EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

EUROCONTROL SAFETY REGULATORY REQUIREMENT
(ESARR)

ESARR 6

SOFTWARE IN ATM FUNCTIONAL SYSTEMS

Edition	**:**	**2.0**
Edition Date	**:**	**06 May 2010**
Status	**:**	**Released Issue**
Distribution	**:**	**General Public**
Category	**:**	**Safety Regulatory Requirement**

SAFETY REGULATION COMMISSION

F.2 DOCUMENT CHARACTERISTICS

TITLE		
ESARR 6 – Software in ATM Functional Systems		
Document Identifier	**Reference**	ESARR 6
esarr6_e2.0_ri	**Edition Number**	2.0
	Edition Date	06-05-2010
Abstract		
ESARR 6 deals with the implementation of software safety assurance systems, which ensure that the risks associated with the use of software in safety related ground-based ATM functional systems, are reduced to a tolerable level. EASRR 6 does not prescribe any type of supporting means of compliance for software. This is the role of software assurance standards. It is therefore outside the scope of this requirement to invoke specific national or international software assurance standards 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 use of software in ATM functional systems.		
Keywords		
Risk Assessment	Severity Classification	
Risk Mitigation	Risk Classification	
Hazard identification	Software	
Contact Person(s)	**Tel**	**Unit**
Florin CIORAN	+32 2 729 51 57	DG/SRU

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

COPIES OF SRC DELIVERABLES CAN BE OBTAINED FROM	
Safety Regulation Unit EUROCONTROL Rue de la Fusée, 96 B-1130 Bruxelles	Tel: +32 2 729 51 38 Fax: +32 2 729 47 87 E-mail: sru@eurocontrol.int Website: www.eurocontrol.int/src

F.3 DOCUMENT APPROVAL

EUROPEAN ORGANISATION FOR THE SAFETY OF AIR NAVIGATION

"EUROCONTROL"

- Decisions of the Permanent Commission -

DECISION No. 116

approving the EUROCONTROL Safety Regulatory Requirement – ESARR 6, Edition 2.0 - entitled "Software in ATM Functional Systems"

THE PERMANENT COMMISSION FOR THE SAFETY OF AIR NAVIGATION,

Having regard to the EUROCONTROL International Convention relating to Co-operation for the Safety of Air Navigation, amended by the Protocol signed at Brussels on 12 February 1981, and in particular Articles 1(c), 2.1(j), 6.1 and 7.1 thereof;

Having regard to the Protocol consolidating the EUROCONTROL International Convention relating to Co-operation for the Safety of Air Navigation, which was opened for signature on 27 June 1997, and in particular Article 2.1(R) of the consolidated version of the Convention annexed thereto;

Having regard to Decisions No. 71 and No. 72 of 9 December 1997 on early implementation of certain provisions in the revised Convention, and in particular paragraph 5 of Decision No. 72;

On the proposal of the Provisional Council,

HEREBY TAKES THE FOLLOWING DECISION:

The Commission approves, for incorporation and implementation in ATM regulatory frameworks of EUROCONTROL Contracting Parties, the EUROCONTROL Safety Regulatory Requirement – ESARR 6, Edition 2.0 – entitled "Software in ATM Functional Systems", as attached.

The present Decision will come into effect on the day of its signature.

Done at Brussels on 6.5.2010

G. TONELLI
President of the Commission

F.4 AMENDMENT RECORD

The following table records the complete history of this document.

Edition No.	Date	Reason for Change	Pages Affected
0.01	18-Jan-01	Creation – Working Draft – ASW drafting group activity between November 2000 and January 2001.	All
0.02	05-Mar-01	Intermediate version following ASW DG 2nd meeting.	All
0.03	11-May-01	Follow up of ASW Drafting Group 3rd meeting.	All
0.04	13-Aug-01	Comments received following ASW DG 3 and in preparation for ASW DG 4.	All
0.05	16-Aug-01	Revised Working Draft following ASW DG 4 and re-formatting into new ESARR format.	All
0.06	12-Oct-01	Revised Working Draft following ASW 3rd meeting (October 2001).	Executive Summary, paras 1.1.c), 2.1, 7.1. definition for software life cycle data and independent software components added
0.07	04-Jun-02	Revised Working Draft following ASW 4th meeting (20 May 2002). Note: All notes except Note 1 in Obligatory Provisions moved in EAM 6 / GUI1.	A ii), A iii), C i), 1.1.b, 1.2. new 1.3, 2.1, 2.2, 2.3, new 2.5. (former 3.4) 3.1, 3.2, 3.4 - deleted, 4.3, 4.4, 5.4. Appendix A Glossary – Terms & Definitions
0.08	26-Jun-02	Consolidated review via correspondence following ASW 4 meeting.	Deletion of all Notes and transfer them into EAM6. 1.1.e), new 1.2.b). new 1.4, 2.4, 3.3.
0.09	03-Jul-02	Work review carried out by the ASW group during ASW 5 meeting.	All
0.10	05-Jul-02	SRU review after ASW 5 meeting: • indication of minimum requirements, • inclusion of DA into applicability section, • clarification of the applicability in ground-based ATM systems, • editorials.	Applicability Section. Headings of sections 2,3,4,5,6,7. Scope A i)
0.11	16-Sep-02	Comments received in preparation of ASW 6 meeting.	1.2.e, 1.3, 2.3

Edition No.	Date	Reason for Change	Pages Affected
0.12	01-Oct-02	Review during ASW 6 meeting and creation of the first Draft Issue.	A i), A ii), B ii), B iii), B iv), B v), Foot note in C i). 1.1, 1.2.a), 1.2.d), 1.2.e), 1.4. moved in ESARR 1, 2.1, 3.2,7.2, former 8.2 deleted, old 8.3 is the new 8.2, Glossary – new def. Cutover and Supporting Services and review of safety req. definition
0.1	27-Oct-02	Document status amended to draft version 0.1. Updated document format.	All
0.2	25-Mar-03	Document status amended to draft version 0.2 following SRC consultation and in preparation for EURCONTROL wide consultation. Starting with Ed 0.2 a Comment Response Document is ensuring the transparency and traceability between editions.	Change in accessibility distribution, Former 8.2 became 8.3, new 8.2, Safety Objective, para 3.1, 4.1. New section 11 Definitions.
0.3	04-Aug-03	Version updated following the EUROCONTROL wide consultation phase.	Abstract, Executive Summary, A. i, A. iii, B. v, C, 1.1, 1.2.a, 1.2.d, 1.2.e, 2.3, 2.4, 4.1.8.1, 8.2, 11 Appendix A.
0.4	12-Aug-03	SRU quality check.	All
0.5	11-Sep-03	Consolidated version for PC submission following final review consultation (RFC 0348)	3.1. Appendix A
0.6	30-Sep-03	SRC18 (7-8.10.2003) approval for submission to PC and EUROCONTROL Permanent Commission	Appendix A
1.0	06-Nov-03	Document adopted by the Provisional Council at their 18th session and approved by the Permanent Commission at their ad-hoc session held on 6th November 2003.	All
1.01	01-Dec-09	Document re-drafted to take into consideration the DRAHG recommendations on the alignment of ESARRs with EC text. Document submitted to SRCCG for discussion.	All
1.1	15-Jan-10	Document updated following SRCCG consultation (RFC No. 0915).	Attachment A (Articles 1, 2 & 5)
1.2	23-Feb-10	Document updated following SRC consultation (RFC No. 1001).	-
1.3	31-Mar-10	Document updated following EUROCONTROL-wide consultation (RFC No. 1002).	New paragraph A13 & Attachment A (Article 2)
2.0	06-May-10	Document adopted/approved at PC33.	-

F.5 CONTENTS

(Space Left Intentionally Blank)

F.6 EXECUTIVE SUMMARY

This EUROCONTROL Safety Regulatory Requirement (ESARR) has been prepared by the Safety Regulation Commission.

ESARR 6 deals with the implementation of software safety assurance systems to ensure that the risks associated with the use of software in safety-related ground-based ATM functional systems are reduced to a tolerable level.

The purpose of this ESARR is therefore to provide a set of harmonised safety regulatory requirements for the use of software in ATM functional systems. It does not identify any software assurance standard as an acceptable means of compliance to meet its mandatory provisions. It is accordingly outside the scope of this ESARR to invoke specific national or international software assurance standards

Pursuant to Regulation (EC) No. 550/2004, the European Commission shall identify and adopt the ESARRs that shall be made mandatory under Community law. Accordingly, Commission Regulation (EC) No. 482/2008 was developed to transpose the provisions of ESARR 6, Edition 1.0, into Community law.

The EUROCONTROL Provisional Council and the Single Sky Committee (SSC) recognised the need to ensure an identical text between the ESARR safety requirements and their corresponding EC legislation and agreed on the recommendations of the joint SRC/EC Double Regulation Ad-Hoc Group's (DRAHG) 'Report on the Resolution of Double ATM Safety Regulation in Single European Sky States', dated 23 November 2007. Following the successful application of the DRAHG recommendations to ESARR 1 and its approval by the EUROCONTROL Provisional Council, the same approach is used to initiate the application of the DRAHG recommendations to ESARR 6 and developed a proposal for the amendment of ESARR 6, Edition 1.0.

According to those recommendations, the proposed amendment is exclusively intended to adopt the text of the rules transposing the relevant safety requirements into Community law, whilst maintaining the existing ESARR 6-related obligations on EUROCONTROL Contracting Parties and the scope of those obligations.

Being that the two texts are equivalent, their full alignment does not modify the previously agreed requirements. Nevertheless, the amendment brings the benefit of removing potential double regulation issues with regard to the use of software in ATM functional systems in EUROCONTROL Member States where EC regulations are directly applicable. It also provides a platform to take advantage of the synergies between the EC and EUROCONTROL frameworks and support the implementation of SES across the ECAC region. In particular, ESARR 6 provides the means to ensure the implementation of an appropriate software safety assurance systems in EUROCONTROL Member States and facilitates implementation in the military domain. This requirement also supports such implementation in those ECAC States outside the scope of both organisations.

The obligations of the EUROCONTROL Member States where EC law is not directly applicable will not be automatically modified by the amendment of the EC rules referred to in Commission Regulation (EC) No. 482/2008. Nevertheless, the amendments introduced by the second package of single European sky legislation have already been taken into consideration in the ESARR 6 text approved by the EUROCONTROL Permanent Commission in May 2010.

INTRODUCTORY MATERIAL

*The provisions in this section are **not** mandatory*

A. RATIONALE

A.1 SRC Decision 6/8/5 approved the inclusion of the development of an EUROCONTROL Safety Regulatory Requirement for software-based ATM functional systems in the SRC Work Programme. At the time, it was recognised that no precedent existed in this area within ICAO Standards and Recommended Practices

A.2 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 functional system are assessed for their significance and that all ATM functional system functions are classified according to their severity. It also requires the assurance of appropriate mitigation of risks where assessment has shown this to be necessary due to the significance of the change.

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 the ATM functional system in terms of people, procedures and equipment (software and hardware) and their interactions when introducing and/or planning changes to the ATM functional system

A.3 ESARR 6 is the continuation of this safety regulatory development process and expands ESARR 4 in regard to the software aspects of ATM functional systems. Complementary safety regulatory requirements for hardware aspects are under consideration.

A.4 Safety is an essential characteristic of ATM functional systems. It has a dominant impact upon operational effectiveness. ATM functional systems, now involving significant interactions in a continuously larger integrated environment, automation of operational functions formerly performed through manual procedures, increases in complexity, and the massive and systematic use of software, are demanding a more formal approach to the achievement of safety.

A.5 The purpose of this ESARR is to provide ATM safety regulatory bodies and ATM service providers with a uniform and harmonised set of safety regulatory requirements for the use of software in ATM functional systems.

(Space Left Intentionally Blank)

A.6 As part of the Single European Sky (SES) initiative, a generic framework for the regulation of ATM in the European Union (EU) has been established through the adoption by the Council of Ministers and the European Parliament of Regulation (EC) No. 549/2004 (the Framework Regulation), Regulation (EC) No. 550/2004 (the Service Provision Regulation), Regulation (EC) No. 551/2004 (the Airspace Regulation) and Regulation (EC) No. 552/2004 (the Interoperability Regulation).

A.7 Pursuant to Regulation (EC) No. 550/2004, the European Commission shall identify and adopt the EUROCONTROL ESARRs and subsequent amendments to those requirements that shall be made mandatory under Community law.

A.8 Commission Regulation (EC) No. 2096/2005 laying down common requirements for the provision of air navigation services" was developed to transpose the provisions of ESARRs 3 and 4 into Community law. Annex II to Commission Regulation (EC) No. 2096/2005 requires providers of air traffic services to implement a safety management system as well as safety requirements for risk assessment and mitigation with regard to changes.

A.9 In addition, Commission Regulation (EC) No. 482/2008 was developed to transpose the provisions of ESARR 6, Edition 1.0, into Community law.

A.10 Following the successful application of the DRAHG recommendations to ESARR 1 and its approval by the EUROCONTROL Provisional Council, the same approach is used to initiate the application of the DRAHG recommendations to ESARR 6.

A.11 According to the recommendations of DRAHG, such an amendment should be exclusively intended to adopt the text of the rules transposing the relevant safety requirements into Community law while maintaining the existing ESARR 6 related obligations on the EUROCONTROL Contracting Parties and the scope of those obligations.

A.12 The result of this alignment is that the text of the safety requirements in Section 3 has been entirely replaced by the relevant Community text. The relevant provisions of Commission Regulation (EC) No. 482/2008 are therefore adopted and presented in Attachment A to this Requirement. The only modifications introduced are related to the references to other provisions included in Commission Regulation (EC) No. 482/2008. In particular, the expression 'relevant requirements' has been introduced wherever EC rules were referenced. The exact meaning of that expression is provided in Attachment B for each article concerned, establishing its correspondence with the EC references which are exclusively valid in the EUROCONTROL Member States where EC legislation is applicable.

A.13 As per the DRAHG Recommendations, the applicability of this amendment of ESARR 6 has not changed. This safety regulatory requirement applies to civil ATM service providers who have the responsibility for the management of safety in ground-based ATM systems and other ground-based supporting services (including CNS) under their managerial control. This safety regulatory requirement applies also to military ATM service providers whenever providing services to GAT.

ESARR 6 supports the implementation of the SES by enabling joint civil/military initiatives with regard to software in ATM functional systems in accordance with the existing regulatory framework. For example, in mixed ATM operational rooms shared by military and civil ATC providers, where software is applied in ATM systems sharing the same data processing, the requirements of this ESARR are to be assured through specific agreements by both the civil and military organisations.

A.14 Being that the two texts are equivalent, their full alignment does not modify the previously agreed requirements. Nevertheless, the amendment brings the benefit of removing potential double-regulation issues with regard to the use of software in ATM functional systems in EUROCONTROL Member States where EC regulations are directly applicable. It also provides a platform to take advantage of the synergies between the EC and EUROCONTROL frameworks and support the implementation of SES across the ECAC region. In particular, ESARR 6 provides the means to ensure the implementation of an appropriate software safety assurance systems in EUROCONTROL Member States. This requirement also supports such implementation in those ECAC States outside the scope of both organisations.

A.15 In that regard, it should be noted that the National Supervisory Authority (NSA) function denotes an existing supervisory task which applies to the competent authorities of any State that has accepted the responsibility for regulating and providing air navigation service functions over its territory and associated areas, and that, consequently, the term ‘National Supervisory Authority’ used in the context of ESARR 6 is not limited to EU Member States.

A.16 ESARR 6, Edition 1.0, became effective in November 2006 for all EUROCONTROL Member States. Commission Regulation (EC) No. 482/2008 became effective as of 1 January 2009 to the new software of EATMN systems and as of 1 July 2010 to any changes to the software of EATMN systems. Taking into consideration the alignment of both texts and that no new obligations have been introduced by means of this new edition of ESARR 6, the applicability date does not need to be extended beyond the date of its original approval by the EUROCONTROL Permanent Commission. The requirements will already be implemented in Member States either by means of Commission Regulation (EC) No. 482/2008, or national provisions wherever EC legislation is not applicable.

A.17 As explained in A.12 above, this Requirement has been drafted in a manner which ensures that the obligations of the EUROCONTROL Member States where EC law is not directly applicable are not automatically modified by the amendment of the EC rules referred to in Commission Regulation (EC) No. 482/2008. Further amendments to those EC rules will require a review of ESARR 6 to ensure consistency between both texts. Nevertheless, the amendments to Regulation (EC) No. 549/2004 and Regulation (EC) No. 550/2004 adopted in the second package of Single European Sky legislation have already been taken into consideration in the text of ESARR 6 as approved by the EUROCONTROL Permanent Commission in May 2010.

B. OBJECTIVES

B.1 The objectives of ESARR 6 are to:

a) The prime software safety objective to be met for ATM functional systems that contain software is to ensure that the risks associated with the use of EATMN software have been reduced to a tolerable level.

b) Ensure the applicability of the ESARR 6 requirements to general air traffic in the Member States of EUROCONTROL;

c) Support implementation in other ECAC States;

d) Support the implementation of the SES by:

i) Allowing the development and implementation of software safety assurance systems within the framework of the safety management system of the ATM service providers defined in the SES regulations,

ii) Enabling joint civil/military initiatives with regard to software in ATM functional systems in accordance with the existing regulatory framework.

(Space Left Intentionally Blank)

MANDATORY PROVISIONS

1. DEFINITIONS

1.1 For the purpose of this requirement, applicable definitions are included in Attachments A and B.

2. APPLICABILITY

2.1 This requirement shall apply to all EUROCONTROL Contracting Parties with regards to the operation of their ATM service providers involved in the provision of Air Traffic Services (ATS), Air Traffic Flow Management (ATFM) and Airspace Management (ASM) to General Air Traffic (GAT).

2.2 The provisions of this requirement become effective on the day of its approval by the EUROCONTROL Permanent Commission.

3. SAFETY REQUIREMENTS

3.1 For the purpose of this Requirement, all applicable provisions are included in Attachment A.

(Space Left Intentionally Blank)

ATTACHMENT A

Article 1
Subject matter and scope

1. This Requirement lays down the requirements for the definition and implementation of a software safety assurance system by air traffic service (ATS) providers, entities providing air traffic flow management (ATFM) and air space management (ASM) for general air traffic and other ground-based supporting services (including CNS) under their managerial control.

2. This Requirement shall apply to the new software and to any changes to the software of the systems for ATS, ASM, ATFM and other ground-based supporting services (including CNS) under their managerial control. It shall not apply to the software of airborne constituents and to space-based equipment.

Article 2
Definitions

For the purposes of this Requirement, the following definitions shall apply:

1. ‘accuracy’ means the required precision of the computed results;

2. ‘achieved with independence’ means, for software verification process activities, that the verification process activities are performed by a person(s) other than the developer of the item being verified;

3. ‘air traffic flow management (ATFM)’ means a function established with the objective of contributing to a safe, orderly and expeditious flow of air traffic by ensuring that ATC capacity is utilised to the maximum extent possible, and that the traffic volume is compatible with the capacities declared by the appropriate air traffic service providers;

4. ‘air traffic management (ATM)’ means the aggregation of the airborne and ground-based functions (air traffic services, airspace management and air traffic flow management) required to ensure the safe and efficient movement of aircraft during all phases of operations;

5. ‘air traffic services (ATS)’ means the various flight information services, alerting services, air traffic advisory services and ATC services (area, approach and aerodrome control services);

6. ‘airspace management (ASM)’ means a planning function with the primary objective of maximising the utilisation of available airspace by dynamic time-sharing and, at times, the segregation of airspace among various categories of airspace users on the basis of short-term needs;

7. ‘CNS’ means communication, navigation and surveillance

8. ‘configuration data’ means data that configures a generic software system to a particular instance of its use;

9. "constituents" means tangible objects such as hardware and intangible objects such as software upon which the interoperability of the EATMN depends;

10. ‘correct and complete EATMN software verification’ means all software safety requirements which 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;

11. ‘COTS’ means a commercial available application sold by vendors through public catalogue listings and not intended to be customised or enhanced;

12. ‘cutover or hot swapping’ means the approach of replacing European air traffic management network (EATMN) system components or software while the system is operational;

13. ‘European air traffic management network (EATMN)’ means the collection of:

    (a) Systems and procedures for airspace management.

    (b) Systems and procedures for air traffic flow management.

    (c) Systems and procedures for air traffic services, in particular flight data processing systems, surveillance data processing systems and human-machine interface systems.

    (d) Communications systems and procedures for ground-to-ground, air-to-ground and air-to-air communications.

    (e) Navigation systems and procedures.

    (f) Surveillance systems and procedures

    (g) Systems and procedures for aeronautical information services.

    (h) Systems and procedures for the use of meteorological information.

14. ‘EATMN software’ means software used in the EATMN systems referred to in Article 1;

15. ‘functional system’ means a combination of systems, procedures and human resources organised to perform a function within the context of ATM;

16. ‘hazard’ means any condition, event, or circumstance which could induce an accident;

17. ‘general air traffic (GAT)’ means all movements of civil aircraft, as well as all movements of State aircraft (including military, customs and police aircraft) when these movements are carried out in conformity with the procedures of the ICAO;

18. ‘independent software components’ means those software components which are not rendered inoperative by the same failure condition that causes the hazard;

19. ‘new software’ means a software that has been ordered or for which binding contracts have been signed after the entry into force of Edition 1.0 of this Requirement;

20. ‘non-developmental software’ means a software not developed for the current contract;

21. ‘organisation’ means either an ATS provider, a CNS provider or an entity providing ATFM or ASM;

22. ‘overload tolerance’ means the behaviour of the system in the event of, and in particular its tolerance to, inputs occurring at a greater rate than expected during normal operation of the system;

23. ‘requirements validity’ means the confirmation by examination and provision of objective evidence that the particular requirements for a specific use are as intended;

24. ‘risk’ means the combination of the overall probability, or frequency of occurrence of a harmful effect induced by a hazard and the severity of that effect;

25. ‘safety assurance’ means all planned and systematic actions necessary to provide adequate confidence that a product, a service, an organisation or a functional system achieves acceptable or tolerable safety;

26. ‘safety objective’ means a qualitative or quantitative statement that defines the maximum frequency or probability at which a hazard can be expected to occur;

27. ‘safety requirement’ means a risk-mitigation means, defined from the risk-mitigation strategy that achieves a particular safety objective, including organisational, operational, procedural, functional, performance, and interoperability requirements or environment characteristics;

28. ‘software’ means computer programmes and corresponding configuration data, including non-developmental software, but excluding electronic items, namely application specific integrated circuits, programmable gate arrays or solid-state logic controllers;

29. ‘software capacity’ means the ability of the software to handle a given amount of data flow;

30. ‘software components’ means a building block that can be fitted or connected together with other reusable blocks of software to combine and create a custom software application;

31. ‘software failure’ means the inability of a programme to perform a required function;

32. ‘software life cycle’ means:

    (a) an ordered collection of processes determined by an organisation to be sufficient and adequate to produce a software product;

    (b) the period of the time that begins with the decision to produce or modify a software product and ends when the product is retired from service;

33. ‘software life cycle data’ means the 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;

34. ‘software malfunction’ means the inability of a programme to perform a required function correctly;

35. ‘software resource usage’ means the amount of resources within the computer system that can be used by the application software;

36. ‘software robustness’ means the behaviour of the software in the event of unexpected inputs, hardware faults and power supply interruptions, either in the computer system itself or in connected devices;

37. ‘software safety requirement’ means a description of what is to be produced by the software given the inputs and constraints, and if met, ensures that EATMN software performs safely and according to operational need;

38. ‘software timing performances’ means the time allowed for the software to respond to given inputs or to periodic events, and/or the performance of the software in terms of transactions or messages handled per unit time;

39. ‘system’ means the aggregation of airborne and ground-based constituents, as well as space-based equipment, that provides support for air navigation services for all phases of flight;

40. ‘system safety requirement’ means a safety requirement derived for a functional system.

Article 3
General safety requirements

1. Whenever an organisation is required to implement a risk assessment and mitigation process in accordance with applicable Community or national law, it shall define and implement a software safety assurance system to deal specifically with EATMN software related aspects, including all on-line software operational changes, and in particular cutover or hot swapping.

2. The organisation shall ensure, as a minimum, that its software safety assurance system produces evidence and arguments that demonstrate the following:

    (a) the software safety requirements correctly state what is required by 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 safety requirements;

    (c) the software implementation contains no functions which adversely affect safety;

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

    (e) assurances are provided confirming that the general safety requirements set out in points (a) to (d) are satisfied, and the arguments that demonstrate the required assurances are at all times derived from:

        (i) a known executable version of the software;

        (ii) a known range of configuration data;

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

3. The organisation shall make available the required assurances, to the national supervisory authority, demonstrating that the requirements provided for in paragraph 2 have been satisfied.

Article 4
Requirements applying to the software safety assurance system

The organisation shall ensure, as a minimum, that the software safety assurance system:

1. Is documented, specifically as part of the overall risk assessment and mitigation documentation;

2. Allocates software assurance levels to all operational EATMN software in compliance with the requirements set out in Annex I;

3. Includes assurances of:

    (a) software safety requirements validity in compliance with the requirements set out in Annex II, Part A;

    (b) software verification in compliance with the requirements set out in Annex II, Part B;

(c) software configuration management in compliance with the requirements set out in Annex II, Part C;

(d) software safety requirements traceability in compliance with the requirements set out in Annex II, Part D;

4. Determines the rigour to which the assurances are established; the rigour must be defined for each software assurance level, and increase as the software increases in criticality; for that purpose:

(a) the variation in rigour of the assurances per software assurance level must include the following criteria:

(i) required to be achieved with independence;

(ii) required to be achieved;

(iii) not required;

(b) the assurances corresponding to each software assurance level must give sufficient confidence that the EATMN software can be operated tolerably safely;

5. Uses feedback of EATMN software experience to confirm that the software safety assurance system and the assignment of assurance levels are appropriate. For that purpose, the effects from a software malfunction or failure reported according to the applicable requirements on reporting and assessment of safety occurrences shall be assessed in comparison with the effects identified for the system concerned as per the severity classification scheme established in the relevant requirements.

Article 5
Requirements applying to changes to software and to specific software

1. For any changes to the software or for specific types of software such as COTS, non-developmental software or previously used software for which some of the requirements of Article 3(2)(d) or (e) or of Article 4(2), (3), (4) or (5) cannot be applied, the organisation shall ensure that the software safety assurance system provides, through other means chosen and agreed with the national supervisory authority, the same level of confidence as the relevant software assurance level whenever defined.

Those means must give sufficient confidence that the software meets the safety objectives and requirements, as identified by the safety risk assessment and mitigation process.

2. In the assessment of the means referred to in paragraph 1, the national supervisory authority may use a qualified entity or notified body.

(Space Left Intentionally Blank)

ANNEX I

Requirements applying to the software assurance level referred to in Article 4(2)

1. The software assurance level shall relate the rigour of the software assurances to the criticality of EATMN software by using the severity classification scheme set out in the relevant requirements combined with the likelihood of the occurrence of a certain adverse effect. A minimum of four software assurance levels shall be identified, with software assurance level 1 indicating the most critical level.

2. An allocated software assurance level shall be commensurate with the most severe effect that software malfunctions or failures may cause, as referred to in the relevant requirements. This shall, in particular, take into account the risks associated with software malfunctions or failures and the architectural and/or procedural defences identified.

3. EATMN 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.

ANNEX II

Part A: Requirements applying to the software safety requirements validity assurance referred to in Article 4(3)(a)

1. Software safety requirements shall specify the functional behaviour in nominal and downgraded modes, of the EATMN software, timing performances, capacity, accuracy, software resource usage on the target hardware, robustness to abnormal operating conditions and overload tolerance, as appropriate.

2. Software safety requirements shall be complete and correct, and compliant with the system safety requirements.

Part B: Requirements applying to the software verification assurance referred to in Article 4(3)(b)

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

2. The EATMN software shall be adequately verified by analysis and/or testing and/or equivalent means, as agreed with the national supervisory authority.

3. The verification of the EATMN software shall be correct and complete.

Part C: Requirements applying to the software configuration management assurances referred to in Article 4(3)(c)

1. Configuration identification, traceability and status accounting shall exist such that the software life cycle data can be shown to be under configuration control throughout the EATMN software life cycle.

2. Problem reporting, tracking and corrective actions shall exist such that safety related problems associated with the software can be shown to have been mitigated.

3. Retrieval and release procedures shall exist such that the software life cycle data can be regenerated and delivered throughout the EATMN software life cycle.

Part D: Requirements applying to the software safety requirements traceability assurances referred to in Article 4(3)(d)

1. Each software safety requirement shall be traced to the same level of design at which its satisfaction is demonstrated.

2. Each software safety requirement, at each level in the design at which its satisfaction is demonstrated, shall be traced to a system safety requirement.

(Space Left Intentionally Blank)

ATTACHMENT B

B.1 For the purpose of this Requirement, 'relevant requirements' mean:

Article in Attachment A	In general	Wherever EC law is directly applicable
In Article 4, Point 5	ESARR 4 Appendix A.	Section 3.2.4 of Annex II to Commission Regulation (EC) No. 2096/2005 of 20 December 2005, published in The Official Journal of the European Union L 335/13 on 21.12.2005.
In Annex I, point 1	ESARR 4 Appendix A.	Section 4 of point 3.2.4 of Annex II to Commission Regulation (EC) No. 2096/2005 of 20 December 2005, published in The Official Journal of the European Union L 335/13 on 21.12.2005.
In Annex I, point 2	ESARR 4 Appendix A.	Section 4 of point 3.2.4 of Annex II to Commission Regulation (EC) No. 2096/2005 of 20 December 2005, published in The Official Journal of the European Union L 335/13 on 21.12.2005.

(***)