EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

ESARR ADVISORY MATERIAL / ACCEPTABLE MEANS OF COMPLIANCE
(EAM/AMC)

EAM 4 / AMC

ACCEPTABLE MEANS OF COMPLIANCE WITH ESARR 4

Edition	:	**4.0**
Edition Date	:	**26 October 2009**
Status	:	**Released Issue**
Distribution	:	**General Public**
Category	:	**ESARR Advisory Material**

SAFETY REGULATION COMMISSION

F.2 DOCUMENT CHARACTERISTICS

TITLE		
EAM 4 / AMC **Acceptable Means of Compliance with ESARR 4**		
Document Identifier	**Reference**	EAM 4 / AMC
eam4amc_e4.0_ri_web	**Edition Number**	4.0
	Edition Date	26-10-2009
Abstract		
This document has been produced by the Safety Regulation Commission. It presents the acceptable means of compliance (AMC) recognised by the SRC as possible harmonised ways to meet ESARR 4 provisions within the ECAC region. This document will include a Statement of Compliance for each means of compliance recognised by SRC as an AMC to meet ESARR 4 provisions. The Statement of Compliance defines the SRC's position about the acceptability of the AMC, and identifies the scope, terms and conditions under which that acceptability applies.		
Keywords		
Statement of Compliance Acceptable Means of Compliance (AMC)	Safety Regulation Commission (SRC) EUROCONTROL Safety Regulatory Requirement (ESARR)	
Contact Person(s)	**Tel No**	**Unit**
Françoise GIRARD	+32 2 729 51 65	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

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

Authority	Name & Signature	Date
Quality Control (SRU)	***« signed by Daniel Hartin »*** (Daniel HARTIN)	26.10.2009
Head of Unit (SRU)	***« signed by Juan Vázquez-Sanz »*** (Juan VAZQUEZ-SANZ)	26.10.2009
Chairman Safety Regulation Commission (SRC)	***« signed by Jos Wilbrink »*** (Jos WILBRINK)	26.10.2009

(Space Left Intentionally Blank)

F.4 AMENDMENT RECORD

The following table records the complete history of this document.

Edition No.	Date	Reason for Change	Pages Affected
1.0	26-Feb-02	Creation of Document after assessment by SRC Expert Panel of AMC for EATMP SAM.	All
1.1	09-Jul-02	Additional AMC for EUROCAE ED78A.	10 - 15
2.0	12-Dec-02	Version 1.1 approved without comment. Document format updated.	All
2.1	06-Apr-04	Additional AMC for LVNL Safety Criteria.	14 & 15
2.2	16-Jun-04	Document sent to SRC for formal approval by correspondence.	All
3.0	10-Aug-04	Document formally issued following SRC approval by correspondence (RFC No. 0407).	All
3.1	20-Nov-06	Additional AMC for SAM V2 and DFS methodology, sent to the AMC panel experts for final review.	All
3.2	25-Feb-08	Finalisation of AMC process for SAM V2 (incorporation of expert position).	Chapter 5
3.3	20-Mar-09	Finalisation of AMC process for SAM V2 (final incorporation of expert position) and SRU quality check.	Chapter 5
4.0	26-Oct-09	Document formally released following RFC no. 0907.	-

(Space Left Intentionally Blank)

F.5 CONTENTS

(Space Left Intentionally Blank)

F.6 EXECUTIVE SUMMARY

This document is intended to present the acceptable means of compliance (AMC) recognised by the SRC as possible harmonised ways to meet ESARR 4 provisions within the ECAC region.

The AMCs recognised by SRC are not mandatory. They represent means, or alternative means, but not necessarily the only possible means, by which mandatory provisions established by ESARR 4 can be met under certain identified conditions. Their acceptability has successfully been demonstrated at SRC level as a result of a formal assessment.

This document will include a Statement of Compliance for each means of compliance recognised by SRC as an AMC to meet ESARR 4 provisions. The Means of Compliance presented in this document are;

- **EAM 4 / AMC 1** - EATMP Air Navigation System Safety Assessment Methodology
- **EAM 4 / AMC 2** - EUROCAE ED78A
- **EAM 4 / AMC 3** - LVNL Safety Criteria
- **EAM 4 / AMC 4** - DFS Safety Assessment Methodology
- **EAM 4 / AMC 5** - EATMP Air Navigation System Safety Assessment Methodology (SAM V2)"

The Statements of Compliance;

- Define the SRC position about the acceptability of the AMC,
- Summarise the conclusions of the SRC's assessment as captured in a more detailed Assessment Document, developed in the form of an SRC Document The associated assessment document provides for a comprehensive rationale to support the SRC's position, and
- Identify the scope, terms and conditions under which the acceptability applies.

(Space Left Intentionally Blank)

1. EAM 4 / AMC 1

ASSESSMENT OF THE PMC "EATMP AIR NAVIGATION SYSTEM SAFETY ASSESSMENT METHODOLOGY (FHA)" AS A MEANS OF COMPLIANCE WITH ESARR 4

STATEMENT OF COMPLIANCE FOR EATMP SAM V1.

(Ref: EAM 4 / AMC 1)

SUMMARY

The EATMP Air Navigation System Safety Assessment Methodology (FHA) has been formally proposed by EATMP for assessment by the SRC as a means of compliance with ESARR 4.

Accordingly, the SRC established an Expert Panel to assess the acceptability of the "EATMP Air Navigation System Safety Assessment Methodology (FHA) - SAF. ET1.ST03.1000-MAN-01-00, Edition 1.0, April 2000". That document constituted the Proposed Means of Compliance (PMC) under consideration.

This "Statement of Compliance", proposed by the Expert Panel and agreed by SRC, summarises the results of that assessment and defines the SRC's position about the acceptability of the PMC "EATMP Air Navigation System Safety Assessment Methodology (FHA)".

Note : EAM 4 / AMC 1 (SAM, Version 1) has been superseded by EAM 4 / AMC 5 (SAM, Version 2)

(Space Left Intentionally Blank)

STATEMENT OF COMPLIANCE[1]

(Ref: EAM 4 / AMC 1)

STATEMENT

For the Proposed Means of Compliance "EATMP Air Navigation Safety Assessment Methodology (FHA), Edition 1.0" to meet the mandatory provisions of ESARR 4, Edition 1.0:

It should be expanded to;

- Address the complete life-cycle of the part of the ATM System under consideration beyond the setting of safety objectives, and
- Adopt a total system approach, except for those situations where the scope and intended functions of the proposed change to the ATM System have been demonstrated to have no direct relationship with the airborne and spatial segments of the ATM System.

It should be modified;

- In order to include a severity scheme which is fully consistent and/or compatible with ESARR 4 (Refer to Appendix A, Fig.A-1),
- In order to include a risk assessment approach and risk classification scheme fully consistent with ESARR 4 (Refer to Section 5.2 (iii) and Appendix A, section A-2),
- So that the meaning of 'risk' is clarified to the user of The PMC.

It should be read and understood according to the following;

- "external events" # "characteristics of environment",
- "Flight Phase" is one characteristics of environment,
- "Operational Conditions = "characteristics of environment".

1 *As included in Section 5 of SRC DOC 12 (Edition 1.0, Released Issue), "Assessment of the EATMP Air Navigation System Safety Assessment Methodology as a Means of Compliance with ESARR 4".*

CROSS REFERENCE TO ESARR 4

The implementation of the Proposed Means of Compliance “EATMP Air Navigation Safety Assessment Methodology (FHA), Edition 1.0” meets the following mandatory provisions of ESARR 4, Edition 1.0:

- ESARR 4 Section 5.1 c)
- ESARR 4 Section 5.2 a)
- ESARR 4 Section 5.2 b) (i)
- ESARR 4 Section 5.2 b) (ii) if slightly modified
- ESARR 4 Section 5.3 (in so far as all activities required under 5.1 c), 5.2 a) 5.2 b) (i) and (ii) are concerned).

The implementation of the Proposed Means of Compliance “EATMP Air Navigation Safety Assessment Methodology (FHA), Edition 1.0” does not meet the following mandatory provisions of ESARR 4, Edition 1.0:

- ESARR 4 Section 5.1 a)
- ESARR 4 Section 5.2 b) (iii)
- ESARR 4 Section 5.2 c)
- ESARR 4 Section 5.2 d)
- ESARR 4 Section 5.3 (in so far as all activities required under 5.1 a), 5.2 b) (iii), 5.2 c) and d) are concerned).

(Space Left Intentionally Blank)

2. EAM 4 / AMC 2

ASSESSMENT OF THE PMC "EUROCAE ED78A - GUIDELINES FOR APPROVAL OF THE PROVISION AND USE OF AIR TRAFFIC SERVICES SUPPORTED BY DATA COMMUNICATIONS - DECEMBER 2000" AS A MEANS OF COMPLIANCE WITH ESARR 4

STATEMENT OF COMPLIANCE FOR EUROCAE ED78A

(Ref: EAM 4 / AMC 2)

SUMMARY

The EUROCAE ED78A "Guidelines for approval of the provision and use of Air Traffic Services supported by data communications" has been formally proposed by EUROCAE for assessment by the SRC as a means of compliance with ESARR 4.

Accordingly, the SRC established an Expert Panel to assess the acceptability of the EUROCAE ED78A "Guidelines for approval of the provision and use of Air Traffic Services supported by data communications", December 2000. That document constituted the Proposed Means of Compliance (PMC) under consideration.

This "Statement of Compliance", proposed by the Expert Panel and agreed by SRC, summarises the results of that assessment and defines the SRC's position about the acceptability of the PMC "EUROCAE ED78A".

(Space Left Intentionally Blank)

STATEMENT OF COMPLIANCE[2]

(Ref: EAM 4 / AMC 2)

STATEMENT

The Proposed Means of Compliance "EUROCAE ED78A" meets the provisions of ESARR 4 except for;

- Some ESARR 4 requirements are not addressed at all by ED78A or not fully addressed (even as process objectives),
- Other ESARR 4 requirements are addressed by ED78A but only as process objectives and without any specific guidance being developed within the document on how to meet those requirements,
- Other ESARR 4 requirements are addressed by ED78A, not only identified as process objectives but also for which a certain level of guidance is provided on how to meet those requirements.

The mandatory provisions of ESARR 4 that are met by the PMC are listed at the end of this section.

For the Proposed Means of Compliance "EUROCAE ED78A" to meet the mandatory provisions of ESARR 4, Edition 1.0, it should be expanded or complemented by additional guidance material by EUROCAE or the user of the PMC to;

- Address all changes to the ATM System,
- Go beyond the current process objective and to provide guidance on how to conduct risk assessment and mitigation within one organisation only, when no co-ordination is required with other stakeholders,
- Provide additional guidance on how to address the three elements, people, procedures, equipment, their interactions and the interactions with the remainder of the ATM System,
- Address the complete life-cycle of the part of the ATM System to include 'transfer to operations', 'maintenance' and 'decommissioning',
- Provide additional guidance on how to determine safety requirements from safety objectives,
- Provide additional guidance on how to determine safety objectives in a manner consistent with ESARR 4,

[2] *As included in section 5 of SRC DOC 20 (Edition 1.0) "Assessment of EUROCAE ED78A as a Means of Compliance with ESARR 4".*

- Provide guidance on how to verify that safety objectives and requirements are and will be met during the whole life cycle of the system, with a specific focus on the verification that the integrated CNS/ATM system meets allocated safety objectives,

- Provide guidance on how a safety argument could be developed, based on an evidence collected, demonstrating that tolerable safety will be achieved and will continue to be met.

It should be modified or clarified by EUROCAE or by the user of the PMC;

- On how to use the severity scheme of The PMC in a manner which is fully consistent and/or compliant with ESARR 4 (Refer to Appendix A, Fig.A-1),

- As related to hazards being based on operational effects,

- The identification of hazards and assessment of related effects shall include, in addition to the provisions of ED78A;

  - An assessment of credible hazards,
  - An assessment of the severity of effects,
    - Taking into account the effects of hazard on ATS functionality,
    - Taking into account the most probable effects of hazards, and
    - Under the worst case scenario.

- How to complement the risk assessment approach and risk classification scheme of the PMC in manner fully consistent/compliant with ESARR 4 (Refer to Section 5.2 (iii) and Appendix A, section A-2) with section which,

- Provides additional guidance on how to determine safety objectives,

- Leads to the setting of quantitative safety objectives consistent with all applicable safety regulatory minima,

- Recognises explicitly that, as a minimum, ATM safety regulatory minima of the airspace where operations take place shall be met,

- Includes additional safety management considerations beyond the pure demonstration of compliance to applicable safety regulatory minima,

- To consider the possible allocation of safety requirements to parts of the ATM system other than the constituent part under consideration,

- So that the meaning of ‘risk’ and ‘element’ and differences with ESARR 4 is clarified to/by the user of The PMC.

CROSS REFERENCE TO ESARR 4

For changes related to ATS supported by data communications and for the risk assessment and mitigation activities which require co-ordination between more than one stakeholder, the implementation of the Proposed Means of Compliance ED78A meets the following mandatory provisions of ESARR 4, Edition 1.0;

- ESARR 4 Section 5.1 b)
- ESARR 4 Section 5.2 a)
- ESARR 4 Section 5.2 b) (i) if slightly expanded
- ESARR 4 Section 5.2 b) (ii) only if clarified and used as consistent with ESARR 4
- ESARR 4 Section 5.2 c) (i)
- ESARR 4 Section 5.2 c) (ii) only if clarified and slightly expanded
- ESARR 4 Section 5.2 c) (iii)
- ESARR 4 Section 5.3 b)

The implementation of the Proposed Means of Compliance ED78 does not fully meet the following mandatory provisions of ESARR 4, Edition 1.0;

- ESARR 4 Section 5.1 a)
- ESARR 4 Section 5.1 c) (more guidance required)
- Section 5.2 b) (iii) (more guidance required and only if clarified and used as consistent with ESARR 4)
- ESARR 4 Section 5.2 d) (i)
- ESARR 4 Section 5.2 d) (ii)
- ESARR 4 Section 5.2 d) (iii)
- ESARR 4 Section 5.2 d) (iv)
- ESARR 4 Section 5.3 a)

3. EAM 4 / AMC 3

ASSESSMENT OF THE PMC "LVNL SAFETY CRITERIA" AS A MEANS OF COMPLIANCE WITH ESARR 4

STATEMENT OF COMPLIANCE FOR LVNL SAFETY CRITERIA

(Ref: EAM 4 / AMC 3)

SUMMARY

The LVNL "Safety Criteria" document has been formally proposed by LVNL for assessment by the SRC as a means of compliance with ESARR 4.

Accordingly, the SRC established an Expert Panel to assess the acceptability of this method.

The "Statement of Compliance", proposed by the Expert Panel and agreed by the SRC, summarises the results of that assessment and defines the SRC's position about the acceptability of the PMC "LVNL Safety Criteria".

(Space Left Intentionally Blank)

STATEMENT OF COMPLIANCE[3]

(Ref. EAM 4 / AMC 3)

STATEMENT

For changes related to ATM under the managerial control of LVNL, the implementation of the Proposed Means of Compliance 'LVNL Safety Criteria' meets the following mandatory provisions of ESARR 4, Edition 1.0;

- ESARR 4 Section 5.2 a)
- ESARR 4 Section 5.2 b) (iii) – only if;
  - supported by a data collection system that validates the apportionment,
  - the LVNL TLS and the ESARR 4 TLS can be shown to be consistent.

The implementation of the Proposed Means of Compliance 'LVNL Safety Criteria' does not fully meet the following mandatory provisions of ESARR 4, Edition 1.0;

- ESARR 4 Section 5.1 c) (more guidance required)
- ESARR 4 Section 5.2 c) (ii) (more guidance required)

The implementation of the Proposed Means of Compliance 'LVNL Safety Criteria' is not intended to meet the following mandatory provisions of ESARR 4, Edition 1.0;

- ESARR 4 Section 5.1 a)
- ESARR 4 Section 5.1 b)
- ESARR 4 Section 5.2 b) (I)
- ESARR 4 Section 5.2 b) (ii)
- ESARR 4 Section 5.2 c) (i)
- ESARR 4 Section 5.2 c) (iii)
- ESARR 4 Section 5.2 d) (i)
- ESARR 4 Section 5.2 d) (ii)

[3] *As included in section 5 of SRC DOC 33 (Edition 1.0) "Assessment of the LVNL Safety Criteria as a Means of Compliance with ESARR 4".*

- ESARR 4 Section 5.2 d) (iii)
- ESARR 4 Section 5.2 d) (iv)
- ESARR 4 Section 5.3 a)
- ESARR 4 Section 5.3 b)

(Space Left Intentionally Blank)

4. EAM 4 / AMC 4

ASSESSMENT OF THE PMC "DFS CORPORATE DIRECTIVE SAFETY ASSESSMENT" AS A MEANS OF COMPLIANCE WITH ESARR 4

STATEMENT OF COMPLIANCE FOR DFS CORPORATE DIRECTIVE SAFETY ASSESSMENT

(Ref: EAM 4 / AMC 4)

SUMMARY

The "DFS Safety Assessment Methodology" has been formally proposed by DFS for assessment by the SRC as a means of compliance with ESARR 4.

Accordingly, the SRC established an Expert Panel to assess the acceptability of the 'DFS Safety Assessment Methodology' as defined in two documents ('Corporate Directive Safety Assessment' (CDSA), Version 1.0.1, dated 1.6.2003, reference VYK.01 and 'Safety Assessment Handbook' Volume 1: Introduction to the Methodology, Version 1.02, dated 24. November 2003). These documents constituted the Proposed Means of Compliance (PMC) under consideration.

This "Statement of Compliance", proposed by the Expert Panel and agreed by SRC, summarises the results of that assessment and defines the SRC's position about the acceptability of the PMC "DFS Safety Assessment Methodology".

(Space Left Intentionally Blank)

STATEMENT OF COMPLIANCE[4]

(Ref. EAM 4 / AMC 4)

STATEMENT

The PMC has been validated by the SRC Expert Panel in charge of assessing to what extent the 'DFS Safety Assessment Methodology', as defined in two documents ('Corporate Directive Safety Assessment' (CDSA), Version 1.0.1, dated 1.6.2003, reference VYK.01 and 'Safety Assessment Handbook' Volume 1: Introduction to the Methodology, Version 1.02, dated 24. November 2003), complies with ESARR 4 "Risk Assessment and Mitigation in ATM", Edition 1.0.

Complementary information has also been provided by DFS:

- "Safety assessment document", template and example;
- Manual on "Assurance and Demonstration of the Safety of External Services" V1.0 (07/2003);
- The latest release of 'Safety Assessment Handbook' (SAH) Volume 1: Introduction to the Methodology, Version 2.02, dated 9 November 2005.

SRC Document 39 comprises the outcome of this assessment and establishes the rationale for the SRC judgement on the acceptability of the 'DFS Safety Assessment Methodology' as a Means of Compliance with ESARR 4. It considers all sections of ESARR 4 and includes a complete mapping between each safety requirement included in ESARR 4, Sections 3 & 5 and Appendix A, and the elements of the Proposed Means of Compliance (PMC), which are considered as meeting the intent of the requirement. It also provides a set of conclusions and recommendations to support the final SRC judgement. The conclusions not only refer to the compliance with the totality of ESARR 4, but also, where necessary, to the compliance with part(s) of ESARR 4. The sets of conclusions and recommendations provide justifications supporting the final statement on the PMC, as well as proposed ways forward for the DFS standard to be fully compliant with ESARR 4.

In general, the DFS Safety Assessment Methodology is well thought out and thoroughly documented. The SAH, in particular, is an expansive document. A translation into English was provided for review. It contains an excellent exposition of the use of probability theory and Baysian networks in risk assessment. During the initial part of the assessment, a significant number of comments were generated. It was felt that many of these could be to the result of misunderstandings caused by differences in culture or errors in translation. Consequently, a meeting was arranged with DFS to discuss the comments. What emerged, for the reviewer of the first assessment, was an understanding of the DFS process and a realisation that, whilst the process itself satisfied ESARR 4, it had not been completely captured in the documentation. Since this assessment is a comparison of the DFS documentation with ESARR 4, these deficiencies have been recorded in Appendix B to this document.

[4] *As included in section 5 of SRC DOC 39 (Edition 1.0) "Assessment of the Deutsche Flugsicherung GmbH (DFS) 'Corporate Directive Safety Assessment' as a Means of Compliance with ESARR 4".*

ESARR 4 contains twenty-three mandatory requirements, many of which cover several aspects in a single requirement, e.g. the whole lifecycle in requirement 5.1.a) and three component classes in requirement 5.1.c). To describe a process that adequately covers all the ESARR 4 requirements leads to the need to cover many additional aspects as well, e.g. how to describe a change.

Therefore, a need exists to include criteria on the interpretation of what ESARR 4 requires. Without such a common basis, there could be number of discrepancies between the Acceptable Means of Compliances (AMCs), depending upon the experience gained in the ATM community before the assessment and depending on the assessor views.

The assessment also raised the fact that it is difficult to consider the PMC of the Air Navigation Service Providers (ANSPs) as stand alone documents since they are mostly linked to the procedures of the overall safety management system. The environment of the PMC needs to be presented as far as possible.

A first assessment was performed on the previous version of the PMC (version 1.02, 24 November 2003) raised several issues with regard to its compliance with ESARR 4. A further assessment was performed on the basis of the most recent version of the PMC (version 2.02, 9 November 2005). The major issues raised by the first assessment have been corrected by an improvement in the documentation; only one issue and two observations remain with regard to the compliance to ESARR4:

The outstanding issue deals with the qualification of “changes in ATM” which appears too restrictive in the CDSA (non conformity with ESARR4 requirement §5.1).

The first observation deals with the use of Bayesian networks, which is a good approach but which is to be used cautiously. The validation of the figures used in the Bayesian networks, together with the estimation made by the experts and the assumptions made on mathematical modelling, should be done with the utmost care. The respective use of Bayesian network and worst case scenario should be clarified within the proposed methodology.

The outlines with regard to the validation of the risk classification scheme have not been kept for the second assessment, in particular because it does not clearly separate the risk classification scheme required for the design of a system from the tolerable level of safety (TLS) with regard to Annex 11, Chapter 2, paragraph 26, which deals with the provision of ATM services.

At the time of the second assessment, the severity definition and the risk classification scheme proposed by the DFS is compliant with ESARR 4. The DFS solution does not contradict ESARR 4. However, the use of this risk classification scheme combined with the Bayesian network needs further clarification and guidance should be provided in order to assess the severity of effects (observation 2).

(Space Left Intentionally Blank)

CROSS REFERENCE TO ESARR 4

For changes related to ATM under the managerial control of DFS, the implementation of the Proposed Means of Compliance 'DFS Safety Assessment Methodology' meets the following mandatory provisions of ESARR 4, Edition 1.0, taking into account the changes which have been included in Version 2 of the Safety Assessment Handbook.

- ESARR 4 Section 3.1)
- ESARR 4 Section 3.2)
- ESARR 4 Section 5.1.a) (within the limitation of the interpretation of "any changes")
- ESARR 4 Section 5.1.b) (within the limitation of the interpretation of "any changes")
- ESARR 4 Section 5.1.c) (within the limitation of the interpretation of "any changes")
- ESARR 4 Section 5.2 a)
- ESARR 4 Section 5.2.b.i)
- ESARR 4 Section 5.2.b.ii) (observation 1 : use of Bayesian network)
- ESARR 4 Section 5.2.b.iii) (observation 1 : use of Bayesian network)
- ESARR 4 Section 5.2.c.i)
- ESARR 4 Section 5.2.c.ii)
- ESARR 4 Section 5.2.c.iii)
- ESARR 4 Section 5.2.d)
- ESARR 4 Section 5.2 Note 1
- ESARR 4 Section 5.2 Note 2 (observation 1 : use of Bayesian network)
- ESARR 4 Section 5.3.a)
- ESARR 4 Section 5.3.b)
- ESARR 4 Appendix A-1 (1)

- ESARR 4 Appendix A-1 (2) (observation 1 : use of Bayesian network)
- ESARR 4 Appendix A-1 (3) (observation 2 : need for guidance to assess the severity of effects)
- ESARR 4 Appendix A-2 (1)
- ESARR 4 Appendix A-2 (2)

The implementation of the Proposed Means of Compliance 'DFS Safety Assessment Methodology' does not fully meet the following mandatory provisions of ESARR 4, Edition 1.0;

- ESARR 4 Section 5.1

  There is no assurance that the DFS approach includes "any changes" as required by ESARR 4 Section 5.1

Observation 1 : the use of Bayesian network is to highlight the need for complementary information to prevent their misuse.

Observation 2 : the assessment of the severity of effects need to be supported by more guidance than it is provided in SAH Version 2.02

Those observations do not prejudge of the lack of advice which could be provided by the ANSP in order to develop best practices with regard to this method.

(Space Left Intentionally Blank)

5. EAM 4 / AMC 5

ASSESSMENT OF THE PMC "AIR NAVIGATION SYSTEM SAFETY ASSESSMENT METHODOLOGY (SAM V2)" AS A MEANS OF COMPLIANCE WITH ESARR 4

STATEMENT OF COMPLIANCE FOR DFS CORPORATE DIRECTIVE SAFETY ASSESSMENT

(Ref: EAM 4 / AMC 5)

SUMMARY

The "Air Navigation System Safety Assessment Methodology (SAM V2)" has been formally proposed by EATM for assessment by the SRC as a means of compliance with ESARR 4.

Accordingly, the SRC established an Expert Panel to assess the acceptability of the "Air Navigation System Safety Assessment Methodology (SAM V2)". This document constituted the Proposed Means of Compliance (PMC) under consideration.

This "Statement of Compliance", proposed by the Expert Panel and agreed by SRC, summarises the results of that assessment and defines the SRC's position about the acceptability of the PMC "Air Navigation System Safety Assessment Methodology (SAM V2)".

Note : EAM 4 / AMC 5 (SAM, Version 2) supersedes EAM 4 / AMC 1 (SAM, Version 1)

(Space Left Intentionally Blank)

STATEMENT OF COMPLIANCE[5]

(Ref. EAM 4 / AMC 5)

STATEMENT

The initial version of this document was presented to the SRC Expert Panel to assess the extent to which the SAM V2.0 ("EATMP AIR NAVIGATION SYSTEM SAFETY ASSESSMENT METHODOLOGY") complies with ESARR 4. It will compile the outcome of the SRC assessment and provides the basis for the SRC's judgement on the acceptability of the SAM as a Means of Compliance with ESARR 4.

The sections of ESARR 4 are grouped according to their nature. Advisory and mandatory statements are grouped into separate chapters. For each statement of ESARR 4, the statements of SAM that meet the intention of ESARR 4 are specified. In the Appendix a complete mapping of ESARR 4 and SAM is provided.

It also provides a set of conclusions and recommendations to support the final SRC judgement. In addition, it lists also the proposed areas of improvement for SAM.

SAM provides detailed guidelines regarding the application of best practices for risk assessment for Air Navigation Service Providers only. Due to the number of information provided a guideline on who should read what is also provided.

An in-depth description concerning functional approach to hazard identification as well as complementary approaches is provided. But there is some imbalance in the information for FHA and the one provided for SSA and PSSA as more detailed information concerning the processes for FHA than for SSA and PSSA is provided. Many PSSA and SSA Guidance Material have not been assessed as either being too low level of detail for this assessment (e.g. maintenance intervention, fault tree) or partially addressing other ESARR scope (e.g. software, human procedure).

SAM is a living document; therefore there are ongoing activities to reconcile information and best practices due to increasing experience in this domain. Due to the amount of information already available it is proposed for further development to provide a detailed list of definitions and a glossary to ensure consistency and to ensure that the SAM Level 1 provide sufficient information for compliance with ESARR 4 on a high level and that Level 2 only provides guidance for the implementation of the requirements of Level 1.

SAM provides comprehensive and detailed guidance for the implementation of ESARR 4 for equipment or systems, with the exception of certain human factor aspects. As SAM is a guidance material and not a regulation certain statements are not applicable for SAM

The recently developed Guidance Material for FHA Chapter 3: "E: Process for Deriving Risk Classification Scheme and Specifying Safety Objectives in ATM "in compliance" with ESARR 4" has been developed as a EUROCAE standard (ED125) and was designed to be used also stand alone. Therefore this document does not fit into the existing SAM straight forward and well explained structure of the documentation, the document need more explanation and some clarification. This document should be approved by Eurocae.

[5] *As included in section 5 of SRC DOC 12 (Edition 2.0, Released Issue), "Assessment of the EATMP Air Navigation System Safety Assessment Methodology as a Means of Compliance with ESARR 4".*

The Level 3 document, FHA Appendixes: "E: Examples of Safety Targets for NAV application Guidance Material (GM)" is the only Level 3 document provided for the evaluation as an AMC. The methodology used is in line with the ESARR4 requirements. The need for this document (different scope of Navigation with regard to ESARR 4) is not explained explicitly. The assumptions and input data were not verified and validated within the scope of this evaluation and, therefore, full compatibility of results with ESARR 4 cannot be stated.

The Eurocae document ED 125 has been proposed for assessment. After review of this documents it appears that no consensus exist within the panel to accept this document as an AMC to ESARR4.

The final comments made by the UK SRG are the following:

Compliance with ESARR 4

ED 125 claims compliance with ESARR 4. Such compliance arguments should be removed as this is not the case for three reasons:

1. ED 125 is not compliant with ESARR 4
2. SRC, the body responsible for declaring such compliance, has not done so – and in the light of 1 should not do so.
3. The referenced version of ESARR 4 will be short lived.

Explicit reference to ESARR 4 has now been removed from the title of ED 125, however there are approximately 30 references to ESARR 4 within the text of which 12 are material. These references clearly imply that the purpose of ED 125 is to be compliant with ESARR 4 and imply that it is indeed compliant – a detailed analysis of these references is available on request.

The reasons for the non compliance are:

1. ED 125 uses a different definition of Hazard. In ESARR 4, by definition, all hazards must potentially lead to an accident (Severity Class 1) they will also potentially to lead to incidents of other severity classes. In ED 125 a hazard does not necessarily lead to an accident.
2. ED 125 does not deal adequately with cumulative (total) risk. Worst Credible Effect, used in the Semi Quantitative Model and all subsequent models, eliminates all effects that are not responsible for setting the Safety Objective (ED 125 pg 39 - 40). The effect of this is to underestimate the cumulative (total) risk associated with each hazard (See 'Comments on Semi Quantitative Method' – Issue 1.2, provided previously). Moreover on page 34, N_j takes the value of the number of hazards with 'significant contribution'. There is no such restriction in ESARR 4 and this would also serve to underestimate the cumulative risk – this form of underestimation applies to the quantitative model as well.
3. Four schemes of various levels of complexity are proposed. To be valid, simpler (and less accurate) schemes should be more conservative than more complex (and more accurate) schemes. The schemes in ED 125 do not meet this criterion.
4. The data used to establish the safety targets for incidents of severity levels 2-4 does not meet the criterion required by ESARR 4: *The quantitative definitions for the safety objectives associated with the maximum tolerable probabilities of ATM directly contributing to incidents of severity class 2, 3, 4 and 5 in* ***the ECAC region*** *(4) remain to be determined once enough and consistent safety data have been collected by EUROCONTROL, which are consistent with the requirements outlined in ESARR 2.* Appendix B 1 shows that the values for ST3 and ST4 are not supported by adequate and consistent data. Moreover, during the RCS mandate process several states challenged the consistency for the value for ST 2.

5. It seems that there is an assumption that a hazard can only cause a single effect in a single severity class:
    a. in 4.5 the risk budget is divided by the number of hazards not the number of effects.
    b. In 4.6 Pe_{ij} is used rather than Pe_{ijk}.
    c. In the example in section 5, the risk budget is established via the number of hazards not the number of effects.

    This assumption is not valid under ESARR 4 which recognises that, in general, there may be many effects (of a given severity level) associated with an individual hazard. While Appendix A demonstrates that a hazard can lead to several effects of the same severity class, the simplifications render the method of little practical utility (see 'fitness for purpose' – 3 - below) and the note at the beginning states that it is "**not** to be used to apply [to] the various models". This last shows that the models are not rigorous or objective since they are not underpinned by a mathematical model.
6. The restrictions placed on Pe_{ij} in 4.6 are not supported in ESARR 4

The claim for the compliance of ED 125 against ESARR 4 is for version 1.0 of ESARR 4. This is of little practical utility and would serve to misrepresent the current state of affairs. There are differences between the ESARRs and the SES legislation and one of the recommendations of the Double Regulation Add Hoc Group (DRAHG) is that existing ESARR text should be removed and be replaced with a reference to (or a copy of) the appropriate SES regulations. Differences in approach are to be dealt with by negotiations between EUROCONTROL and the EC. ESARR 4 is one of the ESARRs for which differences exist. As far as SRG is aware the DRAHG recommendations have been accepted and consequently the context in which ED 125 exists is changing. It would therefore be more appropriate to seek compliance with the SES regulations but this is dealt with next (2).

Relationship to RCS Mandate

There is some concern at the apparent rush to publish ED 125 at this stage. ED 125 cannot validly claim compliance with ESARR 4 and due to the close relationship between ESARR 4 and the SES Common Requirements, ED 125 would not be compliant with these either. Even if ED 125 were to claim compliance with ESARR 4, such compliance will be short lived (see 1 above). It would appear that the most useful outcome of the EUROCAE work would be for ED 125 to be developed into an AMC for the RCS Implementing Rule foreseen by the SES Common Requirements.

However, after the ENPRM process for the RCS Mandate had completed, EUROCONTROL delivered a report to the EC, which clearly indicated that substantial work is still needed before proceeding with the submission of any proposal to the SSC. It recommends that the EC consider the continuation of that work. Furthermore, the report highlights a number of important issues that are still open. Two of these issues: the nature of the advisory material and inconsistencies in proposed methodologies, have a direct bearing on any AMC and therefore by implication on ED 125.

Consequently, if EUROCAE wished ED 125 to become an AMC to the SES regulations on Risk Classification Schemes, it would be premature to release it until the outcome of the development of the RCS Implementing Rule and its associated advisory material is known. To release it in the hope that it will satisfy the RCS Implementing Rule is both naive and gives the impression of a 'solution seeking a problem'.

Usefulness/Fitness for Purpose

The scope of ED 125 is limited and does not include the solution to some more pressing issues, consequently it is difficult to see why ED 125 will be useful in its current form. Some of the guidance also makes its fitness for purpose questionable. This is because ED 125:

- provides scope for inconsistent application
- does not describe sound or useable models
- fails to provide adequate guidance on risk budget setting and limiting the scope of the change
- provides an inappropriate explanation of Ambition Factor

Inconsistent application

SRG believes that the alternative models and wide ranging data values available in ED 125 allow users too much scope so that they can generate an inappropriate RCS.

The criteria for the use of the four models are not present in ED 125. Questions such as: under what circumstances, for what purposes and by whom, each model may be used, are unanswered.

Basically ANSPs are left to select the model they wish to use. Such decisions could be based primarily on their own view of ease of use versus the cost of over engineering. There is risk that immature ANSPs will be driven towards the simpler models without fully understanding the consequences and far from over engineering the system will underestimate its safety risk and so under engineer the system. It is true that NSAs oversee the choice of model and the system solution but an immature NSA may also misunderstand the risk. There is no guarantee that a mature NSA will supervise an immature ANSP and even if this were the case, the NSA is not required to and does not have the resources to do a thorough investigation and may still have difficulty in challenging the ANSPs interpretation of ED 125.

Sound Models

Appendix A, which could provide a firm foundation for the models, has as its opening remarks: "this appendix is not to be used to apply [to] the various models as described in this document", thus apparently destroying the objectivity of the models. The appendix was in fact derived from previous SRG work designed to show that the underpinning mathematics of early versions of ED 125 were incorrect and that assumptions made lead to impractical models. Unfortunately the assumptions remain and worse, become desirable features in the models. The effects and the conditional probability of an effect arising from a hazard (Pe) are 'lumped' variables (as discussed in previous exchanges). It is difficult to understand how a mid air collision and a CFIT having their roots in the same hazard could have the same accident trajectory and the same Pe. While a lumped Pe could be formed connecting a hazard to a lumped effect (in this case both mid air collision and a CFIT) it is very difficult to see why this would be of benefit since it could only be calculated by knowing the Pe's associated with each individual hazard/effect trajectory. Consequently, while lumping both Pe and STj is a mathematical simplification it has no practical utility and to base a model on such a mathematical nicety is to render it useless.

The models rely on knowledge of the number of hazards in the ANSP's system and ED 125 sanctions an assumption that there are approximately 125 of these. Firstly, ESARR 4 requires knowledge of the number of effects as well the number of hazards but ED 125 seems to assume that there will only be one effect (in each severity class) per hazard and secondly, while 125 hazards may be appropriate for a small airport, it is certainly a gross underestimate for an airport of the complexity of LHR. It seems that ED 125 may be dealing with hazard classes rather than actual hazards. The need for knowledge of the total number of hazards is not only the Achilles heel of the method but is probably misleading since all that is of interest in a change scenario is the hazards that are associated with the change.

Risk Budget Setting

ESARR 4 deals with a change to an ATM system i.e. only part of the ANSP's services would be affected by the change. Table 1 describes the safety targets for the whole ECAC airspace. The risk budget for the change is only a small part of this overall safety target. Moreover, when making a change, the ANSP wishes to constrain the Risk Assessment and Mitigation activities to those parts of the system for which it is necessary to re-assess the hazards and effects. ED 125 provides no guidance on apportioning the risk budget or on setting the system limits for the change. Both are crucial in determining the total risk budget for the change. ED 125 would have been more useful if it had concentrated on providing guidance for these aspects rather than the confused guidance it does give on setting STj – sometimes it appears that STj is the total ANSP safety target (risk budget) and at others it is the safety target for the change, as in the example for 5.1 – is the change described here the total set of ANSP services or just part of those services?

Ambition Factor

No explanation of how the ambition factor is arrived at is given in ED 125. In fact the guidance given is wrong – it is unlikely that monitoring would have any bearing on the ambition factor, it is more likely the accuracy of the design analysis should have a bearing on the factor. Consequently it is not so much an ambition factor as a lack of confidence factor. The guidance given leaves the impression that, as far as ED 125 is concerned, it is an arbitrary process aimed at ensuring the service provider always meets the safety target, with some 'headroom'.

In fact this is only one purpose of the ambition factor and has its roots in the need to accommodate ones confidence in ones predictions. The other purpose is to satisfy the safety management principle of continually trying to become safer as technology and science (knowledge of systems analysis) allows. ED 125 would have been more useful had it separated these concerns and provided guidance on how to establish confidence limits and how to use the safety management system to provide more stringent safety targets as the state of the art progresses. As it is, it provides inadequate and inappropriate guidance.

CROSS REFERENCE TO ESARR 4

PMC SAM V2 for Level 1 and 2

The PMC The PMC SAM as listed in chapter 2 for Level 1 and 2 (except Level 3 document: FHA Appendices “E: Examples of Safety Targets for NAV application”, and ED125 - please see next paragraph for details) meets the following provisions of ESARR 4 with regard ATM equipment development;

- ESARR 4 Section 3.1)
- ESARR 4 Section 3.2)
- ESARR 4 Section 5.1
- ESARR 4 Section 5.1.a)
- ESARR 4 Section 5.1.b)
- ESARR 4 Section 5.1.c)
- ESARR 4 Section 5.2 a)
- ESARR 4 Section 5.2.b.i)
- ESARR 4 Section 5.2.b.ii)
- ESARR 4 Section 5.2.b.iii)
- ESARR 4 Section 5.2.c.i)
- ESARR 4 Section 5.2.c.ii)
- ESARR 4 Section 5.2.c.iii)
- ESARR 4 Section 5.2.d)
- ESARR 4 Section 5.2 Note 1
- ESARR 4 Section 5.2 Note 2
- ESARR 4 Section 5.3.a)
- ESARR 4 Section 5.3.b)
- ESARR 4 Appendix A-1 (1)

- ESARR 4 Appendix A-1 (2)
- ESARR 4 Appendix A-1 (3)
- ESARR 4 Appendix A-2 (1)
- ESARR 4 Appendix A-2 (2)

FHA Appendix E (out of scope of the Level 1 and 2 assessment)

Observation 1 (out of the scope of the Level 1 and 2 assessment)

The Level 3 document: FHA Appendices "E: Examples of Safety Targets for NAV application" addresses item 5.2b iii of ESARR 4:

The methodology used is in line with the ESARR4 requirements. The assumptions and input data were not verified and validated within the scope of this evaluation and, therefore, full compatibility of results with ESARR4 cannot be stated.

As there are several assumptions, a sensitivity analysis is proposed with changed assumptions and data near the confidence interval limit to identify the influence of the changed assumptions on the result. The assumptions are the weakest point in any such analysis, and they are also identified as such in chapter 8 of the document.

With regard to the contextual assumption of IRP it is recommended that the differences are identified and the assumptions made should be justified.

The statement made in chapter 6.4 challenges the commonly recognised contribution (e.g. SRC DOC 1 and SRC Policy DOC 1). Therefore, further studies to validate this assumption are recommended.

ED125 (out of scope of the SAM Level 1 and 2 assessment)

Observation 1: ESARR 4 Appendix A-1 (3)

The implementation of the Proposed Means of Compliance SAM (Safety Assessment Methodology) V2 meets the following mandatory provisions of ESARR 4, Edition 1.0 : ESARR 4 Appendix A-1 (3) , however taking into account that the document ED125, has been provided in a version which has not been approved by all the Panel's members. It has been proposed that the final position with regard ED125 will be done after the result of EUROCAE approval process.

(***)