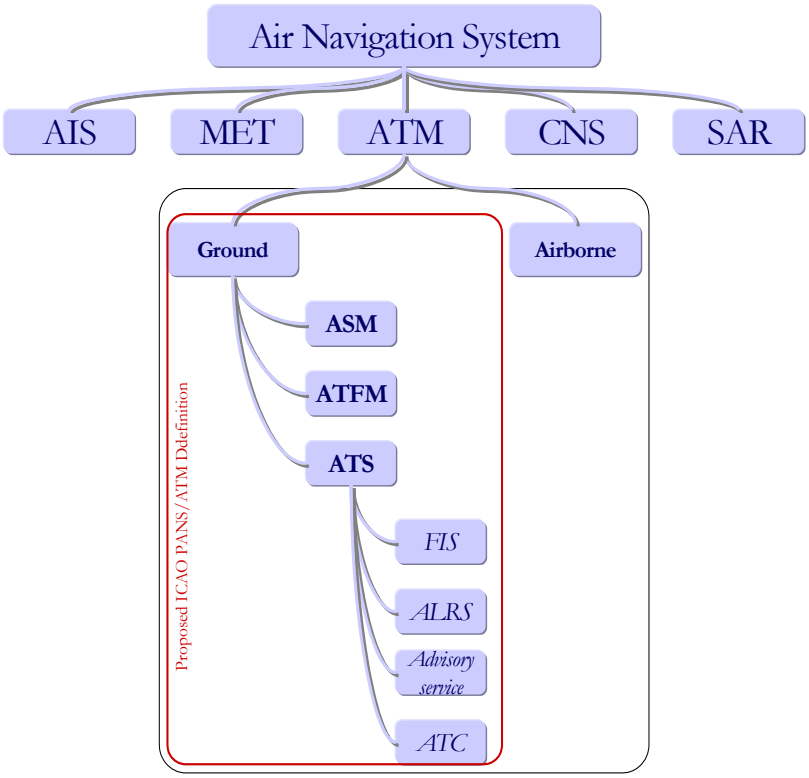


Figure 1: Overview of Air Navigation Service Components

ICAO has introduced the 'CNS/ATM' framework to describe the different components that can contribute to improvements in the global aviation system. The aims are to increase flight safety, improve the capacity and flexibility of air traffic and, as a consequence, reduce the delays and operating costs for aviation operations. As a result, the CNS/ATM concept encompasses many sectors and domains. CNS/ATM applications must, therefore, typically integrate multiple components, including

satellites, aircraft systems, telecommunication networks and air traffic control systems. ESARR 6 is not intended to embrace every aspect of software development across all areas of the ICAO CNS/ATM architecture. It contributions to this wider initiative by focussing on software in safety related ground-based ATM systems supported by ground Communications, Navigation and Surveillance (CNS) functions.

Many of the provisions within ESARR 6 can be usefully applied to the wider class of systems captured in the ICAO ATM/CNS architecture. However, the focus on ground based systems is justified by the lack of previous guidance in this area. In contrast, there is a host of existing regulatory provision covering other components of the ATM/CNS concept. For example, ED-12B/DO-178B provides part of the regulatory background for airborne systems. Documents such as the EUROCAE ED-109 Guidelines on Software Integrity Assurance can also be used to support the development of space based applications. Both of these documents have been informed the development of guidance material for ESARR 6. This helps to ensure that designated authorities can easily integrate the assessment of ground based software systems with software assessments for these wider aspects of the air traffic management infrastructure.

iii) ESARR 6 assumes that an a priori risk assessment and mitigation process is conducted to an appropriate level to ensure that due consideration is given to all aspects of ATM including ATM functions to be performed by software. Additionally ESARR 6 assumes that the effectiveness of risk assessment and mitigation associated with software malfunctions or failures is already in place.

Designated authorities must ensure that the wider risk assessment and mitigation processes described in ESARR 3 are implemented because these are prerequisites for many of the processes documented in ESARR6. In particular, ESARR 3 section 5.2.4 Risk Assessment and Mitigation requires that;

> *Within the operation of the SMS, the ATM service-provider;*
>
> *a) shall ensure that risk assessment and mitigation is conducted to an appropriate level to ensure that due consideration is given to all aspects of ATM;*
>
> *b) shall ensure that changes to the ATM system are assessed for their safety significance, and ATM system functions are classified according to their safety severity;*
>
> c) *shall ensure appropriate mitigation of risks where assessment has shown this to be necessary due to the safety significance of the change;*
>
> *(ESARR3, Page 11)*

ESARR 4 – Risk Assessment and Mitigation in ATM provides further requirements in section 5.1, 5.2 and 5.3. These are not reproduced here for the sake of brevity. ESARR 4 constructs further links with ESARR 6 in a section on Links with ATM software qualification;

> *8.2.2.1 - The safety objectives allocated to each hazard drive the determination of specific means to attain the proper level of confidence in the success of implementing the mitigation strategies and related safety requirements.*

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

(ESARR 4, Page 11)

ESARR 6 focuses on the regulatory links between system-level risk assessments and the development of safety-critical software. Designated authorities must ensure that ATM service providers conduct Functional Hazard Assessments and Preliminary System Safety Assessments. Software frequently plays a role in the mitigation or reduction of the risks identified in these assessments. It follows that the criticality or important of the function provided by the software is measured in terms of the risk reduction that is intended to be provided by that software. If a piece of code reduces an unacceptable risk to one that is now acceptable then it can be argued that the safe operation of the system now relies on that software and, in consequence, additional development resources should be allocated to ensure that the code will function in a reliable and timely manner. Designated authorities must, therefore, work with ATM service-providers to ensure that sufficient resources have been allocated to such critical functions. To summarize;

- It is assumed that the risk assessment and mitigation process derives system-level safety requirements from a hazard and risk analysis of the ATS environment in which the system is required to operate.

- It is assumed that a necessary and sufficient set of system-level safety requirements exist, which describe the functionality and performance required of the system in order to support a tolerably safe ATS.

- It is assumed that the failure modes which the software must detect and mitigate in order to meet the system safety requirements have been identified e.g. those failure modes associated with: other systems, system-system interactions, equipments, pre-existing software and all user-system interactions.

- It is assumed that the failure modes identified include generic failures relevant to the safety related ATS application, e.g. security threats, loss of communications, and loss of power.

- It is assumed that the failure modes identified (including human errors) are representative of the operational environment for the system and workload on the system operators.

Designated authorities must ensure that ATM service providers have considered the interaction between Air Navigation Systems and their environment during any risk assessment. Changes in the systems being used can alter the risk profile of operational practices. Changes in the operating environment can also affect the risks associated with air traffic service provision. In order for designated authorities to assess the degree to which software may reduce the risks associated with service provision it is necessary to consider the current state as well as potential changes both to Air Traffic systems and to their operating environment.

There must be both a necessary and a sufficient set of system level safety requirements before any risk assessment can be completed. Informally, a necessary requirement is one that if it were violated then the system as a whole would have failed. If we forget to include a necessary functional requirement then some key aspect of the infrastructure will have been omitted. For example, a necessary

requirement of air traffic service provision is to ensure adequate separation. Sufficient requirements collectively describe conditions that if they all hold then the system is successful. If we do not have a sufficient set of requirements then some aspect of the system will also be perceived to have failed. For instance, although separation is a necessary requirement it is not sufficient on its own. In particular, it is important to ensure that aircraft arrive at their intended destination in a timely manner. Hence a sufficient set of requirements must also take these constraints into account.

The importance of the previous paragraph is that if any of these requirements are omitted then it can be difficult to accurately conduct the system level risk assessments that are a prerequisite for the assessment of software criticality. For example, if an initial risk analysis did not consider the need to support on-time departures in poor visibility then many aspects of the subsequent development might be compromised because the hazards that relate to these operations would not have been considered. Hence, it would not have been possible to identify the importance of software components that might be necessary to reduce the risks associated with poor visibility operations. From this it follows that designated authorities must be able to trace the arguments that ATM service providers construct in order to demonstrate the sufficiency and completeness of their system level safety requirements.

Once the functional requirements can be identified for Air Traffic Systems, ATM service providers must demonstrate to designated authorities that they have considered the different ways in which ATM systems may fail. For example, a failure is total if it prevents the system from providing a particular function from the moment at which it occurs. A partial failure may degrade the provision of a function but will not totally eliminate it. An intermittent failure removes some or al provision of a system function but only during particular intervals of time at other times full functionality is resumed. Within each of these high-level categories there are more complex modes that must be considered during a risk assessment. Unless ATM Service Providers consider a broad range of failure modes then it is unlikely that they will be able to convince designated authorities that they have adequately addressed the many different hazards to be mitigated by safety-critical software.

Human factors and operator behaviour significantly increases the complexity of any risk assessment. ATM service providers must show designated authorities that they have considered the many different ways in which ATCOs, managers and technical staff could inadvertently undermine key system functionality. However, if human intervention is not considered within a preliminary risk assessment then it is unlikely to adequately reflect the true operational environment of Air Navigation Systems. In consequence, it would be difficult both to anticipate the need for software risk mitigation and to adequately assess the criticality of any existing software provision.

iv) ESARR 6 does not prescribe any type of supporting means of compliance for software. This is the role of software assurance standards. It is outside the scope of this requirement to invoke specific national or international software assurance standards.

ESARR 6 is an “objective–based” regulation. It leaves the selection of compliant software assurance standards as a matter of commercial freedom to be agreed between the ATM service-provider and system manufacturer.

Traditionally, in many industries including ATM, safety regulation was done prescriptively, i.e. the regulator defined the rules and standards to be followed, used

audit and inspection to check compliance with them, and quite commonly would issue a safety certificate to that effect. In so doing, the designated authority implicitly (if not explicitly) inherited a substantial part of the responsibly from the ATM service provider. That required a great deal of specialist resource on the part of the regulator and was often over-constraining for the ATM service provider, particularly in the introduction of new processes and technologies.

Many involved in European Air Traffic Management have recognised these difficulties. This recognition has led to a recent trend towards objective-based safety regulation in which safety is much more clearly the responsibility of the ATM service provider. The role of the regulator, or designated authority, is to ensure that the service provider discharges his responsibilities properly. The designated authority sets objectives for the achievement and demonstration of safety and the service provider has to show (by argument and evidence) that he has met those objectives. The use of standards is appropriate but the service provider has to show that the standards he chooses to use are appropriate – not merely claim compliance with them.

There are many benefits associated with the use of objective based regulations by designated authorities. For instance, software development techniques are likely to change rapidly over time as new hardware and software platforms emerge. Any regulatory instrument that embodies or advocates particular development techniques is, therefore, likely to have an extremely short shelf-life. There are also strong national and international differences over the suitability of particular development methodologies within the context of their national systems in terms of cultural, commercial and technical concerns. The validity of any regulatory instrument be undermined by the inclusion of such recommendations. Such a prescriptive approach would also impose inappropriate constraints on the ATM service providers who must apply their provisions and on the designated authorities who would have to establish compliance. All of these reasons help to justify the objective based approach embodied in ESARR 6.

[This space is intentionally left blank]

3. SECTION B – RATIONALE

Why Do We Need Safety Regulatory Requirements for ESARR 6? The introduction of Safety Management Systems (SMS) by ATM service-providers has been identified as an essential measure to preserve and improve safety. These guidelines provide a high-levelk framework for the management of safety within complex organisations. Accordingly, there is also a need for regulations stating further detailed requirements for the ways in which service providers deal with ATM software provision.

The drafting of regulations for the development of Safety Management Systems does not reduce the importance of existing safety standards and regulatory requirements. Compliance with these wider safety standards and requirements is recognised as essential to ensure minimum criteria across the industry in a range of technical areas. Safety standards and requirements also create a framework on which ATM service providers can build robust safety arguments. These arguments, in turn, help to demonstrate to designated authorities that service providers have achieved the safety objectives that motivate the introduction of SMS. Hence there are very close links between the development of Safety Management Systems, covered in ESARRs 3 and 4, and the introduction of more detailed technical software safety regulations in ESARR 6.

Errors in the design, operation or maintenance of the ATM System, or failures in the ATM System functions supported by software, could result in, or contribute to, a hazard to aircraft. The increasing integration, automation and complexity of the ATM System in the ECAC region necessitates the use of formal processes to demonstrate that all changes to the ATM System, including its software-based elements, can be introduced while preserving tolerable levels of safety.

It is the SRC's view that further continuation of this safety regulatory development process is necessary in applying the principles of Risk Assessment and Mitigation to the specialised safety-related area of software-based ATM systems.

(Introductory Material – The provisions of this section in ESARR 6 are not obligatory)

i) The SRC decision number 6/8/5 approved the inclusion of the development of a EUROCONTROL Safety Regulatory Requirement for software-based ATM systems in the SRC work programme. It is recognised that there is no precedent in this area neither by ICAO nor by any other international regulatory body responsible for ATM system safety.

The concern to develop regulatory material specifically to support software development in ATM systems reflects the growing importance of programmable systems within aviation safety. At the time when ESARR 6 was first drafted, there was little specific guidance on appropriate techniques for software development within this domain. More general standards, such as IEC61508, provided some support to designated authorities and to ATM service providers. However, they lacked the specific focus on ATM systems requirements. The development of ESARR 6 can also be justified in terms of the need to integrate the requirements for software development within the suite of other regulatory instruments in European Air Traffic Management.

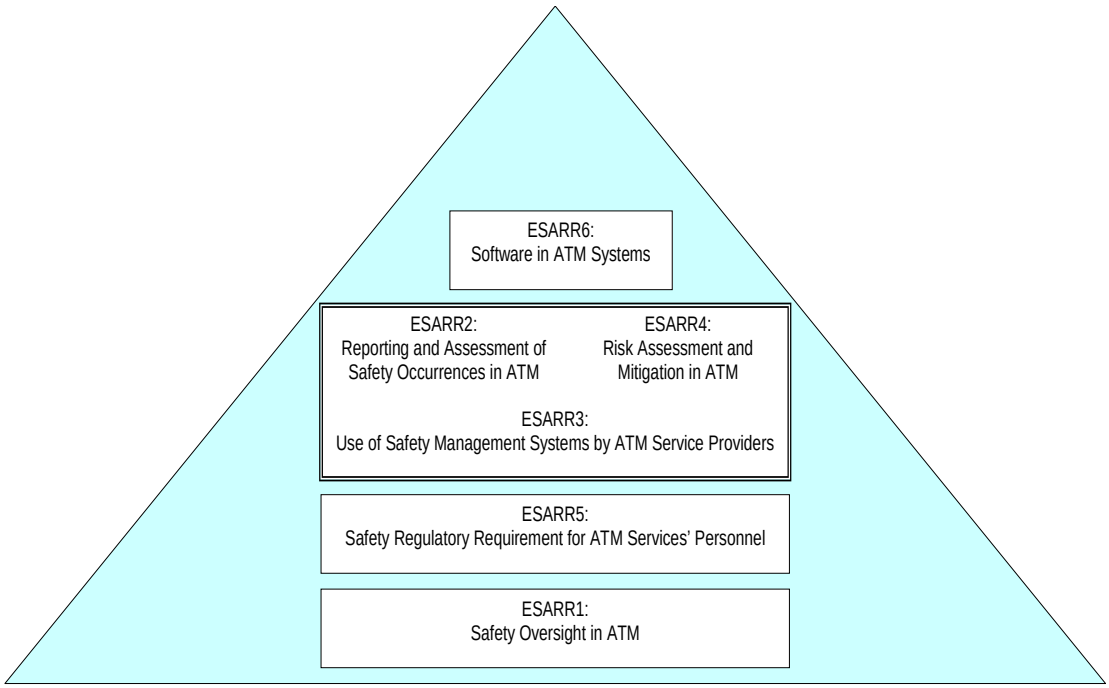


Figure 2: Regulatory Pyramid Showing Relationships Between ESARRs

Figure 2 provides an overview of the relationship between ESARR 6 and the other safety regulatory requirements. Previous sections have described how ESARR 1 helps to establish requirements on member states to establish a framework for safety oversight in Air Traffic Management. ESARR 5 builds on this and describes requirements for designated authorities to monitor the adequacy of staffing and training within national service providers. ESARR 3 provides requirements for the procedural mechanisms and processes that these staff must follow. In particular, ESARR 2 sets out minimum requirements for the reporting and assessment of adverse events. Not only does this establish an important component of any safety management system but it also provides valuable input and validation for the risk assessment and mitigation activities that are described in ESARR 4. Figure 2 shows how ESARR 6 builds upon these other regulatory requirements. The roles described within ESARR 1 help to establish obligations on the designated authority and on the ATM service provider(s). ESARR 5 sets out the key requirements that service providers must satisfy for the specialist staff needed to implement software safety processes. ESARR 3 maps out a high-level approach to the management of both the staff and the processes that they perform, including the risk assessment and incident analysis activities in ESARRs 2 and 4.

It is important to consider the justification for developing a separate ESARR dealing with software. Programmable systems introduce considerable opportunities for innovation. They support the integration of many diverse applications and hence can be used in safety related systems to guard against many different hazards. This increases the importance of software for overall system safety. However, software also fails in novel ways that are quite different from hardware systems. Software does not age in the way that mechanical devices will wear out. A logical fault may remain hidden for weeks, months even decades without causing any problems until the relevant section of code is called upon. This property is compounded by the difficulty of testing all possible execution paths through complex software applications. This is particularly difficult where software functionality depends upon many million sets of instructions that can be contingent on multiple combinations of operator input and environmental observations. One consequence is that conventional testing techniques can only be used to identify the presence of bugs

and not their absence; because we cannot be sure that we have covered all possible sequences of instructions. The difficulty of testing software has a knock-on effect in terms of project management. It can be difficult for designated authorities to know when ATM service providers and other development organisations have devoted sufficient resources to software development. All of these reasons provide the rationale for a set of regulatory requirements that specifically address software in ATM systems.

ii) ESARR 3 (Use of Safety Management Systems by ATM Service Providers) requires that safety management systems include risk assessment and mitigation to ensure that changes to the ATM system are assessed for their significance and all ATM system functions are classified according with their severity. It also requires assurance of appropriate mitigation of risks where assessment has shown this to be necessary due to the significance of the change.

ESARR 3 helps designated authorities to assess whether ATM service providers have adopted a rigorous approach to the development of Safety Management Systems. This safety regulatory requirement provides the context for ESARR 6 because it advocates an iterative approach to the improvement of system safety. Risk assessment, design innovation and operational experience help to form a 'virtuous circle' by which appropriate lessons are learned from the small number of adverse events that do occur. This iterative framework is also advocated in the ESARR 6 guidance on safety-related software for ATM systems. In consequence, ESARR 3 and ESARR 6 provide designated authorities with a common structure for audit and inspection.

There are multiple links and dependencies between ESARR 3 and ESARR 6. For example, the safety management systems within ESARR 3 help to ensure that operational staff and safety managers cooperate to monitor adverse events and their precursors. This helps to both validate and extend existing risk assessments in the light of operational experience. It follows that if a risk assessment does not mirror the actual incidents that are being observed then there is a risk that it will not adequately anticipate potential problems. In consequence, it is unlikely that the software mitigation described within ESSAR6 will adequately address key safety concerns. The provisions of ESARR 3 are also important in other ways for the application of ESARR 6 by designated authorities. For example, it is important for ATM service providers to demonstrate that information about software failures is fed back into the operational experience that informs the risk and criticality assessments proposed in ESARR 6.

iii) ESARR 4 (Risk Assessment and Mitigation in ATM) expands ESARR 3 requirements on Risk Assessment and Mitigation, and provides for a comprehensive process to address people, procedures and equipment (software and hardware), their interactions and their interactions with other parts of the ATM system when introducing and/or planning changes to the ATM System.

ESARR 6 provides an important component in the landscape of regulatory requirements that help to shape practice in European Air Traffic Management. It focuses on a particular technical area that has important implications for the more general safety regulatory requirements. ESARR 4 provides designated authorities with criteria for risk assessment and mitigation. It distinguishes between three broad areas of concern: people; procedures and equipment. Hazards stem both from within these areas and in the interactions between them. Software and hardware are explicitly distinguished within the equipment component. The provisions dealing with

software systems in ESARR 4 can be summarised by the following excerpt from the regulatory requirements from section 8.2.2 entitled 'Link with ATM Software Qualification':

> *8.2.2.1 The safety objectives allocated to each hazard drive the determination of specific means to attain the proper level of confidence in the success of implementing the mitigation strategies and related safety requirements.*
>
> *8.2.2.2 These means may include a set of different levels of constraints being set on specific software elements of the ATM System.*
>
> *(ESARR 4, Page 11)*

The provisions within ESARR 4 are consistent with the broad scheme identified in ESARR 6. Each hazard is associated with a safety objective. If this objective is achieved then the associated risk will be acceptable. This concept of an 'acceptable risk' is important because it is, typically, not possible to guarantee absolute safety given finite resources of money, time and expertise. In consequence, ATM service providers must demonstrate to the designated authority that the risks which remain in an application are broadly acceptable or that it is impracticable to support any further risk reduction. In order to achieve these safety objects ATM service providers must demonstrate to the designated authorities that they have employed appropriate mitigation strategies. Service providers must also present arguments that software systems have been developed in such a way that designated authorities have sufficient 'confidence' in their ability to meet the overall objectives.

Clause 8.2.2.2 in ESARR 4 establishes the background for ESARR 6 by recognizing that there may be different levels of confidence associated with different software components. For example, ATM service providers and their development teams may associate lower levels of criticality with software that mitigates low risk events. In consequence, designated authorities would apply a more flexible set of constraints over its development and testing than software that is used to mitigate against high risk failures. Hence the previous two clauses illustrate the close complementary relationship between ESARRs 4 and 6.

iv) ESARR 6 is the continuation of this safety regulatory build up process and expands ESARR 4 in regard with the software aspects of ATM systems. Complementary safety regulatory requirements for hardware aspects are under consideration.

The unique characteristics of software, in terms of its failure modes and the difficulty of testing, as well as the increasing reliance on programmable systems in risk mitigation make it very important that we expand and focus the regulatory framework that is provided within the risk assessment provisions of ESARR 4.

v) Safety is an essential characteristic of ATM systems. It has a dominant impact upon operational effectiveness. ATM systems involving significant interactions in a continuously larger integrated environment, automation of operational functions formerly performed through manual procedures, increase in complexity. The massive and systematic use of software to challenge ATM system complexity is now demanding a more formal approach to the achievement of safety.

The increasing pressure on ATM service providers to improve performance against a range of metrics has helped to motivate a range of technological innovations. Many

of these innovations depend upon the introduction of advanced software systems into different operational areas. These innovations have increased the interconnections and dependencies between subsystems, for example between flight planning and radar systems or between multiple sectors and flight levels. Interconnections imply that a fault in one area can have a massive impact on other aspects of ATM service-provider operations. The consequences of software failure, therefore, create a need for guidance that designated authorities can use to support the audit and inspection of acquisition, development and deployment practices within ATM service providers.

vi) The purpose of this requirement is to provide ATM safety regulatory bodies and ATM service providers with a uniform and harmonised set of safety regulatory requirements for software in ATM systems.

ESARR 6 helps to establish minimum applicable standards. These can be shared across the designated authorities in different countries while also allowing the diversity of implementation practices that is appropriate for the varying needs of different ATM service-providers. By having common software requirements, it is also possible to exchange best practice in meeting the constraints of ESARR 6 within a wider community.

The need to establish minimum applicable standards is reinforced by operational experience. This has identified problems that can only be resolved by a more formal assessment and control of risks induced by new operational concepts, including software development. Errors in design and operational practices have led to air proximity reports and aircraft hazards. Accident and incident investigations have also identified ATM causes. These adverse events have demonstrated the need for a more systematic *a priori* assessment and control of ATM software related risks. In particular, it is necessary to consider the impact of these risks in an ever changing environment. It should be noted that ICAO is mandating the use of safety assessment of significant changes to ATS in amendment 40 to Annex 11. The provisions of ESARR 6 are consistent with the requirements of Annex 11. They help to strengthen ICAO provisions in the key technical area of software development. In addition, the MATSE IV institutional strategy advocates the harmonization of safety levels in ECAC. SRC Terms of Reference also include a requirement to harmonize safety standards and requirements. ESARR 6 supports these objectives by providing designated authorities with consistent guidance across member states.

ESARR 3 provides high level requirements in the area of risk assessment and mitigation. It is not sufficiently detailed to ensure harmonized or consistent processes and outcomes at the ECAC level. In consequence, ESARR 6 has been drafted to provide designated authorities with additional guidance in the technical area of safety-related ATM software. It is now in force and should be implemented throughout ECAC by;

Service providers of ATM, and
ATM designated authorities/safety regulators.

[This space is intentionally left blank]

4. SECTION C – SAFETY OBJECTIVE

(Introductory Material – The provisions of this section in ESARR 6 are not obligatory)

i) The prime software safety objective to be met for ATM systems that contain software, is to ensure that the risks associated with operating ATM software have been reduced to a tolerable level.

To achieve the above safety objective a number of safety regulatory requirements are placed on;

- The ATM service Provider as part of its responsibility to ensure the provision of safe services,

- The Designated Authority as part of its responsibility to;

  - set minimum acceptable levels of safety (in the public interest), including by means of target levels of safety,
  - define applicable national safety regulatory requirements, including those necessary to meet international commitments,
  - define any relevant Standards and Practices that apply to support or complement the requirements,
  - ensure that minimum acceptable levels of safety are met by service-providers,
  - ensure ongoing compliance with national safety regulatory objectives and requirements.

Software helps to mitigate the risks associated with hazards that threaten the integrity of service infrastructure and public safety. Software itself cannot directly cause any injury within an ATM system. Hence the focus here is on the risks associated with *operating* the software and not the software itself.

The objective of ESARR 6 is to reduce any residual risk to a tolerable level. The definition of tolerability is determined by social, political and environmental factors. Hence, there are strong differences between different areas of the globe in terms of the level of acceptable risk within Air Traffic Management. However, ESARR 6 is intended to establish minimum standards across member states. The safety regulatory requirement helps designated authorities to identify the common practices that help ensure the broad tolerability for software related systems in the mitigation of ANS risk between different states.

Subsequent clauses in Section C on Safety Objectives help to establish an organisation set of responsibilities for the provisions within the regulatory requirements of ESARR 6. The requirements to support software safety are part of the wider responsibilities on ATM service-providers to ensure the provision of safe services. These clauses also place responsibilities on the designated authorities that are established in each member state to regulate the activities of the national ANSP. Designated authorities must take the public view into account when establishing the measurable targets for safety that provide a concrete representation of the more subjective bounds for tolerable levels of safety related performance. In other words, in the immediate aftermath of an accident the general public may have unrealistic expectations for safety targets and may be extremely intolerant of any risk

however remote. The designated authority must carefully balance this strong public view against the reasonable technical objectives that might be achieved by an ANSP. Setting objectives that are technically or economically infeasible can lead to a culture of cynicism and tolerance that discredits the most fundamental components of a regulatory framework.

Designated authorities have an international responsibility to establish national requirements for software related systems. EUROCONTROL is one of several bodies that support safety improvements across the aviation industry. Previous sections have cited companion documents, guidance material and standards from bodies such as the ICAO that apply in addition to the regulator structures in ESARR 6. The designated authorities must also monitor the effective implementation of national regulations across their aviation industry. They must determine whether or not organisations actually satisfy the process requirements that are typically outlined in the ESARR requirements. Designated authorities must also conduct a higher level monitoring function to determine whether these particular processes actually do help to achieve the overall safety targets that have been identified for national service providers.

[This space is intentionally left blank]

5. OBLIGATORY PROVISIONS

5.1 ESARR 6 – Section 1 – General Safety Requirements

Guidance in this section elaborates the general Safety Requirements from ESARR 6 section 1 of Obligatory Provisions.

1.1 Within the framework of its Safety Management System, and as part of its risk assessment and mitigation activities, the ATM service-provider shall define and implement a Software Safety Assurance System to deal specifically with software related aspects, including all on-line software operational changes (such as cutover/hot swapping).

The requirement to develop a Software Safety Assurance System (SSAS) does not impose entirely new constraints on ATM service providers because it is a constituent part of the Safety Management System as described in Figure 3.

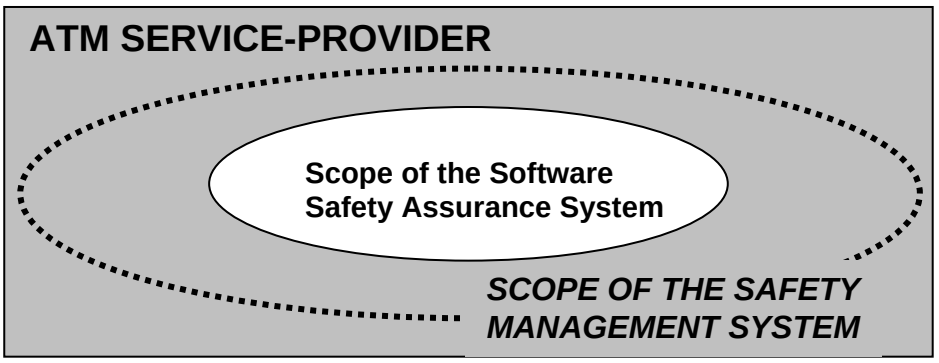


Figure 3: Scoping ESARR 6 within a Safety Management System

Software Safety Assurance Systems cover those aspects of the Achievement and Assurance layers that relate to ATM software within a wider Safety Management System. It is difficult for designated authorities to adequately assess the overall safety of any proposed air traffic management system unless software related risks are explicitly considered. Conversely, software is increasingly implicated in adverse events. Hence there must be a mechanism for ATM service providers to feed back information about previous failures involving programmable systems to inform risk assessment practices and software development techniques.

The growing importance of programmable systems within the provision of air traffic services helps to justify the development of a specific Software Safety Assurance System. Software does not age in the same way that hardware. We cannot reuse existing hardware development techniques to help improve system reliability and availability. In contrast, the introduction of software updates paradoxically increases the chances of an immediate failure in a way that goes well beyond the 'burn in' effects that characterise some hardware components. The establishment of a specific assurance system helps reflect the unique demands of software development. It can create the organisational credibility and funding streams that are necessary if ATM service providers are to adequately resource this function within large, complex and often distributed service providers. The development of these

systems also creates requirements within designated authorities to create the technical skills and expertise to adequately regulate the operation of these software safety assurance systems.

Paragraph 1.1 in ESARR 6 Section 1 – General Safety Requirements, cited above, includes a reference to cutover and hot swapping as a particular issue in software development. ATM service-providers are often required to support continuous operations. There is a requirement to replace systems components, including software, without interrupting service provision. This approach is termed 'cutover' or 'hot swapping' and creates considerable technical challenges including the maintenance of appropriate levels of availability and integrity. In particular, ATM service-providers must be able to provide designated authorities with documented assurance of their ability to resume operations and meet all safety and operational requirements after a swap. They must also provide some assurance of their ability to achieve tolerable levels of risk at all points during and after the cutover.

1.2 The ATM service-provider shall ensure, as a minimum, within its Software Safety Assurance System that;

a) The software requirements correctly state what is required of the software, in order to meet safety objectives and requirements, as identified by the risk assessment and mitigation process;

b) Traceability is addressed in respect of all software requirements,

c) The software implementation contains no functions which adversely affect safety,

d) The ATM software satisfies its requirements with a level of confidence which is consistent with the criticality of the software;

e) Assurances that the above, in order to meet safety objectives and requirements, as identified by the risk assessment and mitigation process;

i. a known range of configuration data, and

ii. a known set of software products and descriptions (including specifications) that have been used in the production of that version.

Software assurance systems help to identify the actions that are necessary to provide evidence that a software product or process satisfies given requirements. The results of a safety assessment process should be used to establish the appropriate software assurance level for all elements of the CNS/ATM system. The previous clauses from ESARR 6 help to establish high level objectives for the Software Safety Assurance System. Point a) establishes a duty to verify that the software requirements actually capture the constraints identified by the need to mitigate particular risks. This is important because there is a danger that the products of a risk assessment are not carried forward into the software acquisition process. In such circumstances, the ATM service-provider would support each necessary stage within ESARR 6 but the integrity of the transitions between stages would not be maintained.

Point b) in ESARR 6 clause 1.2 encourages ATM service providers to demonstrate the traceability of system requirements through to software implementation. Traceability enables independent observers and analysts to reconstruct the path from

an initial risk assessment through the design of mitigation strategies to software criticality assessments and on into implementation. The key idea is that it should be possible for designated authorities to look at any software element and identify its criticality level and then to justify or explain its importance in terms of mitigating key systems risks.

It can be difficult for ATM service providers to convince designated authorities that their software does not contain functions that adversely affect safety. Software can have functioned without bugs in the past; however, this provides no guarantee of future safety. Subtle changes in the environment or in operational practices can lead to input values that trigger the execution of instructions that have not been used in previous operations. Similarly, dynamic testing cannot easily be used to examine the many millions of instruction sequences that are encapsulated within even relatively commonplace systems in Air Traffic Management. The designated authority must, therefore, determine whether or not an ATM service-provider has discharged their obligation under ESARR 6 to apply the appropriate blend of techniques that is required to increase confidence in safety related software even when it is impossible to establish 'safety' in an absolute sense.

Software is an element of the overall system architecture. It can be used to implement a broad range of system requirements, only some of which stem from a concern to mitigate high-risk failures. The software architectures and processes that are used to meet these requirements will, therefore, also vary. For example, individual elements of code might be used to implement low criticality functions. In contrast, high-risk failures might be addressed using redundant software that detects and resolves or mitigates any potential system problems. This diversity creates problems for the designated authority who must ensure that ATM service providers have devoted appropriate resources to these different software systems. ESARR6 introduces the concept of the Software Assurance Level (SAL) to help designated authorities and ATM service providers address these problems. The software assurance level represents the criticality of the ATM software within the ATM system design and the operational environment.

Point c) in ESARR 6 clause 1.2 charges the designated authority with ultimate responsibility for ensuring that ATM service-providers and other associated companies develop software to the required level of confidence. This level of confidence is expressed in terms of software assurance levels. These are determined by the processes of risk assessment and mitigation, described in earlier sections of ESARR 6 building upon ESARRs 3 and 4.

Designated authorities must base their analysis on a 'known range of configuration data, and a known set of software products and descriptions (including specifications) that have been used in the production of that version'. Software is based on a series of abstractions that can be modified, replicated and deleted with minimal effort. This creates considerable potential for confusion if small changes in the executable version of a program are not reflected by consequent changes in the support documentation. Traceability will not be possible unless ATM service-providers and their subcontractors have carefully developed policies for tracking changes. Without this necessary infrastructure it will be possible for designated authorities to follow the development of risk mitigation software from an initial risk assessment into its final implementation in particular lines of code.

[This space is intentionally left blank]

1.3 The ATM service-provider shall provide the required assurances, to the Designated Authority, that the requirements in section 1.2 above have been satisfied.

Although the designated authority has ultimate responsibility for the oversight of the requirements listed above, it is clear that ATM service providers are responsible for their implementation. ESARR 6 places a requirement on ATM service providers to demonstrate to the designated authorities that they have met the various safety objectives cited in the regulatory requirement. It follows that ATM service-providers and their associated sub-contractors must document their means of compliance. Problems can arise if sub-contractors must disclose implementation details of software elements that are commercially sensitive, including COTS ('Commercial off the Shelf') components.

ESARR 6 does not apply to existing or legacy software. It only applies to changes that are made to any CNS/ATM ground systems that already existed when this regulatory requirement came into force. When changes are proposed to existing software, ATM service providers must consult with the designated authority to determine the scope of ESARR 6 requirements. However, ESARR 1 addresses the degree of regulatory involvement that should be anticipated when changes are proposed for existing systems. ESARR 1 makes it clear that a designated authority cannot devote the same level of safety oversight resources to every change in an ATM system. The degree of the regulator's involvement will depend upon the scope of the change.

The criteria and conditions driving the level of safety oversight effort, the degree of the designated authority's involvement and related procedures must be explicitly specified. In that context, ESARR 1 establishes specific safety oversight actions depending upon the type of change under consideration. It identifies minimum boundaries for each category of change which must be addressed through review and acceptance mechanisms. Major changes include, as a minimum, any new system or change:

> Whose assessment of the potential effects of hazards on the safety of aircraft conducted in accordance with ESARR 4, identifies hazards with potential to lead to an accident or serious incident; or
>
> Whose implementation introduces a need for new aircraft standards.

The introduction of new operational units, equipment, operational procedures or airspace structure design provides some clear examples of possible major changes. However, the identification of major and minor changes must, typically, be supported by an initial risk assessment and by an associated high-level safety argument. These arguments are developed by the ATM service provider to demonstrate to designated authorities that a proposed change can be implemented safely, i.e. within tolerable levels of safety. However, nothing should prevent a designated authority from reviewing minor changes. This would be appropriate if, for example, the ATM service provider or the designated authority wanted to improve staff competency in the areas covered within the development of safety-related ATM software.

ESARR 6, paragraph 1.4 has now been moved into ESARR 1.

Each nation (State) is responsible for ensuring that the services provided meet minimum levels of safety in the public interest. Safety regulation is concerned with

the safety competence of the organisations, of systems and of those individuals conducting safety related tasks. Within this more general requirement, the national designated authority is responsible for the three fundamental processes of safety regulation:

- setting safety regulatory objectives and requirements;
- ensuring safety regulatory approval of organisations, operations and where required of the individuals undertaking safety related tasks ;
- ensuring ongoing safety oversight

These high level goals provide a direct link between ESARR 1 (national ATM Safety Regulatory Framework) and the designated authorities that are responsible for monitoring the provisions within ESARR 6. In other words, ESARR 1 describes the manner in which designated authorities must establish safety objectives and requirements through regulatory intervention. They must also be responsible for issuing the approvals to individuals and organisations who conduct safety critical operations within Air Traffic Management. Finally, ESARR 1 establishes the framework by which national designated authorities ensure that their safety oversight and the safety processes of the organisations they support are monitored on a continual basis. ESARR 6 develops these high level requirements within the context of software systems in air navigation service provision.

Competence is a key issue for both the individuals and organisations involved in ensuring the safety of air traffic management services. Even if an ATM service provider establishes exhaustive safety management systems and conducts rigorous risk assessments, there is a danger that safety will be undermined if staff are not competent to implement these processes. Similarly, designated authorities must ensure that their own staff are competent to audit the implementation of software safety processes. These observations reinforce further links between the requirements of ESARR 6 on software development and those of ESARR 5 that describe key requirements for the recruitment and training of ATM personnel.

[This space is intentionally left blank]

5.2 ESARR 6 - Section 2 - Requirements Applying to the Software Safety Assurance System

Guidance in this section elaborates the requirements applying to the Software Safety Assurance System from ESARR 6 Section 2 of Obligatory Provisions.

2.1 The ATM service-provider shall ensure, as a minimum, that the Software Safety Assurance System - Is documented specifically as part of the overall Risk Assessment and Mitigation Documentation;

This clause reinforces the links between ESARR 6 on software development and ESARR 3 on the use of Safety Management Systems by ATM service-providers:

> *5.3.4. Risk Assessment and Mitigation Documentation Within the operation of the SMS*
>
> *…shall ensure that the results and conclusions of the risk assessment and mitigation process of a new or changed safety significant system are specifically documented, and that this documentation is maintained throughout the life of the system.*
>
> *(ESARR 3, page 12)*

The ATM service provider must create and maintain a system for documenting the products of a Software Safety Assurance System within the wider processes for documenting risk assessment and mitigation. This is an important requirement because of the specialist, technical nature of software safety assessments. There is a danger that the individuals and teams responsible for this work will fail to adequately communicate their results to their co-workers who must support the wider systems risk assessments in other areas of ATM service-provider operations. If the results of a software safety assessment are not well integrated with these wider processes of risk assessment and mitigation then it will also be difficult for the ATM service provider to demonstrate to the designated authority that they have met the traceability requirements in ESARR 6. In other words, it will be hard if not impossible to trace the ways in which software elements help to mitigate the risks that arise from equipment under control. ESARR 3 requires that documentation must not simply be developed and then forgotten during the later stages of deployment. ESARR 6 extends these requirements. ATM service providers must show designated authorities that they have considered the links between software safety assessment processes and wider risk assessments. These links must be documented and maintained during the operational lifetime of ATM/CNS systems, including decommissioning.

2.2 The ATM service-provider shall ensure, as a minimum, that the Software Safety Assurance System - Allocates software assurance levels to all operational ATM software;

Software assurance levels provide the link between systems risk assessments and the level of rigour to be associated with different software components. In other words, the more significant a software component is to the detection, avoidance or mitigation of system risks then the higher the level of assurance that is necessary. As we have seen, however, this requirement relates only to new systems and to

existing software where major changes have been proposed, as defined within ESARR 1.

ESARR 6 establishes a framework in which software assurance levels help determine the development, verification and validation resources allocated to software elements. The assurance levels in turn are related to the risk and hazard assessments that shape the functional and non-functional requirements for the software. The key contribution of section 2.2 in ESARR 6 is to clearly state that it must be possible for designated authorities to identify the software assurance level that is associated with every software element, including documentation and associated data, in ATM systems.

There are complex interconnections and dependencies between ATM software. It is possible for software elements that are associated with a relatively high assurance level to be compromised by bugs in software components that do not have a particular criticality level. These dependencies create a considerable challenge for ATM service-providers given the diverse software systems that are integrated across many different operational areas. It should be noted that the previous paragraph does not explicitly focus on 'front line' operations such as control room software. In contrast, it applies to ATM/CNS systems in general.

2.3 The ATM service-provider shall ensure, as a minimum, that the Software Safety Assurance System - Includes assurances of software;

- requirements validity,
- verification,
- configuration management, and,
- traceability.

The first bullet point in ESARR 6, clause 2.3 refers to 'requirements validity'. Validation provides an assessment of the value or worth of particular requirements. It is an important concept for designate authorities who must assess the validity of system requirements. If ATM service providers identify flawed requirements then a system may be unsafe even if they can demonstrate to the designated authorities that software components meet those requirements. In other words, ATM service providers must convince designated authorities of the validity of system requirements for safety-related ATM/CNS software.

The second item in ESARR 6, clause 2.3 refers to verification. This is the process by which we establish whether or not the software actually does meet system safety requirements. This is an important distinction. Validation can only be seen in terms of application goals, as a means of determining the value of a set of requirements. Verification can be seen as a more technical process of proving whether or not software meets a set of requirements. Hence it is closely related to issues of traceability between requirements and particular software elements within an implementation. ATM service providers must demonstrate to the designated authority that they have adopted appropriate techniques to test or verify there software systems meet those safety requirements that have been validated for an ATM/CNS system.

The third bullet point in ESARR 6, clause 2.3 focuses on configuration management. This is critical because software systems offer considerable flexibility in the

implementation techniques that are available to ATM service-providers and their contractors. The configuration of programmable systems can be modified in response to changes in the operational environment. They offer a degree of flexibility that could not have been considered with previous generations of hardware based systems. However, this creates dangers that can arise for ATM service providers during the deployment of safety-related software systems. It can be difficult to determine which of many versions of a program is actually running on a target platform. It can also be difficult to ensure that the software which controls infrastructure configuration does not accidentally disable key support functions. Hence, the management of configuration information and its associated documentation are an important concern during the development and operation of ATM software. They are also, therefore, of considerable importance to the designated authorities who must assess the processes and procedures that are used during the development and operation of safety related systems.

The final point in ESARR 6, clause 2.3 refers to traceability. This relates to the ability to identify the links between risk analysis and mitigation, software requirements, criticality assessments, design and implementation documentation and testing. In other words, it must be possible for ATM service providers and designated authorities to trace the way in which risk mitigation is implemented within particular software elements in ATM applications. If this cannot be done then there is a danger that some hazards will be overlooked.

2.4 The ATM service-provider shall ensure, as a minimum that the Software Safety Assurance System - Determines the rigour to which the assurances are established. The rigour shall be defined in terms of a software assurance level, and shall increase as the software increases in criticality. For this purpose:

a) the variation in rigour of the assurances per software assurance level shall include the following criteria;

- required to be achieved with independence,
- required to be achieved,
- not required.

b) the assurances corresponding to each software assurance level shall give sufficient confidence that the ATM software can be operated tolerably safely.

The previous section from ESARR 6 requires that ATM service-providers must use software assurance levels to determine the level of rigour in developing software elements. ATM service providers must demonstrate to designated authorities that greater resources of time, effort and expertise are allocated to the design, development and testing of software that is associated with higher assurance levels. Resources must be allocated in proportion to the criticality of the mitigation function that is implemented by each section of code.

The ‘minimum’ reference in ESARR clause 2.4 indicates that additional resources may be allocated to software over and above those normally associated with a particular level of criticality. This would be the case if, for example, a section of code implements a particularly complex function. In general, there is an assumption that ATM service-providers will strive to achieve the highest level of rigour that is possible. However, the resource allocation should never fall below the minimum that designated authorities recommend for each level of criticality.

ESARR clause 2.4 goes on to identify three further issues that must be considered by ATM service providers and designated authorities when determining the degree of rigour to be associated within each software assurance level. The clause distinguishes between requirements that are to be achieved 'with independence', those that are required to be 'achieved' and those that are important but are not requirements in themselves. The term 'independence' is clarified within the appendices of ESARR 6:

> *For software verification process activities, independence is achieved when the verification process activities are performed by a person(s) other than the developer of the item being verified; a tool(s) may be used to achieve an equivalence to the human verification activity. (ESSAR 6, page 17)*

ATM service providers can call upon human auditors and automated tools to increase the independence of any verification carried out during the software assurance process. ATM service-providers must assess the degree of independence that is to be achieved. This can determine whether or not external agencies must be used or whether independence can be achieved through inspections by individuals and groups from other areas of an organisation. This decision may initially involve some consultation with representatives of a designated authority until ATM service providers develop additional expertise in the implementation of ESARR 6. Similarly, consultations between service providers and designated authorities may be needed to determine the level of assurance provided by automated tools. For example, it can be difficult for members of a development team to consider the wide range of safety properties that must be considered during the application of these tools and techniques. Independent consultants can add a fresh perspective that is often missing from in-house assurance projects.

The final sentence of ESARR clause 2.4 requires that the rigour associated with each assurance level is sufficient to justify confidence that the 'software can be operated tolerably safely'. ATM service-providers must ensure that the techniques and processes that are recommended as minimum requirements for software development at each assurance level will achieve the necessary confidence in the overall system. The designated authority provides the final arbiter for determining whether or not a service provider has achieved the necessary level of rigour for a particular software assurance level. This reinforces links between ESARR 6 and clause 2.4 and clause 1.3 introduced in previous sections:

> *1.3 The ATM service-provider shall provide the required assurances, to the Designated Authority, that the requirements in section 1.2 above have been satisfied.*
>
> *(ESARR 6, page 11)*

If these techniques and processes are too onerous then the resulting application may be over-engineered and finite development resources may be diverted from other more critical aspects of a safety-critical system. Conversely, if the minimum requirements for each assurance level are too lax then it is likely that any resultant software will fail to achieve the intended mitigation that was identified in previous risk assessments.

2.5 The ATM service-provider shall ensure, as a minimum, that the Software Safety Assurance System - Uses feedback of ATM software experience to confirm that the Software Safety Assurance System and the assignment of assurance levels is appropriate. For this purpose, the effects resulting from any software malfunction or failure from the ATM operational experience reported according to ESARR 2, shall be assessed in respect of their mapping to ESARR 4.

ESARR 6 clause 2.5 argues that ATM service providers must validate assumptions about the frequency and severity of adverse events using the insights obtained from incident reporting systems. Designated authorities must, therefore, ensure that service providers implement feedback mechanisms to support learning from previous instances of software failure. ESARR 2 deals with the development of Safety Measurement and Improvement Programmes. In an appendix to this document, there is an explicit reference to the need for ATM service-providers to consider software within the causal classification of incidents and near misses:

> *A-3.3.1 Causes that combined to result in the occurrence shall be classified according to the following high level categories:*
>
> *…*
>
> *ATM service infrastructure/facilities/technical systems*
>
> - *Hardware issues*
> - *Software issues*
> - *Integration issues*
> - *Aerodrome layout and infrastructure*
>
> *…*
>
> *(ESARR 2, page 16)*

Clause 2.5 from ESARR 6, given above, identifies this connection between the two EUROCONTROL regulatory documents. The analysis of adverse events provides important feedback about whether or not the techniques associated with different software assurance levels are helping to prevent the causes or mitigate the consequences of software failures. Given that many software systems perform novel and innovative functions, it is critical that ATM service-providers make best use of the operational experience gained from their software systems. This is also important because resources often have to be specifically allocated to ensure that investigatory personnel have sufficient training to diagnose when software is involved in the causes of a minor accident or near-miss incident.

2.6. The ATM service-provider shall ensure, as a minimum, that the Software Safety Assurance System - Provides the same level of confidence, through any means chosen and agreed with the Designated Authority, for developmental and non-developmental ATM software (e.g. Commercial Off The Shelf software, etc) with the same software assurance level.

Much safety-related ATM software is developed through private negotiation between developers and ATM service-providers. However, there are increasing pressures to use ‘Commercial off the Shelf’ (COTS) software in ATM/CNS systems. COTS applications are, typically, sold by vendors through public catalogue listings. They are not usually intended to be customised or enhanced. COTS are, therefore, referred to as non developmental items (NDI).

COTS software has considerable attractions. These go beyond the lower costs that are often associated with acquiring these systems. The increased user-base for COTS can provide additional data about potential failures, which can be shown to designated authorities. Any known problems are reported and resolved over a relatively short timescale. The large volume of sales often implies higher levels of

support and documentation than can be expected for developmental software systems. However, the development practices associated with COTS may not meet the requirements for assurance and traceability in ESARR 6. In particular, the commercial sensitivity of these systems makes it unlikely that ATM service-providers will obtain the source code that can be necessary to perform 'white box' tests that deliberately expose potential weaknesses using knowledge of the internal implementation. It is, therefore, more difficult to convince designated authorities that the requisite level of rigour has been used to support the development and deployment of COTS for higher software assurance levels.

ESARR 6 requires that ATM service providers demonstrate the same level of rigour to designated authorities for both developmental and non-developmental software at the same software assurance level.

ATM service providers cannot automatically rely on "success stories" about the previous uses of software in other applications to increase designated authority's confidence in new applications. Such successes may not be replicated when software is exploited in another operating environment or by different groups of end users. However, in-service experience can be used as part of a wider argument between the service provider and the designated authority. The rigour and depth of this argument will always need to be established on a case by case basis.

ATM service providers may find it necessary to reduce the assurance level associated with software components for which it is difficult or impossible to access developmental data. For example, State X might operate the same ATM software application at a different level of assurance than it operated in State Y due to a range of local factors. These can include access to developmental data that might be restricted in some states. Different levels of assurance may also reflect the use of different hardware, different operating procedures, staff training and expertise etc.

It is not always possible to provide the same level of assurance for COTS applications as it is for developmental software systems. However, ATM service providers can use alternate methods to augment design assurance data for COTS software components at a desired assurance level. When COTS are used on a CNS/ATM system, designated authorities shold expect the allocation of additional resources to software planning, acquisition and verification. Risk mitigation techniques may also be used to reduce the CNS/ATM system's reliance on COTS. The goal of these mitigation techniques is to reduce the effect of COTS on CNS/ATM system functions. Risk mitigation techniques can be implemented through combinations of people, equipment, procedures or architecture.

There are no 'special exemptions' for COTS software. Designated authorities should expect the same levels of rigour for code that was developed 'in house' as for code developed by other organisations at the same level of criticality.

[This space is intentionally left blank]

5.3 ESARR 6 - Section 3 – Requirements Applying to the Software Assurance Level

Guidance in this section elaborates the requirements applying to the Software Assurance Level from ESARR 6 Section 3 of Obligatory Provisions.

3.1 The software assurance level relates the rigour of the software assurances to the criticality of ATM software by using the ESARR 4 severity classification scheme combined with the likelihood of a certain adverse effect to occur. A minimum of four software assurance levels shall be identified, with software assurance level 1 indicating the most critical level.

Software is used in many diverse aspects of ATM/CNS systems. Many software components implement critical system requirements while others do not have any strong relation to systems safety. It is, therefore, important to categorise software according to different levels of criticality. Designated authorities can then refer to these criticality assessments when determining whether or not an ATM service provider has demonstrated a sufficient level of rigour during systems development. The assessment of criticality may lead developers to implement redundant architectures or to depend upon single paths of execution. Criticality assessment can be done using the Software Assurance Level (SAL) approach that is described in ESARR 6. The software assurance level represents the criticality of the ATM software within the ATM system design and the operational environment.

ESARR 4 identifies a five level severity classification scheme that can be summarised as follows:

1. Accidents.

   Examples of the effects on operations include one or more catastrophic accidents, one or more mid-air collisions, one or more collisions on the ground between two aircraft, one or more Controlled Flight Into Terrain, total loss of flight control. In addition there exists no independent source of recovery mechanism, such as surveillance or ATC and/or flight crew procedures can reasonably be expected to prevent the accident(s).

2. Serious incidents,

   Examples of the effects on operations include a large reduction in separation (e.g., a separation of less than half the separation minima), without crew or ATC fully controlling the situation or able to recover from the situation, one or more aircraft deviating from their intended clearance, so that abrupt maneuver is required to avoid collision with another aircraft or with terrain (or when an avoidance action would be appropriate).

3. Major incidents.

   Examples of the effects on operations include large reduction (e.g., separation of less than half separation minima) in separation with crew or ATC controlling situation and able to recover the situation. minor reduction (e.g., separation of more than half separation minima) in separation without crew or ATC controlling the situation, hence jeopardizing the ability to recover from the situation (without use of collision or terrain avoidance maneuvers).

4. Significant incidents.

   Examples of the effects on operations include q increasing workload of the air traffic controller or aircraft flight crew, or slightly degrading the functional

capability of the enabling CNS system, minor reduction (e.g., a separation of more than half the separation minima) in separation with crew or ATC controlling the situation and fully able to recover from the situation.

5. No immediate effect on safety.

   Examples of the effects on operations include no hazardous condition i.e. no immediate direct or indirect impact on the operations .

There is no one-to-one mapping between ESARR 4 and ESARR 6. For example, if a System is assessed to be at criticality level 2 then it does not follow that all of the software components will be at Software Assurance Level 2. Appropriate procedural, human, environmental mitigations can be used to downgrade the assurance level associated with the ATM software that supports system functions.

ATM service-providers and designated authorities must consider the mapping between the two ESARRs in determining appropriate software assurance levels for ATM software components. it is important consider:

- the criticality of ATM software using the ESARR 4 severity classification scheme combined with the likelihood of a certain adverse effect occurring;

- the allocated software assurance shall be commensurate with the most adverse effect, following the requirements of ESARR 4, taking into account the software failures but also the identified defences;

- independence between components and their criticality

3.2 An allocated software assurance level shall be commensurate with the most adverse effect that software malfunctions or failures may cause, as per ESARR 4. This shall also take into account the risks associated with software malfunctions or failures and the architectural and/or procedural defences identified.

Adverse effects are not limited to the boundaries of the system being analyzed. They can extend beyond the components and systems involved in ATM/CNS services out into the environmental context for ATM operations. Service providers must demonstrate to designated authorities that they have considered the combined effect of hazards. These will usually be related to the operations of aircraft (e.g. aircraft deviating from cleared flight level) and provisions of ATM services (e.g. transfer of communication between FIRs); failure conditions will then relate to the functions enabling the provision of ATM services (e.g. loss of surveillance function).

ESARR 4 does not specify whether or not ATM service providers should consider the extent of a hazard (e.g. loss of surveillance for more than 30 seconds). The use of such quantifiers during a risk assessment relates to the implementation of the regulatory requirement rather than to the regulatory requirement itself and hence is outside the scope of ESARR 6.

ESARR 4 establishes a framework for considering the worst case scenario. This is important because ATM service providers must demonstrate to designated authorities that they have considered these adverse consequences when identify the software assurance level to be associated with particular components of ATM/CNS systems. The severity of hazards will be determined by the credible consequences on the managed aircraft, when the outcomes of all the safeguards which may exist in

the other parts of the ATM System have been taken into consideration. ESARR 4 states that the most severe class will only be chosen in such cases when the total ATM System has exhausted its possibilities to affect what continues to happen and only chance determines if the consequence will be a collision or not.

3.3. The ATM service-provider, as a minimum within the Software Safety Assurance System, shall ensure that: - ATM software components that cannot be shown to be independent of one another shall be allocated the software assurance level of the most critical of the dependent components.

ESSAR 6 describes independent software components in the following terms:

> *"Those software components which are not rendered inoperative by the same failure condition that causes the hazard".*
>
> *(ESSAR 6, page 17)*

It, therefore, follows that any two software components that can be affected by the same failure condition should not be considered independent. Dependencies often exist between software components where a common fault impairs the operation of those components but where the fault does not necessarily lead to a complete failure to operate. The previous excerpt from the regulatory requirement formalises the intuition that where any dependencies exist the different software components should inherit the highest software assurance level of any of the dependent components. If this heuristic were not to be followed then the assurance level might be diluted by the introduction of less critical code into high assurance software.

[This space is intentionally left blank]

5.4 ESARR 6 - Section 4 – Requirements Applying to the Software Requirements Validity Assurances

This section of the ESARR 6 guidance addresses section 4 of the obligatory provisions. The following paragraphs focus on the assurances that ATM service providers must provide to the designated authority in order to demonstrate that they have validated software requirements.

The ATM system definition process can be divided into two separate activities. The first is system requirements definition which captures and specifies the services and/or functions to be performed by the ATM system. The second is system design which allocates system requirements to hardware, software and in certain cases, to the operator.

The ESARR 6 software requirements deal exclusively with safety aspects and are directly derived from system level requirements. ESARR 6 develops key definitions from ESARR 4:

- System requirements are derived following the approach described in ESARR 4 using a risk mitigation strategy.

- System requirements may take various forms, including organisational, operational, procedural, functional performance and interoperability requirements or environment characteristics.

- Software requirements are derived from system requirements and provide a description of the intended software behaviour given a particular set of inputs and environmental constraints.

- If an implementation meets a set of software requirements then it will satisfy operational needs without endangering the safety of ATM operations.

ESARR 6 demands that Software Safety Assurance Systems are used to avoid the introduction of any function that adversely affects safety. It also states that software requirements must be correct and complete. In other words, they must correctly identify the system safety requirements that are to be met by software systems. There is an assumption in ESARR 6 that the term ‘software requirements’ refers to safety-related constraints. This safety regulatory requirement DOES NOT address the Quality Assurance of ATM Software.

4.1 Specify the functional behaviour (nominal and downgraded modes) of the ATM software, timing performances, capacity, accuracy, software resource usage on the target hardware, robustness to abnormal operating conditions and overload tolerance, as appropriate.

As mentioned in the guidance on ESARR 6 clause 2.3, validation focuses on the value or utility of a requirement while verification establishes the truth of whether or not a requirement has been satisfied.

Software specifications must consider an adequate range of constraints that collectively characterise the intended operational behaviour of an implementation. These characteristics include timing performance, software resource usage on the target hardware, robustness to abnormal operating conditions and overload tolerance. This list from ESARR 6, clause 4.1 is a minimum set of validation requirements. In other words, this information must be specified in order to have a 'valuable' or 'valid' specification.

Some of the concepts used in clause 4.1 deserve further explanation. Timing issues are relatively straightforward and consider a range of scheduling constraints, including hard real-time deadlines. The term 'software resource usage on the target hardware' encourages ATM service providers to consider many different issues including processor requirements, primary and secondary memory requirements, network bandwidth and so on. Designated authorities must ensure that these different aspects of resource usage are considered at a level of detail that is likely to yield accurate results. The reference to overload tolerance and to abnormal operating conditions urges regulators to ensure that ATM service providers have considered what might happen if software applications exceeded the resources that are anticipated for ATM safety-related software systems. In addition, they must also consider a range of adverse scenarios that can often be triggered by changes in the operational environment. Other terms used in the previous excerpt are defined within ESARR 6 itself.

4.2 The ATM service-provider, as a minimum, within the Software Safety Assurance System, shall ensure that software requirements - Are complete and correct, and are also compliant with the system safety requirements.

ESARR 6 provides initial guidance for the interpretation of this clause by defining the completeness and correctness of software requirements as follows:

> *"All software requirements correctly state what is required of the software component by the risk assessment and mitigation process and their implementation is demonstrated to the level required by the Software assurance level. Therefore, the software component will remain tolerably safe as required by ESARR 4".*
>
> *(ESARR 6, page 16)*

A 'correct and complete software verification process' assumes that the requirements correctly state what is required of the software component in order to satisfy any risk mitigation that was required by a system level risk assessment. Designated authorities must also ensure that ATM service providers can demonstrate the implementation of software requirements conforms to the level of rigour required by any associated software assurance level.

ESARR 4 and ESARR 6 require that ATM service providers can demonstrate to designated authorities that ATM/CNS applications are tolerably safe. This is a minimum requirement. Many national bodies also require that system level risks should be 'as low as is reasonable' (ALAR). In other words, the level of risk should not only be tolerable but it should be further reduced to the extent that is reasonable given existing technological constraints. During the drafting of ESARR 4, it was concluded that ALAR is a UK specific legal concept. It does not apply "*ad-literam*" in other European States. However an equivalent concept to ALAR is embedded within ESARR 4 Annex A-2:

> *….additional safety management considerations shall be applied so that more safety is added to the ATM system whenever reasonable*
>
> *(ESARR 4, page 17)*

This clause should be read in conjunction with ESARR 4 requirement 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:-*
>
> *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 including, as appropriate, specifications of any predictive, monitoring or survey techniques being used;*
>
> b. *that all safety requirements related to the implementation of a change are traceable to the intended operations/functions.*
>
> *(ESARR 4, page 10)*

[This space is intentionally left blank]

5.5 ESARR 6 - Section 5 – Requirements Applying to the Software Verification Assurances

Guidance in this section elaborates the Requirements applying for Software Verification Assurance from ESARR 6 section 5 of the Obligatory Provisions.

5.1 The functional behaviour of the ATM software, timing performances, capacity, accuracy, software resource usage on the target hardware, robustness to abnormal operating conditions and overload tolerance, comply with the software requirements.

This section of the ESARR 6 regulatory requirements extend previous constraints from clauses 2.3 and 4.1, which focused on the validation of functional behaviours, to now consider the verification of those behaviours. Validation focuses on the value or utility of a requirement. In contrast, verification establishes the truth of whether or not a requirement has been satisfied.

It is a non-trivial task for ATM service providers to demonstrate to a designated authority that an implementation or design will meet particular behavioural requirements. For example, the calculation of performance timings creates a host of practical and technical problems that must be addressed during the more detailed development stages. The impact of caching techniques must be addressed in order to accurately anticipate task performance on particular target platforms. Similarly, establishing whether or not software will meet resource usage constraints can involve complex static analysis and a host of more dynamic techniques, including the monitoring of CPU and bus or network utilisation under a broad range of conditions. The verification of these properties can lead on to further issues of validation. For example, ATM service providers and their contractors must ensure not just that software performs in the manner anticipated but also that any environmental factors used in performance simulation are valid approximations for a broad enough range of likely operational conditions. Designated authorities must also have staff with the relevant technical skills to determine whether or not service providers have used verification techniques that provide an appropriate level of rigour for the assurance level associated with particular software components.

5.2 The ATM service-provider, as a minimum, within the Software Safety Assurance System, shall ensure that :- The ATM software is adequately verified by analysis and/or testing and/or equivalent means as agreed with Designated Authority.

The Software Safety Assurance System provides a framework that ATM service providers can use to guide the allocation of development resources to different software components in a considered and consistent manner. Software assurance levels can be selected using system level risk assessments. The criticality of the software is determined by the impact that a programmable application has for the mitigation of system risks. These software assurance levels can be used to determine the level of rigour that is required during development activities, including verification. Each stage of the Assurance System can be documented and demonstrated to the designated authority.

Appropriate testing and analysis tools are determined by the software assurance level. These verification techniques increase confidence in software reliability. They are, therefore, a very important element of the software development process. However, they are not the central feature of software development as they were in previous generations of product based standards.

ATM service-providers must supply designated authorities with arguments and evidence to show that each and every software requirement has been satisfied completely and correctly. These arguments and evidence can be based on a number of different sources including testing, field service experience or analysis. If more than one source of evidence is provided then designated authorities should be able to access supporting information from each of these sources.

Where direct tests are used then the designated authority must be able to access arguments and evidence to show that the tests have been designed to consider all behaviors that might affect each safety requirement. ATM service provides must also demonstrate that the tests have been executed and passed as anticipated. Evidence should include test specifications, test criteria, test results, an analysis of test results as well as any faults discovered during testing. Service providers must also ensure that testing techniques have been approved for the relevant assurance level by the designated authority. Tests must accurately characterize the operational environment and working demands, including normal and more extreme situations. Tests must be designed to provide adequate coverage of the input domain and should be independent from the design process. It should also be possible for the designated authority to establish that any faults discovered during testing have been adequately addressed. ATM service providers must demonstrate that such faults do not continue to affect system level safety.

Where field service experience is used then the designated authority must be provided with well documented criteria to determine whether field data supports or weakens arguments about safety requirements. The supporting analysis must establish that these fail/pass criteria have been met. Service providers must collate all of the supporting evidence including history of modifications, bug reports, etc. They must demonstrate that field service evidence is obtained from systems that can easily be compared to the software that is under development. Similarly, the existing environment and hardware platforms must be comparable to those for the proposed deployment. ATM service-providers must demonstrate that field service data captures the full range of software requirements from previous deployments. Any faults exposed during existing operations must be well documented and evidence must be provided to demonstrate that these faults have been resolved in any subsequent implementation.

ATM service providers can use design evidence to demonstrate that to designated authorities that an appropriate level of rigor has been used during the development of software elements. Pass/fail criteria must again be identified to establish whether or not suitable design processes have been used for particular software assurance levels. These criteria can impose constraints on the transformations that are used in order to generate executable programs from high-level designs. For example, if an approved design process is used to support the development of source code then ATM service providers must show the designated authorities that the intended behavior of the source code is preserved in any object code. If design notations are to be used to support software development then they must capture attributes of the software behavior that can influence system level safety. ATM service-providers must also convince designated authorities that their staff has the competence and expertise to successfully conduct any analysis. Any assumptions about hardware and operator performance must be easily reviewed and validated. Abstractions must be adequate to capture all attributes that might have an impact on system requirements. Formal proofs and other forms of annotated argument must be demonstrated to be correct by either manual inspection or through automated tool, including theorem provers and model checkers. If tools are to be used then service

providers must supply designated authorities with arguments and evidence to establish confidence in the results that they produce.

5.3 The ATM service-provider, as a minimum, within the Software Safety Assurance System, shall ensure that :- The verification of the ATM software is correct and complete.

ESARR 6, clause 5.3 extends correctness and completeness criteria from validation to include the verification of safety-related ATM software. This creates traceability requirements between different levels of verification. In other words, establishing that a particular design will satisfy higher level safety requirements need not guarantee that any software implementation will also meet those requirements. Hence, it is important to show that those same tests can be fulfilled at each successive level of development towards implementation and the execution of object code on a target processor.

[This space is intentionally left blank]

5.6 ESARR 6 - Section 6 – Requirements Applying to the Software Configuration Management Assurances

Guidance in this section elaborates on the requirements applying to the Software Configuration Management Assurances from ESARR 6 section 6 of the Obligatory Provisions.

6.1 The ATM service-provider, as a minimum, within the Software Safety Assurance System, shall ensure that - Configuration identification, traceability and status accounting exist such that the software life cycle data can be shown to be under configuration control throughout the ATM software life cycle.

ATM service-providers must demonstrate to designated authorities that they maintain good control over the configuration of their software. Previous sections have stressed that the flexibility of programmable systems creates enormous opportunities to adapt safety-critical systems in response to environmental changes or revised operational practices. Similarly, software updates can be implemented, distributed and installed over a relatively short timescale. These benefits create significant logistical problems. It can be difficult to determine the precise version of a program that is running on particular platforms. Inadequate configuration management and version control can undermine confidence, for example, if ATM service providers cannot convince designated authorities that test results relate to a particular software system.

The ability to reconfigure hardware components using dynamic programming or plug and play techniques creates significant additional complexity. It is likely that the application of these approaches will grow from their present, limited levels. Hence status accounting is a key issue for the support and technical staff who must maintain safety-critical software. The closing sentence of ESARR 6, clause 6.1 reiterates the importance of keeping this information up to date from the initial development through to decommissioning. During subsequent operational phases, the initial development team may no longer be available to help diagnose software configuration problems in the aftermath of bug reports and other adverse events.

6.2 The ATM service-provider, as a minimum, within the Software Safety Assurance System, shall ensure that - Problem reporting, tracking and corrective actions exist such that safety related problems associated with the software can be shown to have been mitigated.

ATM service providers must demonstrate to designated authorities that they have mechanisms to ensure that any problems identified during software development are documented and corrected. Similarly, there must be means for operational staff to feed back experience with programmable systems into the development of subsequent safety related software applications. It is equally important to monitor any occurrence of the system level hazards that software is intended to mitigate. If such failures occur then software requirements may have been incomplete or incorrect. ATM service providers must also have procedures in place to determine whether or not system level failures stemmed from the inadequate implementation of software components.

Service providers can call upon evidence from a variety of sources to convince designated authorities that they have an appropriate approach towards configuration management. The designated authority must be able to determine that all arguments and any associated evidence relates to a known executable version of the

software. If evidence is provided that is not related to the current executable version then additional arguments must be produced to convince designated authorities of the clear and direct relationship between different versions of the system. If any evidence or data has been altered then the designated authority must be able to identify those changes and accept the justification to support the alterations. These sources of evidence and artifacts relating to configuration consistency include but are not limited to source code, object code, system safety requirements, software requirements as well as any data that supports key aspects of ATM service provision. Configuration data also includes manuals and other forms of documentation, test designs and test results. ATM service providers must also supply the designated authority with information about the compilers and associated development tools, as well as the hardware upon which the tools are executed.

If ATM service providers use configuration management tools then they must be able to convince designated authorities that these support systems preserve critical properties of the application software. In other words, configuration management tools must be validated and verified to a level of rigor that reflects the impact that they can have upon the behavior of safety-related ATM software.

6.3 The ATM service-provider, as a minimum, within the Software Safety Assurance System, shall ensure that - Retrieval and release procedures exist such that the software life cycle data can be regenerated and delivered throughout the ATM software life cycle.

Most of the previous requirements within ESARR 6 create processes that generate documentation. It is impossible, for instance, to demonstrate the traceability that was advocated in the Software Assurance Framework without having sufficient documentation to support comparisons between the various activities involved in risk assessment, mitigation, software design and implementation. It is clearly important for ATM service-providers to be able to manage and maintain the mass of documentation that can be generated by these different activities. Similarly, there is little prospect of ensuring consistency between different teams or development projects if key documents cannot easily be shared, for instance to show that similar hazards are related to similar risks in different development projects.

ESARR 1 charges the designated authority with a responsibility to conduct reviews following the introduction of new systems or major changes to existing applications. These review processes depend upon ATM service providers delivering appropriate documentation for inspection by the designated authority. Nothing prevents a designated authority from reviewing the documentation associated with minor changes should this also be deemed necessary. The objective of the review is to provide a rationale for the designated authority's decision to accept or reject proposed changes to the ATM infrastructure.

Guidance material for ESARR 6, clause 5.2 has described a range of sources that provide evidence to support arguments about the safety of ATM/CNS software. In order to eliminate discrepancies in the application of the technical software review process, it is necessary to use documented procedures. In addition, specific documentation is required to provide the safety oversight personnel who are involved in the process with guidance on how to perform their functions. Designated authorities also conduct audits to verify that service providers follow the documented processes during the introduction of new applications and during major changes to existing systems.

ESARR 1 also stresses the need for coordination with Airworthiness and Flight Operations Authorities. Aviation services increasingly depend upon a network of inter-related ground and airborne elements. Changes in ATM service provision can, therefore, have consequences for many other organizations, including airlines, airport management, ground service teams etc. Conversely, the safe introduction of changes in any of these wider systems must be coordinated if they are not to adversely affect the safety of ATM operations. The nature of this coordination and the necessary exchange of documentation depend on the nature of the changes being planned and upon the consequences of any software developments within these wider development activities.

[This space is intentionally left blank]

5.7 ESARR 6 - Section 7 – Requirements Applying to the Software Requirements Traceability Assurances

Guidance in this section elaborates on requirements for Software Traceability Assurance in ESARR 6, section 7 of the Obligatory Provisions.

7.1 The ATM service-provider, as a minimum, within the Software Safety Assurance System, shall ensure that :- Each software requirement is traced to the same level of design at which its satisfaction is demonstrated.

It must be possible for designated authorities to trace the manner in which software elements satisfy particular system level safety requirements. The rigor or extent of this requirement depends upon the software assurance level associated with code. For instance, if a relatively high level of assurance is required then ATM service providers must create documentation that traces the relationship between high-level requirements and particular lines of source code. It may be sufficient to trace the implementation of less critical requirements to higher levels of abstraction, such as a description of the software architecture.

7.2 The ATM service-provider, as a minimum, within the Software Safety Assurance System, shall ensure that :- Each software requirement, at each level in the design at which its satisfaction is demonstrated, is traced to a system requirement.

ESARR 6 clause 7.2 is the complement of clause 7.1. To meet this regulatory constraint, arguments of software safety requirements' traceability shall be available to demonstrate that:

(a) All hazards identified at each level in the design or in the software implementation are traceable to a mitigation/barrier or to a justification that no such defence is necessary. These mitigating factors or barriers include but are not limited to safety requirement for software, hardware or operational practices.

(b) The set of software safety requirements includes all criteria derived or changed during the requirements determination and design processes.

(c) Each system level safety requirement that generates a software requirement can be traced to an element of the design, ranging from high-level architectural descriptions through to the source code, at a level of rigour that is determined by the software assurance level.

(d) Any non-safety functions existing in the implementation cannot degrade safety.

To give confidence in the traceability of design documentation, ATM service providers must collate evidence to demonstrate to designated authorities that:

(a) The software safety requirements are unambiguously and consistently identified.

(b) The implementation of all software safety requirements is unambiguously and consistently identified.

(c) Traceability encompasses all pre-existing software items included in or called from the application source code

(d) Any tools used to support traceability do not corrupt the traceability structures.

(e) Procedures or tools have been used to ensure that any loss of traceability or incorrect traceability is detected and corrected.

Any tools used to construct or maintain traceability, have been verified and validated to an appropriate level for the SW Assurance Level.

[This space is intentionally left blank]

5.8 ESARR 6 - Section 8 – Applicability

8.1 This safety regulatory requirement shall apply to civil and military ATM service providers who have the responsibility for the management of safety in ground-based ATM systems and other supporting services (including CNS) under their managerial control.

ESARR 6, clause 8.1 stresses that both military and civilian systems are within the scope of this regulatory requirement. Military risk assessment requires specific expertise; the causes of hazards vary significantly between civil and military applications. The scope of the regulatory requirement has been extended to recognize that there are significant interactions between military and civil systems. Military exclusions can have a significant impact upon commercial operations. Airspace design and the mechanisms for implementing airspace segregation can themselves constitute hazards. Military systems also often interface with the software that controls civilian flights. It can, therefore, be necessary to propagate assurance levels between integrated software systems in order to ensure that each reaches the appropriate level of safety assurance. When interdependencies exist between two applications at difference assurance levels, ESARR 6 makes it clear that both systems must be developed to the level of rigor associated with the higher of the assurance levels.

In accordance with the set of definitions used by SRC, a provider of ATM service(s) is an organization responsible and authorized to provide service(s) for the purpose of Air Traffic Management. Furthermore, Air Traffic Services are comprised of: Air Traffic Control (i.e. Area Control service, Approach Control Service, Aerodrome Control service, and Air Traffic Advisory Service, Flight Information Service and Alerting Service). In addition, these services can be applied in the 7 types of airspace (A through G) as defined in ICAO Annex 11. All these services and airspaces are therefore within the scope of ESARR 6. Designated authorities should also ensure where necessary that ATM service providers have coordinated the implementation of ESARR 6 with airport services that are not directly part of ATM service provision.

8.2 The software safety assurance system already existing for ATM systems under the direct managerial control of the military ATM organisation can be accepted, provided it accords with the obligatory provisions of ESARR 6.

The acceptability of assurance in these cases is to be decided in accordance with the national institutional arrangements. Depending on the State internal arrangements, the relevant designated authority can be military or civil authority.

8.3 The obligatory provisions of this ESARR shall be enacted as minimum national safety regulatory requirements.

ESARR 6 establishes ‘base line’ requirements. Designated authorities can choose to introduce additional requirements to guide the development and operation of safety related ATM/CNS software by service providers. It is the duty of designated authorities to ensure that safety minima are met both in anticipation of a planned operations and during operations.

Designated authorities and ATM service-providers must work together to implement the requirements of ESARR 6 within their national systems. However, it is important

not to underestimate the importance of international cooperation and exchange in the development of software safety assurance methods. The low frequency of many safety-related software failures creates a need to share information across national boundaries. Similarly, the highly technical nature of validation and verification techniques will create training and competency requirements that can be reinforced by international collaboration via mechanisms such as those provided by EUROCONTROL.

5.9 ESARR 6 - Section 9 – Implementation

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

The core components of ESARR 6 are effective from the 6th November 2006. The provisions do not cover legacy systems, as described in previous sections of this guidance.

5.10 ESARR 6 - Section 10 – Exemptions

None

6. ADDITIONAL GUIDANCE

The EUROCONTROL Recommendations for Air Navigation Systems Software provide a strong rationale for the approach advocated embodied within ESARR 6. These recommendations establish the lifecycle requirements for Air Navigation Systems software within the context of a wider risk assessment process. This document also described how risk assessments can be structured around techniques such as those embodied within the EUROCONTROL Safety Assessment Methodology (SAM). [[See Chapter 1, page 2 of SAF.ET1.ST03.1000]. In addition, the EUROCONTROL Recommendations for Air Navigation Systems Software document provides:

- A recommended definition of ANS software lifecycle by reusing IEC/ISO12207 processes structure,

- Coverage, traceability matrices between three selected standards: ED12B/DO178B, IEC 61508, ISO/IEC 12207 and the recommended ANS software lifecycle,

- Expert feedback on the use of ED12B/DO178B and IEC 61508 safety standards within specific industrial domains.

7. CONCLUSIONS

ESARR 6 describes a set of requirements that designated authorities, or safety regulators, impose upon ATM service providers in order to ensure that the *risks associated with operating ATM software have been reduced to a tolerable level.*

In particular, the safety regulatory requirement describes how Software Safety Assurance Systems must be integrated within wide Safety Management Systems.

It is the responsibility of the designated authority to ensure the adequate safety oversight of the service-provider Software Safety Assurance Systems. In order to do this, ATM service providers must demonstrate and document a systematic approach to:

- The allocation of software assurance levels,
- The validation of software requirements,
- The verification of software requirements,
- The maintenance of software configuration management data,
- The traceability of software requirements.

The designated authority must ensure that the processes used to satisfy these requirements are properly supported throughout a Safety Management System and associated Safety Software Assurance System. ESARR 6 also stipulates that these requirements apply to COTS or non-developmental items in the same way that they apply to bespoke or developmental systems.

[This space is intentionally left blank]

8. APPENDIX A

Glossary – Terms and Definitions

Definitions for specific terms used in this document are given in the EUROCONTROL Safety Regulatory Requirements – Software in ATM Systems (ESARR 6), and repeated for ease of reference in this appendix.

TERM	DEFINITION
Assessment	An evaluation based on engineering, operational judgement and/or analysis methods.
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 Equipment approved for operational use	All engineering systems, facilities or devices that have been used either by airspace users (e.g. ground navigation facilities) directly, or are used in the provision of operational air traffic management services.
ATM Service	A service for the purpose of ATM.
ATM Service-Provider	An organisation responsible and authorised to provide ATM service(s).
ATM Software	Software used in ATM Environment. *See later the definition for software.*
CNS	Communication, Navigation and Surveillance.
Configuration data	Data that configures a generic software system to a particular instance of its use (for example, data that adapts a flight data processing system to a particular airspace, by setting the positions of airways, reporting points, navigation aids, airports and other elements important to air navigation).
Hazard	Any condition, event, or circumstance which could induce an accident.
Independent software components	Those software components which are not rendered inoperative by the same failure condition that causes the hazard.

TERM	DEFINITION
Mitigation or Risk Mitigation	Steps taken to control or prevent a hazard from causing harm and reduce risk to a tolerable or acceptable level.
Operating Software	For the purpose of ESARR 6 it is understood the software used in ATM equipment approved for operational use. *See above the definition for ATM Equipment approved for operational use.*
Risk	The combination of the overall probability, or frequency of occurrence of a harmful effect induced by a hazard and the severity of that effect.
Risk Assessment	Assessment to establish that the achieved or perceived risk is acceptable or tolerable.
Risk Mitigation	See mitigation.
Safety	Freedom from unacceptable risk.
Safety Achievement	The result of processes and/or methods applied to attain acceptable or tolerable safety.
Safety Assurance	All planned and systematic actions necessary to provide adequate confidence that a product, a service, an organisation or a system achieves acceptable or tolerable safety.
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.
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.

TERM	DEFINITION
Software	Computer programs and corresponding configuration data, including non-developmental software (e.g. proprietary software, Commercial Off The Shelf (COTS) software, re-used software, etc.), but excluding electronic items such as application specific integrated circuits, programmable gate arrays or solid-state logic controllers.
Software failure	The inability of a program to perform a required function correctly.
Software life cycle data	Data that is produced during the software life cycle to plan, direct, explain, define, record, or provide evidence of activities. This data enables the software life cycle processes, system or equipment approval and post-approval modification of the software product.
Software Requirements	The specifications, if met, will ensure that ATM software performs safely and according to operational need.
Validation	Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled (usually used for internal validation of the design).
Verification	Confirmation by examination of evidence that a product, process or service fulfils specified requirements.

(PAGE INTENTIONALLY LEFT BLANK)

9. APPENDIX B

Applicability of ESARR 6

The Requirement includes a Section TBD, '*Applicability*' to specify the scope of applicability of its provisions in term of categories of organisations that are subject to the requirements. The scope of ESARR 6 is the same as of ESARR 3 i.e. the Software Safety Assurance System as part of the Safety Management System is to be implemented by those organisations determined in Section TBD. This appendix is intended to provide guidance on these aspects.

B1 Applicability to EUROCONTROL Member States

The Safety Regulation Commission (SRC) is responsible for the development of harmonised safety regulatory objectives and requirements for the ATM System, which will be implemented and enforced by Member States after being approved by EUROCONTROL.

The requirements are known as ESARR (EUROCONTROL Safety Regulatory Requirements). In practical terms, each ESARR is developed by the SRC, approved by the EUROCONTROL Permanent Commission through the Provisional Council, and implemented and enforced by the Member States.

Member States are bound by decisions taken under either the current or revised EUROCONTROL Convention, and consequently have to implement and enforce within their national legal order the safety regulatory requirements contained in such decisions.

This also concerns those ESARR that apply to ATM service-providers and/or Designated Authorities and/or individuals, such as ESARR 3, ESARR 5 and ESARR 6. Member States will have to ensure through appropriate safety oversight that ATM community meets these requirements.

B2 Applicability to ATM providers

ESARR 6 is applicable to all providers of ATM services that fall under the jurisdiction of the national ATM safety regulatory body.

Accordingly, the implementation concerns all organisations providing not only ATS services (encompassing ATC, FIS, and alerting and advisory services), but also other ATM services such as Air Traffic Flow Management (ATFM) and Airspace Management (ASM). That scope is consistent with ICAO and EUROCONTROL definitions for Air Traffic Management.

(Figure B.1 – Applicability of ESARR 6 to ATM Service-Providers)

NOTE: Applicability of ESARR 6 is the same as for ESARR 3.

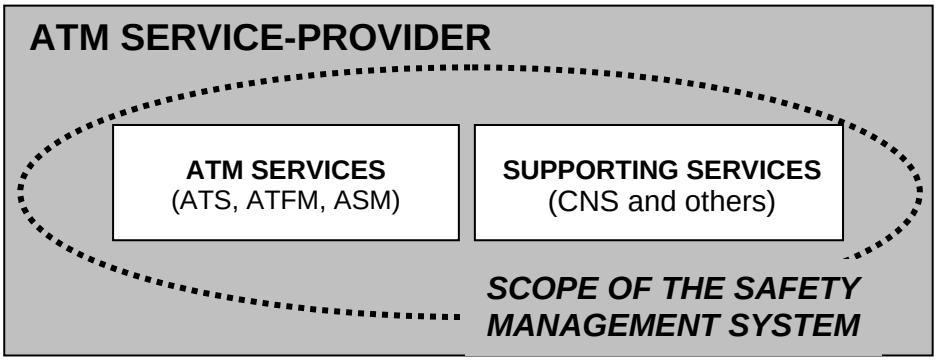
Situations exist where different organisations provide these services separately. Requirements will apply to all of them when those functions uses operational software.

ATM services can be provided simultaneously by different organisations operating within specific geographical regions or having responsibilities for parts of the navigable airspace associated with a flight phase. For instance, we may conceive situations where a national organisation is responsible for en-route ATM, while TWR or AFIS services are delivered by organisations owning local airports. Again, we may say that all those organisations will have to meet ESARR 6 requirements.

B3 Applicability to ATM safety regulators (Designated Authority)

B4 The SMS Scope

The SMS operated by each ATM service-provider will have to cover not only its ATM services, but also any supporting service (including CNS functions and services) which are under the managerial control of the organisation. As such the Software Safety Assurance System should be a distinct component ensuring safety assurances when operating ATM software.



(Figure B.2 – Scope of the SSAS required by ESARR 6)

Supporting services include systems, services and arrangements, including Communication, Navigation and Surveillance services, which support the provision of an ATM service. Any supporting service under the managerial control of the organisation has to be covered by the SSAS.

Supporting services outside the managerial control of the organisation should be considered as external inputs and addressed in accordance with the External Services requirement (ESARR 3, Section 5.2.6).