EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

EUROCONTROL SAFETY REGULATORY REQUIREMENT
(ESARR)

ESARR 6

SOFTWARE IN ATM SYSTEMS

Edition	:	**1.0**
Edition Date	:	**06 November 2003**
Status	:	**Released Issue**
Distribution	:	**General Public**
Category	:	**Safety Regulatory Requirement**

SAFETY REGULATION COMMISSION

F.2 DOCUMENT CHARACTERISTICS

TITLE		
ESARR 6 **Software in ATM Systems**		
Document Identifier :	**Reference :**	ESARR 6
esarr6_e10_ri	**Edition Number :**	1.0
	Edition Date :	06-11-2003

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 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 systems.

Keywords :		
Risk Assessment	Hazard identification	Risk Classification
Risk Mitigation	Severity Classification	Software

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

EUROPEAN ORGANISATION FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

- Decisions of the Permanent Commission -

DECISION No 100

approving the EUROCONTROL Safety Regulatory Requirement - ESARR 6 - entitled "Software in ATM 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(i) 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 national ATM regulatory frameworks of EUROCONTROL Member States, the EUROCONTROL Safety Regulatory Requirement - ESARR 6 - entitled "Software in ATM Systems", as developed by the Safety Regulation Commission.

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

Done at Brussels on 06.11.2003

J. TURECKY
President of the Commission

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	18/01/01	Creation – Working Draft – ASW drafting group activity between November 2000 – January 2001.	All
0.02	05/03/01	Intermediate version following ASW DG 2nd meeting.	All
0.03	11/05/01	Follow up of ASW Drafting Group 3rd meeting.	All
0.04	13/08/01	Comments received following ASW DG 3 and in preparation for ASW DG 4.	All
0.05	16/08/01	Revised Working Draft following ASW DG 4 and re-formatting into new ESARR format.	All
0.06	12/10/01	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	04/06/02	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

EDITION NUMBER	EDITION DATE	REASON FOR CHANGE	PAGES AFFECTED
0.08	26/06/02	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	03/07/02	Work review carried out by the ASW group during ASW 5 meeting.	All
0.10	05/07/02	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	16/09/02	Comments received in preparation of ASW 6 meeting.	1.2.e, 1.3, 2.3
0.12	01/10/02	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

EDITION NUMBER	EDITION DATE	REASON FOR CHANGE	PAGES AFFECTED
0.1	27/10/02	Document status amended to draft version 0.1. Updated document format.	All
0.2	25/03/03	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	04/08/03	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	12/08/03	SRU quality check.	All
0.5	11/09/03	Consolidated version for PC submission following final review consultation (RFC 0348)	3.1. Appendix A
0.6	30/09/03	SRC18 (7-8.10.2003) approval for submission to PC and EUROCONTROL Permanent Commission	Appendix A
1.0	06/11/03	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

F.5 CONTENTS

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 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 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

The provisions of this ESARR are to become effective within three years from the date of its approval by the EUROCONTROL Permanent Commission.

(Space Left Intentionally Blank)

INTRODUCTORY MATERIAL

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

A. SCOPE

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 all on-line software operational changes (such as cutover / hot swapping).

ii. The scope of ESARR 6 is confined to the ground component of ATM, and to ground-based supporting services, including CNS systems, under the managerial control of the ATM service-provider. ESARR 6 cannot be applied, unless modified and adequately assessed, to the airborne or space component of ATM systems.

iii. The provisions of this safety regulatory requirement have been developed on the basis that an *a priori* effective 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.

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 accordingly outside the scope of this requirement to invoke specific national or international software assurance standards.

B. RATIONALE

i. SRC Decision 6/8/5 approved the inclusion of the development of an EUROCONTROL Safety Regulatory Requirement for software-based ATM 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.

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 that all ATM 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.

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

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

v. Safety is an essential characteristic of ATM systems. It has a dominant impact upon operational effectiveness. ATM 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.

vi. 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 systems.

C. SAFETY OBJECTIVE

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

(Space Left Intentionally Blank)

MANDATORY PROVISIONS

1. GENERAL SAFETY REQUIREMENTS

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).

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 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 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 General Safety Requirements are satisfied, and the arguments to demonstrate the required assurance are at all times derived from: -

i. a known executable version of the software,

ii. a known range of configuration data, and

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

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.

2 REQUIREMENTS APPLYING TO THE SOFTWARE SAFETY ASSURANCE SYSTEM

The ATM service-provider shall ensure, as a minimum, that the Software Safety Assurance System:

2.1 Is documented, specifically as part of the overall Risk Assessment and Mitigation Documentation.

2.2 Allocates software assurance levels to all operational ATM software.

2.3 Includes assurances of:

a) software requirements validity,

b) software verification,

c) software configuration management, and

d) software requirements traceability.

2.4 Determines the rigour to which the assurances are established. The rigour shall be defined for each 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:

i. required to be achieved with independence,

ii. required to be achieved,

iii. not required,

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

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

2.6 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. COTS - commercial off-the-shelf software, etc) with the same software assurance level.

3. REQUIREMENTS APPLYING TO THE SOFTWARE ASSURANCE LEVEL

The ATM service-provider shall ensure, as a minimum, within the Software Safety Assurance System, that:

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.

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.

3.3 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.

4. REQUIREMENTS APPLYING TO THE SOFTWARE REQUIREMENTS VALIDITY ASSURANCES

The ATM service-provider shall ensure, as a minimum within the Software Safety Assurance System, that software requirements:

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.

4.2 Are complete and correct, and are also compliant with the system safety requirements.

5. REQUIREMENTS APPLYING TO THE SOFTWARE VERIFICATION ASSURANCES

The ATM service-provider shall ensure, as a minimum, within the Software Safety Assurance System, that:

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.

5.2 The ATM software is adequately verified by analysis and/or testing and/or equivalent means, as agreed with Designated Authority.

5.3 The verification of the ATM software is correct and complete.

6. REQUIREMENTS APPLYING TO THE SOFTWARE CONFIGURATION MANAGEMENT ASSURANCES

The ATM service-provider shall ensure, as a minimum, within the Software Safety Assurance System, that:

6.1 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.

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

6.3 Retrieval and release procedures exist such that the software life cycle data can be regenerated and delivered throughout the ATM software life cycle.

7. REQUIREMENTS APPLYING TO THE SOFTWARE REQUIREMENTS TRACEABILITY ASSURANCES

The ATM service-provider shall ensure, as a minimum, within the Software Safety Assurance System, that:

7.1 Each software requirement is traced to the same level of design at which its satisfaction is demonstrated.

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

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 ground-based supporting services (including CNS) under their managerial control.

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.

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

9. IMPLEMENTATION

9.1 The provisions of ESARR 6 are to become effective within three years from the date of its approval by the EUROCONTROL Commission.

10. EXEMPTIONS

None.

11. DEFINITIONS

11.1 Use of the terms and definitions listed in Appendix A shall be considered mandatory.

(Space Left Intentionally Blank)

APPENDIX A

Glossary – Terms and Definitions

TERM	DEFINITION
Accuracy	The required precision of the computed results.
Achieved with independence	See definition for independence
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.*
ATM System	A part of ANS system composed of a ground based ATM component and an airborne ATM component.
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).
Correct and Complete ATM Software Verification	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.

TERM	DEFINITION
Cutover (Hot Swapping)	The approach of replacing CNS/ATM system components or software while the system is operational.
Hazard	Any condition, event, or circumstance which could induce an accident.
Independence	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.
Independent Software Components	Those software components which are not rendered inoperative by the same failure condition that causes the hazard.
Mitigation or Risk Mitigation	Steps taken to control or prevent a hazard from causing harm and reduce risk to a tolerable or acceptable level.
Non-Developmental Item – NDI (Software)	An item (software) not developed for the current contract. Note: This is equivalent to the previously developed software definition in DO-178B/ED-12B. It can be considered as a COTS
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.*
Overload Tolerance	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.
Resource Usage	The amount of resources within the computer system that can be used by the application software. *Note: Resources may include main memory of various categories (such as static data, stack and heap), disc space and communications bandwidth, and may include internal software resources, such as the number of files which may be simultaneously open.*
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.

TERM	DEFINITION
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.
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 Capacity	The ability of the software to handle a given amount of data flow.
Software Components	A component can be seen as a building block that can be fitted or connected together with other reusable blocks of software to combine and create a custom software application.
Software Failure	The inability of a program to perform a required function correctly.
Software Life Cycle	(1) An ordered collection of processes determined by an organisation to be sufficient and adequate to produce a software product. (2) 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.

TERM	DEFINITION
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 Requirement	A description of what is to be produced by the software given the inputs and constraints, and if met, will ensure that ATM software performs safely and according to operational need.
Software Robustness	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.
Software Safety Integrity	Measures that signifies the likelihood of the software in achieving its function under all stated conditions within a stated period of time.
Software Timing Performances	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.
Supporting Services	Systems, services and arrangements, including Communication, Navigation and Surveillance services, which support the provision of an ATM service.
System Requirement	Safety Requirement derived for a System as per ESARR 4.
Safety Requirement (as per ESARR 4)	A risk mitigation means, defined from the risk mitigation strategy, that achieves a particular safety objective. Safety requirements may take various forms, including organisational, operational, procedural, functional, performance, and interoperability requirements or environment characteristics.

Safety Objective (as per ESARR 4)	A safety objective is a planned safety goal. The achievement of an objective may be demonstrated by appropriate means to be determined in agreement with the safety regulator. More specifically for ESARR 4 and therefore for ESARR 6 as well, a safety objective is a qualitative or quantitative statement that defines the maximum frequency or probability at which a hazard can be expected to occur.

TERM	**DEFINITION**
Requirements Validity	Confirmation by examination and provision of objective evidence that the particular requirements for a specific use are as intended.
Verification	Confirmation by examination of evidence that a product, process or service fulfils specified requirements.

(***)