



The European Organisation for Civil Aviation Equipment
L'Organisation Européenne pour l'Équipement de l'Aviation Civile

RECOMMENDATIONS FOR REVISION OF ED-78A

This document is the exclusive intellectual and commercial property of EUROCAE.
It is presently commercialised by EUROCAE.

This electronic copy is delivered to your company/organisation for internal use exclusively.

In no case it may be re-sold, or hired, lent or exchanged outside your company.

ER-007

June 2012

RECOMMENDATIONS FOR REVISION OF ED-78A

This document is the exclusive intellectual and commercial property of EUROCAE.

It is presently commercialised by EUROCAE.

This electronic copy is delivered to your company/organisation for internal use exclusively.

In no case it may be re-sold, or hired, lent or exchanged outside your company.

ER-007

June 2012

ER-007 is composed of 2 Volumes:

- Volume 1: Recommendations for Revision of ED-78A – Report
- Volume 2: Recommendations for Revision of ED-78A – Additional Input Material



The European Organisation for Civil Aviation Equipment
L'Organisation Européenne pour l'Équipement de l'Aviation Civile

RECOMMENDATIONS FOR REVISION OF ED-78A

VOLUME 1 – REPORT

This document is the exclusive intellectual and commercial property of EUROCAE.
It is presently commercialised by EUROCAE.

This electronic copy is delivered to your company/organisation for internal use exclusively.

In no case it may be re-sold, or hired, lent or exchanged outside your company.

ER-007 Volume 1

June 2012

RECOMMENDATIONS FOR REVISION OF ED-78A

VOLUME 1 – REPORT

This document is the exclusive intellectual and commercial property of EUROCAE.

It is presently commercialised by EUROCAE.

This electronic copy is delivered to your company/organisation for internal use exclusively.

In no case it may be re-sold, or hired, lent or exchanged outside your company.

ER-007 Volume 1

June 2012

FOREWORD

1. This document was prepared by EUROCAE Working Group 91 with support from the European Aviation Safety Agency, EUROCONTROL, SESAR Joint Undertaking, national civil authorities, Air Navigation Service Providers, and industry bodies and was approved by the Council of EUROCAE in June 2012. The contributions received from these organisations are gratefully acknowledged.
2. EUROCAE is an International not-for-profit organisation, formed to advance the art and science of aviation and aviation electronic systems for the benefit of the public.
3. Since EUROCAE is not an official agency of any European State, its recommendations may not be regarded as statements of official government policy unless so enunciated by the appropriate government organisation, conference of governments, or agency having statutory jurisdiction over any matters to which the recommendations relate.
4. The report addresses coordination processes leading towards safety, performance and interoperability assessment, with an eventual aim to support also airworthiness certification and operational approval.
5. Details of any amendments and updates of this report may be found on the EUROCAE web site.
6. Copies of this report may be obtained from:

EUROCAE
102, rue Etienne Dolet
92240 MALAKOFF
France

Telephone: 33 1 40 92 79 30

Fax: 33 1 46 55 62 65

Email: eurocae@eurocae.net

Website: www.eurocae.net

TABLE OF CONTENTS

FOREWORD	I
EXECUTIVE SUMMARY	V
CHAPTER 1 INTRODUCTION	1
1.1 THE HISTORY OF ED-78A & FURTHER DEVELOPMENTS SINCE PUBLICATION	1
1.1.1 USE OF ED-78A IN AVIATION.....	1
1.1.2 OTHER ACTIVITIES IN THE FIELD OF AVIATION SAFETY SINCE ED-78A...	1
1.1.3 LESSONS LEARNED IN APPLICATIONS OF ED-78A.....	3
1.2 TERMS OF REFERENCE	3
1.3 STRUCTURE OF THE REPORT.....	4
1.4 HISTORY OF WG-91 ACTIVITIES AND METHOD OF WORKING	4
1.4.1 TEAM COMPOSITION	4
1.4.2 MEETING SCHEDULE.....	4
1.4.3 REVIEW OF SOURCE AND REFERENCE DOCUMENTS.....	5
1.4.4 IDENTIFICATION AND COLLATION OF ISSUES	5
1.4.5 EXPANSION OF ISSUES AND CONCLUSIONS	5
CHAPTER 2 GENERAL.....	7
2.1 INCREASING THE SCOPE OF CHANGES THAT ED-78A CAN ADDRESS	7
2.2 RECOMMENDATIONS	7
CHAPTER 3 OSED.....	8
3.1 LINKAGE OF OSED WITH 'OPERATIONAL USAGE'	8
3.2 LINKAGE OF OSED DESCRIPTIONS WITH ICAO (AND OTHER ORGANIZATIONS) SERVICE DESCRIPTIONS	9
3.3 INTERACTIONS WITH OTHER SYSTEMS	9
3.4 PARTIAL IMPLEMENTATIONS.....	10
3.5 OSED MATURITY	10
3.6 OSED LEVEL OF ACCEPTANCE BY STAKEHOLDERS	11
3.7 EMPHASIS ON CORE TEAM ACTIVITIES.....	11
3.8 RELATIONSHIP OF OSED – SPR – INTEROP WITH OTHER EUROCAE MATERIAL MOPS ETC.....	12
3.9 DEFINITION OF SAFETY TARGETS WITHIN THE OSED STAGE	13
3.10 GUIDANCE ON COLLECTION OF ENVIRONMENTAL CHARACTERISTICS.....	13
3.11 NEW SYSTEMS THAT REMOVE EXISTING FUNCTIONALITY	13
3.12 SUMMARY OF OSED SECTION.....	14
CHAPTER 4 OSA	15
4.1 ITERATION OF OSA AND OSED.....	15
4.2 DEPTH OF OSA	15
4.3 COMPLETENESS AND ADEQUACY OF HAZARD IDENTIFICATION AND CLASSIFICATION	16
4.4 NECESSARY INFORMATION REQUIRED IN SPR	16
4.5 SEVERITY CLASSIFICATION SCHEME: TABLE 4-1 OF ED-78A	16
4.6 TOLERABILITY OF RISK WITHIN ED-78A	17
4.7 ALLOCATION OF SAFETY OBJECTIVE AND REQUIREMENT (QUALITATIVE AND QUANTITATIVE ASPECTS)	18
4.8 HUMAN ERROR CONTRIBUTION	18
4.9 FORMAT OF OUTPUT EVIDENCE	19
4.10 ITERATIVE PROCESS FOR THE SPR DOCUMENT	19
4.11 IDENTIFIED SOURCES OF GUIDANCE MATERIAL	20

	4.12 SUMMARY OF OSA SECTION	20
CHAPTER 5	OPA	22
	5.1 NEEDS TO BE LINKED TO EXISTING STANDARDS.....	22
	5.2 IS OPA NOW PART OF SAFETY ASSESSMENT?	22
	5.3 ACCEPTABILITY OF OPA CLAIMS	23
	5.4 OPA GUIDANCE ON USE OF RCP CONCEPT	23
	5.4.1 NEW PERFORMANCE SPECIFICATION	23
	5.4.2 NEW GUIDANCE ON PERFORMANCE PARAMETERS	24
	5.5 OPA LINKAGE WITH OSA.....	25
	5.5.1 CONTINUITY	25
	5.5.2 AVAILABILITY	25
	5.5.3 INTEGRITY	26
	5.6 SUMMARY OF OPA SECTION	26
CHAPTER 6	INTEROPERABILITY	27
CHAPTER 7	TRANSITION / OPERATIONS	28
	7.1 ISSUES RELATING TO COORDINATED ENTRY INTO SERVICE	28
	7.2 ISSUES RELATING TO OPERATIONS.....	28
	7.3 EVIDENCE FOR APPROVAL	28
	7.4 TRANSITION HAZARDS	29
	7.5 RISKS ASSOCIATED WITH MULTIPLE CHANGES.....	29
	7.6 SUMMARY OF TRANSITIONS - OPERATIONS SECTION	29
CHAPTER 8	CERTIFICATION	31
	8.1 LINKAGE OF SPR WITH 'COORDINATED APPROVAL & CERTIFICATION PLANNING'	31
	8.2 LINKAGE OF MOPS & MASPS WITH 'COORDINATED APPROVAL & CERTIFICATION PLANNING'	31
	8.3 LINKAGE OF APPROVAL PLANNING WITH 'COORDINATED APPROVAL & CERTIFICATION PLANNING'	32
	8.4 VALIDATION OF SPR AND SYSTEM DESIGN	32
	8.5 MULTI-DOMAIN TESTING FOR VERIFICATION PURPOSES IN CERTIFICATION	33
	8.6 ARP4754	33
	8.7 DEVIATIONS DURING IMPLEMENTATION OR OPERATIONS	34
	8.8 TRANSITION CRITERIA.....	34
	8.9 DEVELOPMENT ASSURANCE LEVELS	34
	8.10 REAL APPROVAL PROCESS	35
	8.11 EASA-SES	35
	8.12 APPROVAL	36
	8.13 SUMMARY OF CERTIFICATION SECTION	36
CHAPTER 9	TRAINING PACKAGE	38
CHAPTER 10	RATIONALE AND RECOMMENDATIONS	39
	10.1 RATIONALE	39
	10.2 PROPOSALS FOR FURTHER ACTION BY EUROCAE	40
	10.3 CONSOLIDATED LIST OF RECOMMENDATIONS.....	40
	10.3.1 LEVEL 1 RECOMMENDATIONS	40
	10.3.2 LEVEL 2 RECOMMENDATIONS	40
	10.3.3 LEVEL 3 RECOMMENDATIONS	40
	10.3.4 LEVEL 4 RECOMMENDATIONS	40
	10.4 CONCLUSIONS	41

APPENDIX A	INDEX OF REFERENCES	42
APPENDIX B	REFERENCE SUMMARY CONTENT	45
APPENDIX C	ACRONYMS & ABBREVIATIONS.....	54
APPENDIX D	WG-91 TERMS OF REFERENCE.....	57
APPENDIX E	WG-91 MEMBERSHIP	61

EXECUTIVE SUMMARY

Background.

Working Group 91 was set up because of realisation that, since the publication of ED-78A in 2000, safety assessment processes have significantly advanced and extensions to processes which are described in ED-78A have been developed in an uncoordinated manner by several other Working Groups.

Method of Working.

The WG identified issues based on inputs to the group from material identified in the TORs, as well as the group members' own experience. These were then related to the major topic areas of ED-78A. The areas are: OSED, OSA, OPA, Interoperability, Transition/Operations, Certification, together with some overall considerations.

For each issue, the WG collected the present status of material to assess industry opinion and the maturity of approaches to the issue. The WG then developed recommendations on how the issue could be addressed by future activities within EUROCAE.

The WG used the following assessment criteria to formulate its recommendations:

- Is ED-78A currently deficient?
- Has an approach to the issue been practically demonstrated?
- To what degree has consensus agreement been reached on the approach?
- Are any activities already in progress to address the issue (e.g. within SESAR or EASA)?
- Does the issue remain within the current scope of ED-78A?
- Would another organisation be more appropriate to address the issue?

Recommendations.

The resulting recommendations have been grouped in four levels, corresponding to their priority/maturity, which EUROCAE may wish to consider in deciding how the issues identified can be addressed.

The grouping was:

- **Level 1.** Recommendations of issues to be addressed in a short-term update of ED-78A. These arise mainly due to errors and developments since ED-78A was originally issued and which are now mature.
- **Level 2.** Recommendations of issues to be addressed in a medium-term update of ED-78A with unchanged scope. These arise due to developments of mature consensus material since ED-78A was originally issued.
- **Level 3.** Recommendations of issues to be addressed in a longer term update of ED-78A, which could be carried out by a continuation of WG-91. These arise due to possible developments for which material is available, but which are not yet mature or do not have sufficient consensus..
- **Level 4.** Recommendations of issues that are better addressed by another body.

The basis for each recommendation is developed in detail in each section and a summary is provided at the end of the section. The complete set of issues, grouped as explained above, with cross references to the detailed discussion, is listed in the final Chapter.

Conclusions.

The WG considered that ED-78A has proven itself as a document that has focused the efforts of users in developing the idea of coordinated requirements determination. It is still actively used by many users. However, the WG recognise that there have been, and continue to be, developments in the areas of safety assessment and oversight. Some of these developments should be captured in ED-78A to reflect the current situation, but other developments indicate that ED-78A should not be the focus of development activity. The WG also recognise that ED-78A has never been formally captured into the regulatory framework.

The recommendations for action are therefore split into phases that reflect the maturity and consensus on possible developments.

The WG considers that

- The Level 1 recommendations must be actioned to maintain the applicability of ED-78A.
- The Level 2 recommendations should be actioned as they correspond to the capture of developments for which consensus could be reached.
- However the Level 3 recommendations should be actioned only if it is felt by EUROCAE that ED-78A should continue to be a lead vehicle for the development of coordinated requirement capture. If EUROCAE, EASA, RTCA and FAA consider that such developments are already being planned in other areas, then these recommendations should be actioned in those areas rather than via ED-78A.
- There are no actions envisaged by the WG for level 4 recommendations.

In general, the WG also considers that any development activities should include the involvement of all of EUROCAE, EASA, RTCA and FAA.

CHAPTER 1

INTRODUCTION

1.1 THE HISTORY OF ED-78A & FURTHER DEVELOPMENTS SINCE PUBLICATION

EUROCAE Document “Guidelines for approval of the provision and use of Air Traffic Services supported by Data Communications” (ED-78A) was issued in 2000. [1]. It was developed jointly by EUROCAE WG-53 and RTCA SC-189 and was originally intended for use in the data communications environment.

Since then, many elements of the processes described in ED-78A have been taken up and adapted for use in other environments. The main documentary components proposed in ED-78A have become part of the recognised set of EUROCAE documents, being regarded together as very similar to a Minimum Aviation System Performance Specification (MASPS). These components are:

- Operational Service and Environment Description (OSED);
- Safety and Performance Requirements (SPR)
- Interoperability Requirements (INTEROP).

However, the manner of use in other environments is not consistent, nor have the benefits and experiences obtained from this approach been shared for the benefit of ATM community as a whole.

Further, although ED-78A does not describe safety and performance assessment processes in detail, these have evolved since publication, and this has a bearing on how the ED-78A processes interact with the safety and performance processes.

1.1.1 Use of ED-78A in aviation

Undertaking industry-based safety assessments of CNS/ATM systems for global air- and ground implementations requires the use of an internationally agreed approach to the formulation of safety and performance requirements. Such guidance exists today through the ED-78A/DO-264 document.

The ED-78A approach generates coordinated Safety and Performance Requirements (SPR) at the boundaries of the ground and aircraft domains (i.e. at aircraft system or ground system as a whole) that are used by aircraft/avionics manufacturers, ANSP and other aviation stakeholders (e.g.: providers of supporting services) as input for implementation of new systems and services within their own organisation.

These stakeholders will then proceed with a more detailed safety assessment of their system or service, including the generation of safety requirements for sub-systems, based on the SPR cornerstone of the OSA results and assumptions concerning the safety requirements and/or mitigations held by the other stakeholders. For example, aircraft/avionics manufacturers and ANSPs typically apply their domain specific safety assessment approaches, e.g. ARP-4754 [2] or the EUROCONTROL Safety Assessment Methodology (SAM) [3].

1.1.2 Other activities in the field of aviation safety since ED-78A

A number of evolutions taken place in the last decade in USA and Europe within the domain of Safety Management Systems (SMS).

1.1.2.1 Europe

1.1.2.1.1 Safety Assessment

EUROCONTROL developed a Pan-European Safety Assessment Methodology (SAM), which currently provides best practices and guidance for safety assessment of ATM ground systems, covering Functional Hazard Assessment (FHA), Preliminary System Safety Assessment (PSSA), and System Safety Assessment (SSA).

In its present form the SAM is in fact a framework and a toolbox, suitable to perform safety assessments for ATM ground systems. However SAM is insufficient to provide full confidence in the safety assessment when both airborne and ground domains are involved or when new operational concepts presenting paradigm changes to the way ATM is operated have to be addressed. European representatives, participating in EUROCAE committees conduct safety assessments based on ED-78A, supplemented with ARP4761 and SAM.

The SAM has been further developed into SAME (Safety Assessment Made Easier), which is a specific interpretation of the more general SAM approach. The SAME [4] incorporates a change from a process approach to an objective approach and to include the 'success' approach. The SAME has been further developed by the SESAR Joint Undertaking and has become what is now known as the Safety Reference Material [16]. SAME has also been approved by the EUROCONTROL Safety Team

While the SAM method is currently commonly used to conduct Safety assessments by ANSPs, ARP4754/4761 [5] and EASA AMC25.1309 [6] are used for the Airborne domain.

Since 2006, the SAM and SAME method has also been introduced for the SPR/safety development within various EUROCAE/RTCA committees for the ground domain, in particular for WG-51 / SC-186, WG-78 / SC-214 and WG-76.

1.1.2.1.2 Safety Regulation

The EUROCONTROL Safety Regulation Commission (SRC) published EUROCONTROL Safety Regulatory Requirements (ESARR4) [7] in April 2001. They have been partially transposed into European law, and are published as SES IR2096/2005 [8] superseded by EC1035/2011 [9].

There are also plans for these regulations to be more fully integrated into the EASA regulatory framework and EASA rule making groups (RMT 0469 and RMT 0470) are in progress to achieve this. These rule making tasks are intending to address existing deficiencies in regulation such as (i) present focus of safety assessments on causes and consequences of internal failures only; (ii) present focus on over-prescriptive in the process to be followed; (iii) the present focus on application to individual changes only with little consideration of systemic effects.

ESARR4 required the use of a quantitative risk-based approach for risk assessments and mitigation of ATM systems, comprising airborne and ground elements. EC1035/2011 requires now that *"Safety objectives based on risk shall be established in terms of the hazard's maximum probability of occurrence, derived both from the severity of its effect, and from the maximum probability of the hazard's effect. As a necessary complement to the demonstration that established quantitative objectives are met, additional safety management considerations shall be applied so that more safety is added to the ATM system, whenever reasonable."* It can be interpreted from this that a quantitative risk-based approach is acceptable when feasible; however it shall be systematically complemented by safety management considerations.

1.1.2.2 USA:

Similarly, the FAA has developed in its Safety Management System (SMS) manual [10], a methodology for safety assessment describing the FHA and PSSA process for CNS/ATM systems, covering aircraft and ground-domain. FAA staff participating in RTCA committees, conduct safety assessments based on ED-78A/DO-264, supplemented with the SMS manual and ARP4754

1.1.3 Lessons learned in Applications of ED-78A

Traditionally, the development of SPR standards for CNS/ATM applications that involve the aircraft and ground domain, are carried out through the EUROCAE organisation and where the application has use outside Europe, typically involves RTCA. Before conducting joint safety assessments, it is crucial to combine the two regional approaches (satisfying the safety evolutions) into a common approach that works for both. This point is absolutely essential and would not suffer any exception, due to the global nature of the aviation system. This point is as important as for the interoperability aspects.

Three different EUROCAE/RTCA groups (WG-51/SC-186; WG-78/SC-214 and WG-76/SC-206), while developing SPR and INTEROP standards respectively in the area of AIS/MET data link services, ADS-B applications and the next generation of ATS data link services, based their work on the same common approach. Their experience shows that the common approach they have used works and that they have produced with the OSA process a set of meaningful generic (minimum) Safety Requirements the AOs, Aircraft/Avionics manufacturers and ANSPs use as input for certification of their products and operations.

The common approach did use the ED-78A/DO-264 document, but was supplemented with the following material from the EUROCONTROL-based SAM, the USA-based SMS and compatible with the globally agreed approach for safety assessment promulgated by airworthiness regulations (i.e.: ARP & Certification Specifications/ (FAA & EASA)).

The OSA adopted the use of a quantitative risk classification scheme. The ASOR/PSSA used a fault tree for each hazard to allocate in a top-down manner the hazard (top) Safety Objective to the stakeholders involved in the operation of the ATM system under assessment (aircraft system, ground system and humans) and to derive qualitative (humans, systems) and quantitative (systems only) safety requirements (SR).

In particular regarding qualitative and quantitative aspects of safety process, the EUROCAE/RTCA groups made use of several documents which have been proposed as a reference to be used to harmonize the process of coordinated requirements determination between domains (ARP4754, ED125 [11]...).

This experience has indicated that the ED-78A/DO-264 guidance alone does not sufficiently meet the needs of an overall, comprehensive demonstration of safety, when such a demonstration would be the compositional result of individual demonstrations, and not managed and monitored by a unique SMS.

As a result, EUROCAE decided to set up WG-91 to determine a possible path for the development of ED-78A to allow the document to be updated with the experience and developments since its publication, in particular to:

- Examine current situation with extended use of ED-78A
- Identify potential extensions and improvements.
- Identify reference material that describes extended use.
- Identify other activities already in progress that could have a bearing on the contents of ED-78A
- Consider also difficulties with use and identify where improvements could be made to alleviate such difficulties.
- Consider need for Guidance Material on use of ED-78A and identify candidate GM by reference.

1.2 TERMS OF REFERENCE

The points above were considered and elaborated by the EUROCAE Technical Advisory Committee (TAC) as well as by participants in WG-78 over a period of a couple of years, and documented in [12] *“Proposal for the revision of the Operational Safety Assessment (OSA) section ED-78A/RTCA DO-264 Guidelines to enhance applicability outside the data link application domain and to take into account lessons learnt when applying ED-78A in EUROCAE WG-78/SC-214”* and 0 *“EUROCAE Strategic Lines N°11 - Update of ED-78A”*.

A first draft Terms of Reference (TORs) was issued by EUROCAE TAC in mid 2010 and a Call for Participation (CFP) was issued. Despite not attracting a large response, a Kick Off Meeting (KOM) was held in October 2010. However, this was not effective and, although the participants made useful comments on the first draft TORs, there was no agreement to continue with the work as then proposed.

Following this, the TAC reconsidered the TORs and the need for the activity, including the interests of the SESAR Joint Undertaking (SJU) and the European Aviation Safety Agency (EASA). A second CFP was issued with slightly revised draft TORs and a second KOM was held in mid 2011. This attracted just sufficient interest to commence the work.

The draft TORs were adjusted by WG-91, as a result of slight rescoping of the original task. They were recommended by TAC to the EUROCAE Council and adopted in July 2012. The TORs are in Appendix D.

The current Report responds to Step 1 of the WG objectives as stated in the TORs.

1.3 STRUCTURE OF THE REPORT

The Report is structured in 2 volumes; Volume 1 being the main Report and Volume 2 containing some reference material.

Following this General section, which discusses the background, approach and history of WG-91, Volume 1 is structured around the main elements of the ED-78A process, namely the OSED, Operational Safety Assessment (OSA), Operational Performance Assessment (OPA) and Interoperability Assessment (Interop). In addition, sections on the Transition process to Operations and Certification have been included. The TORs called for assessment of Training related to ED-78A but time and effort constraints precluded more than a very cursory statement.

Chapter 10 provides the rationale for each category of recommendation (structured to facilitate further action as decided by EUROCAE); the allocation of recommendations to categories; and cross-reference to the detailed discussion regarding each recommendation.

Volume 2 of the Report consists of those items of reference material that are not publicly available.

1.4 HISTORY OF WG-91 ACTIVITIES AND METHOD OF WORKING

1.4.1 Team composition

After the Kick off meeting, the KOM attendees assigned various resources to the WG-91 group. The persons involved are listed in Appendix E. It was felt by the group that this membership gave a reasonably broad spectrum of attendees, but it was also noted that the attendees were always under time pressure from other activities, and although several requests were made to the KOM attendees, the amount of resources allocated by the KOM attendees did not increase through the time of the WG.

1.4.2 Meeting schedule

To reflect the availability and cost issues associated with WG activities, it was decided to conduct the WG activities principally by electronic means, and to hold face to face meetings only where necessary to collect and distribute coordination information.

The following meetings were held.

1st meeting (Kick Off Meeting) 6th – 7th June 2011 EUROCONTROL HQ

2nd meeting 29th-30th September 2011 EUROCONTROL HQ

3rd meeting 7th November 2011 WEBEX

4th meeting 28th – 29th November 2012 EASA Cologne

5th Meeting 31st January 2012 EURCONTROL HQ

6th meeting 24th February 2012 WEBEX

7th meeting 15th March 2012 WEBEX

8th meeting 26th March 2012 EASA Cologne

9th meeting 20th April 2012 WEBEX

10th meeting 10th & 11th May 2012 WEBEX

11th meeting 24th & 25th May 2012 WEBEX

12th meeting 26th June EUROCONTROL HQ

The work of the WG was conducted in the following main phases:

- An initial collection of comments, based on source documents (see 1.4.3)
- Identification and collation of issues (see 1.4.4).
- Expansion of issues and conclusions (see 1.4.5)
- Assembly into complete document and review of complete document

1.4.3 Review of Source and Reference documents

The principal input to the WG was on the basis of a collection of source documents that had been identified within the TORs. The WG also identified additional inputs at the KOM. The following specific documents were referred to by the WG. Documents which are not available in the public domain are included in Volume 2 of this report.

- Input 1 WG-78-SC-214_RevED-78A [12] (see Volume 2)
- Input 2 SC-214 – WG-78-11_FAA SPR issues_V1 [14] (see Volume 2)
- Input 3 Future ADS-B Standards Development Proposal [19] (See Volume 2)
- Input 4 SMPversion [15] 1.0
- Input 5 SESAR Safety Reference Material_v2.2 [16]
- Input 6 SL11 ED 78a V5-7sep 09 for TAC36 0 (see Volume 2)
- Input 7 WG-91 questionnaire v1 [17] (See Volume 2)
- Input 8 Safety Methodology in Compliance with RTCA DO-264 0 (See Volume 2)

Other documents consulted in the course of the development of this Report are termed reference documents and are listed in Appendix A.

The relevance of each item is summarised in brief form in Appendix B.

1.4.4 Identification and collation of issues

The reference documents were reviewed and, as a result, a collected set of identified issues was produced. This list was reviewed and expanded by the WG to ensure that the issues had been adequately described and understood.

At the same time, the issues were assigned to a set of groupings. These groupings were selected on the basis of the present contents of ED-78A. ED-78A is structured on the basis of a series of objective steps. In order to ensure that any new material would be usable against the existing ED-78A, the issues were aligned to the structure of ED-78A. They have been further developed into the Chapters of the current Report.

1.4.5 Expansion of issues and conclusions

The identified issues were then allocated to individuals on the WG. As the issues had been allocated to the structure of ED-78A, it was possible to identify particular members of the WG with the specific background that was appropriate to the particular area of ED-78A.

These individual were then tasked to produce individual issue papers based on the identified issues.

As these individual papers were developed, they were distributed to the members of the WG to ensure that the various members had adequate input to the papers, so ensuring that the implications of the conclusions reflected the widest possible breadth of input.

The individual papers generally take the following structure.

- Identification of issue – traced from the consolidated list of issues
- Re-statement of the issue;
- What ED-78A presently says about the issue;
- What ED-78A does not say about the issue;
- Identification of possible existing guidance that would help address the issue (from SPRs or other documents in the public domain)
- Discussion on possible guidance that can be given based on the developments in material since ED-78A was published.
- Identification of any present arrangements in place in other areas that are already addressing the issue
- Development of expanded explanation of consolidated issues: to identify difficulties, improvements, explanatory and other material suitable for guidance, and remaining difficulties.
- Conclusions and recommendations to EUROCAE on feasibility and means of addressing the issue.

The following individual papers were produced. Although the papers are incorporated in this report in later chapters, reference is provided here to identify the considerable efforts of the individual authors.

- General section (G Morton EUROCONTROL)
- OSED section (G Morton EUROCONTROL)
- OSA section (D Bunouf AIRBUS)
- OPA section (W Brondsema EUROCONTROL)
- Transition / Operation section (G Morton EUROCONTROL)
- Certification section (D Mancebo EASA)
- Consolidation of papers into this Report, together with supporting material in Appendices.

CHAPTER 2

GENERAL

This Chapter describes and explains issues identified by WG-91 that do not fall into the other areas of this Report.

2.1 INCREASING THE SCOPE OF CHANGES THAT ED-78A CAN ADDRESS

It was noted to the WG that the present scope of ED-78A addresses only '*Air Traffic Services Supported By Data Communications*'. Several applications had used the principles of ED-78A but outside this scope.

The WG noted that the scope of ED-78A was originally bounded by the group in which it was developed. There were no specific provisions in ED-78A that would prevent its use outside the original scope of application. However the WG noted that the ED-78A authors came primarily from the ATS Domain, and then predominantly from the Aircraft System certification and Ground ATM domains.

The WG noted that even within the scope of data communications, the lack of a regulatory framework addressing the 'communication service providers' had already indicated difficulties in obtaining input from this particular domain. The WG further noted that such difficulties also occurred with the inclusion of the MET and AIS domains. The WG further noted that the inclusion of Surveillance applications, such as ADS-C, had been successful, for example in ED-120 [20] and ED-122 [21].

The WG identified that ED-78A is oriented and specific to Data Link Aspects (for example the OPA focusing on RCP. ED-78A also concentrates on "multiple organizations" elements. This is obvious in data-link context but the concepts and organisations are less clear in other ATS domains, for example where multiple organizations may be involved in purely Ground applications). To expand the ED-78A more generic terms would be needed for the wider ATM context and would require definition of different domains). This would require additional suggestions. Not only for terms, but also for defining a generic context of development within multiple organizations, of different types: ANSP, AO, providers of support services or products.

It is noted that SESAR is one of the potential users of the WG-91 outcome and will probably have a wider scope of application (e.g. standards jointly developed with RTCA). The WG identified that increasing the scope to include ATS, CNS, AIS and MET would require coordination with other groups that would be outside the normal framework for EUROCAE. Therefore, the visibility of, use of, and involvement in the production of, a EUROCAE Document might be problematic to other domains.

The WG considered that the scope of applicability of ED-78A has been sufficiently described with ED-78A, and there are sufficient examples of how the scope had been successfully widened beyond ATS supported by Data Communications in a consensus manner by a number of users of ED-78A. The working group considered that it would be possible to use ED-78A as the basis for increasing the scope to ATS, CNS, AIS and MET. The WG considered that there was insufficient experience of use of ED-78A in other domains, particularly Aerodromes and Airspace Design to promote the use of ED-78A in these areas.

2.2 RECOMMENDATIONS

The WG recommends that EUROCAE should consider the production of an additional guidance document to address the following issues to capture the experience gained in the application of ED-78A;

[Rec 1](#) *Increasing the scope of changes that ED-78A can address to include ATS, CNS, AIS and MET. See section 2.1.*

The WG recommends that EUROCAE should consider the possibility of further activities to address the lack of existing guidance and existing experience for the following issues.

[Rec 2](#) *Increasing the scope of changes that ED-78A can address to Aerodromes and Airspace Design. See section 2.1.*

CHAPTER 3

OSED

This Chapter describes and explains issues identified by WG-91 in the area of the OSED.

3.1 LINKAGE OF OSED WITH 'OPERATIONAL USAGE'

It was noted to the WG by some of the EUROCAE groups that typical OSED generated during the application of ED-78A did not always equate to the full operational usage. In particular, the OSED only defined the new part of the system that was to be brought into use. As an example, the OSED for Data Link in the Oceanic Environment (ED-122) considered the use of various CPDLC services and was intended to be technology independent. The OSED did not consider the use of specific application technologies that would deliver this service, for example FANS 1/A+, ATN-B1 aircraft along side each other in the same airspace. The commenter noted that the use of multiple systems could introduce new hazards that were not considered in the ED-78A analysis. The description of the supporting system of the Data Link service should consider possibility of multiple sub-networks. The point to highlight when building an OSED is to attain the sufficient level of granularity in the breakdown of functions.

The WG felt that ED-78A is clear that the scope of the change being assessed is the responsibility of the user. It is therefore possible to include multiple systems in the scope of an assessment. However, in most cases the applications had been for single applications and systems.

However, it should be identified that wherever possible, the OSED and SPR should ensure that the boundary of the change and the boundaries of certified items are consistent, but that the OSED and SPR should not constrain the certified elements.

The main characteristics to highlight are that the change considered with ED-78A shall be

- o single,
- o complete,
- o realistic
- o implementable,
- o should identify the boundaries where mitigation means are to be shared between stakeholders.
- o Should be defined at a level sufficient for each individual stakeholder to identify its role in terms of functions and operations and relations with the other stakeholders.

It was noted to the WG by some of the EUROCAE groups, for example, the ADS-B groups, that these questions had also been asked, and the SPR produced by EUROCAE had been developed into Eurocontrol Preliminary Safety Cases that were intended to focus on the operational usage. However, the WG recognized that this approach was quite new, and there were a limited number of examples produced.

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was insufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. It would therefore be possible to produce additional guidance material based on present material.

3.2 LINKAGE OF OSED DESCRIPTIONS WITH ICAO (AND OTHER ORGANIZATIONS) SERVICE DESCRIPTIONS

It was noted to the WG that the system definitions in the OSED did not always directly equate to other definitions of operational requirements, services or capabilities. It was noted to the WG that the purpose of a new system was generally to give some form of operational capability that would fulfil the operational requirements of either ICAO, or maybe in the future, of other bodies, such as SES who would make use of Operational roadmap packages, CONOPS and Detailed Operational Descriptions etc.

However, the WG noted that in several EUROCAE SPR (note published docs called SPR often include the OSED as well), that relate to CNS changes, the relationship between the OSED and the associated ICAO Operational requirements had been made explicit, for example ED-120 chapter 2.2, ED-122 chapter 2.2, ED-175 chapter 2.2. For other EUROCAE SPR, the OSED is tied closely to the related ICAO provisions, for example ED-165 Section A4 [24].

The WG identified that certain EUROCAE working groups had already extended the ED-78A guidance by liaising with ICAO to allow ICAO to make use of EUROCAE material in the development of ICAO guidance and recommended practices. This liaison made use of existing ICAO standardisation structures. For example the ICAO Manual on the Required Communication Performance (DOC 9869 [25]) was based on the OPA determined in ED-120 and ED-122. Furthermore the message set from ED-120 and ED-122 was used in ICAO DOC 4444 [26].

The WG felt that this issue was sufficiently addressed for CNS, in ED-78A at present, and furthermore, there was sufficient evidence of how the issue had been successfully addressed in a consensus manner by a number of users of ED-78A. It would therefore be possible to produce additional guidance material, or pointers to the existing material, if felt necessary.

3.3 INTERACTIONS WITH OTHER SYSTEMS

It was noted to the WG that the OSED did not always identify the other systems that could be affected by the particular system under consideration, for example, for data link applications, the use of the data by other systems, such as the FMS was not identified. In the first applications, use of data was “by the crew”. This was then modified to become use “within the cockpit”. Clearly, here, if the concern is “internal” to one stakeholder (link FMS / ATSU equipments) and the level of requirements is sufficient for that stakeholder for the design, there is no need to continue the breakdown further in the OSED.

The WG identified that this issue was clearly within the scope of ED-78A, as the OSED should clearly identify the interfaces between systems and enable the owner of these systems to be identified.

However, the WG noted, that depending on the level of the system definition, this was not always possible. For example, an application that was only being defined at the service level, or the functional level would not be able to identify all the possible systems affected because such an OSED had not yet identified a physical description of how the functions would be implemented by the physical system. Another example is with a stakeholder who is a TSOA holder where the definition should be continued down to equipment level.

The WG identified several EUROCAE SPR, (for example ED-120 Chapter 2, ED-122 Chapter 3, ED-165 Figure 3.1 and ED-175 Figure 1-1), which attempted to describe the boundaries and interfaces of the system under consideration. The purpose of these sections is to define to the users of the document what interfaces had, and had not, been included.

The focus on ED-78A is for the coordinated requirements determination, so wherever possible the objective is to determine the owners of the systems affected. It is however recognised that the relationship between stakeholders and systems may not always be identifiable as there is not necessarily a one-to-one mapping-. With the increasing use of services, definition of boundaries has become more and more complicated.

The WG felt that the identification of which systems were within the scope of the OSED and the consequent analysis was clearly within the scope of ED-78A, and there were sufficient examples of how the issue had been successfully addressed in a consensus manner by a number of users of ED-78A. It would therefore be possible to produce additional guidance material, or pointers to the existing material.

3.4 PARTIAL IMPLEMENTATIONS

It was noted to the WG that for Data Link, the implemented systems did not always implement all the functionality included in the SPR. For example, ED-120 Figure 2-2 considers a number of ATS services that can be supported by Data Link. However, not all the services described in ED-120 are required by the European Commission Data Link Services Implementing Rule 29/2009 (DLS IR) [27]. The business case demonstrated that a limited set of DL services, to be used in the En-Route airspace, would give the best cost/benefits ratio for air and ground users. Consequently, the Programme wide and local safety cases that were produced, considered the 'DLS-IR' 29/2009 scope.

The WG considered that the relationship between the SPR and the necessary further safety work required for a physical implementation has not been sufficiently described with ED-78A, but this is line with the intentions of ED-78A which was written specifically to address the coordinated requirement coordination process, while providing pointers to other material necessary for the approval / certification process (see ED-78A chapter 2.2). There were however, sufficient examples of how the issue had been successfully addressed in a consensus manner by a number of users of ED-78A. It would therefore be possible to produce additional guidance material, or pointers to the existing material.

3.5 OSED MATURITY

It was noted to the WG that, before an SPR was conducted, the OSED should be mature. Maturity was suggested to include two concepts. The first one concerns the level of refinement and "granularity" in the breakdown of functions. Progress in this dimension is under control of the type of outcomes expected by the stakeholders. The second dimension concerns the description of the behaviour of the system out of its optimal/nominal states. Progress in this dimension is highly dependent of the iterations with OSA and OPA processes. The WG noted, in particular, that analysis at a functional level for example in ED-122 and ED-175, without the analysis of the corresponding physical implementation layer was not complete. The WG also noted that when the OSED was immature, the actual Operational Context was not sufficiently clear.

The WG noted that ED-78A already identified that the OSED and SPR stages were iterative, in that it would be expected that the SPR stages may result in the identification of additional limitations, particularly when a physical implementation is considered. However, this was only identified in later stages of the document i.e. E3.1, and earlier stages of the document, for example the overall process diagram in Figure 2.1 may not provide adequate emphasis on this point. The WG noted however that Figure 2.3 does show OSED iteration.

Although the OSED and SPR stages are considered separate, evidence of application shows that both are generally published at the same time. Furthermore, in one example, for ED-175 and ED-151 [23], specific difficulties were noted due to the fact that the OSED and SPR were different documents and at the time of the SPR development it was not possible to amend the OSED.

The WG considered that the maturity of the OSED, and consideration of when to start the SPR, has not been sufficiently described with ED-78A, and there were sufficient examples of how the issue had been successfully addressed in a consensus manner by a number of users of ED-78A. It would therefore be possible to produce additional guidance material, or pointers to the existing material.

3.6 OSED LEVEL OF ACCEPTANCE BY STAKEHOLDERS

It was noted to the WG that the OSED should have an agreed level of acceptance before starting the OSA-OPA stages. Here, acceptance can be understood as regard to some stability of the descriptions. It was noted to the WG that it was essential that the operational and the environment descriptions should be agreed before expending resources on the safety work that would then be wasted if the operational description and environments were changed. Acceptance was defined as including both the acceptance by the eventual users of the OSED as well as acceptance by the regulatory bodies, however, this implicitly assumes that OSED and SPR developments are two separate processes (and that there is no feedback from SPR to improve the OSED). This is not the case in practice. Furthermore, acceptance by the regulatory bodies might also require completeness and consistency.

The concept of 'user' acceptance is highlighted through ED-78A through the emphasis on the participation of the various 'domain' representatives. A EUROCAE document only appears with the active involvement of the various domains and only reaches a maturity with explicit acceptance by the domains that are represented at all stages of the EUROCAE working group and document acceptance process. This area was therefore felt to be adequately described in ED-78A.

The concept of regulatory 'approval' or acceptance of the OSED stage is not considered explicitly with ED-78A, which is focused on certification / approval of system elements. Furthermore, although the OSED and SPR stages are considered separate, evidence of application shows that both are often published at the same time.

The WG considered that the issue of explicit approval / acceptance of the OSED by regulatory organizations is not sufficiently described in ED-78A, but there were insufficient examples of how the issue had been successfully addressed in a consensus manner by a number of users of ED-78A. It was also felt that due to the iterative nature of the OSED – SPR activities, splitting the stages with an acceptance step would not be an effective approach. The WG recommends that the OSED should NOT be separately developed and accepted.

3.7 EMPHASIS ON CORE TEAM ACTIVITIES

It was noted to the WG that certain parts of ED-78A relied on the involvement of a cross domain core team of representatives. A particular concern identified to the WG was that certain of this core team would not be available.

The WG identified the statement in ED-78A: "All potential applicants including the operators, A/C modifiers, system integrators, equipment designers, ATS providers, communications service providers, and approval authorities are involved in the OSEIC". Clearly, this is specific to Data Link but can reasonably be updated to include other domains, such as those involved with airport operations, surveillance applications etc. Examples include ED-165 Fig 3-1, ED-163 Fig 1 [28].

The WG considered that this is the essential emphasis of ED-78A, which is not intended to be a process for the entire safety and interoperability process, but is focused on the part of the development process requiring coordinated requirement definition. ED-78A emphasizes this at many points, 1.3.1.1, which talks about coordinated requirements determination, 1.3.2.2, which talks about coordination of objectives to requirements, 1.3.2.3, which talks about the interoperability between domains and Fig 1-4 which shows the handover of SPR requirements to the individual domains.

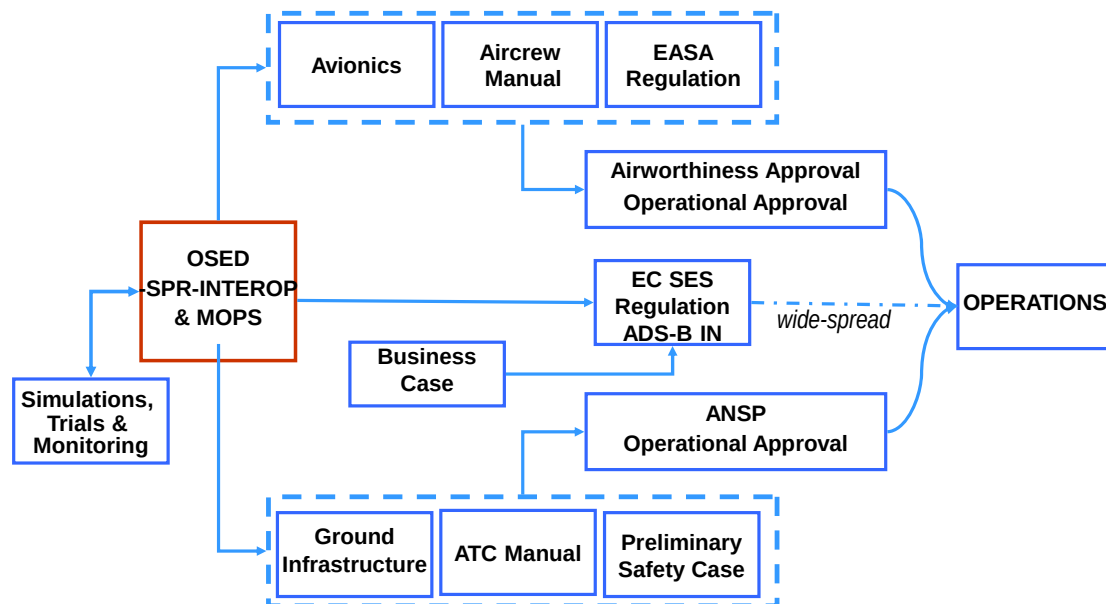
The expectation of the authors of ED-78A was to produce a document that only addresses those situations where coordination is necessary; to derive requirements that can then be used by the individual domain and the 'certification'/ approval processes used within those domains. ED-78A processes therefore depend entirely on the core team involvement.

The WG considered that the issue of emphasizing the core team – coordinated – aspect of ED-78A has been sufficiently described in ED-78A. There were sufficient examples available that would allow more guidance to be issued on the possible members of the core team. It would therefore be possible to produce additional guidance material to illustrate members of the core team, but would not be possible to give guidance on how the SPR should progress in the absence of the core team.

3.8 RELATIONSHIP OF OSED – SPR – INTEROP WITH OTHER EUROCAE MATERIAL MOPS ETC

It was noted to the WG that the certification and approval frameworks are focused on the system elements and many SPR are focused on the new functionality under consideration. It was noted to the WG that there was insufficient guidance on how to produce the certification / approval material for these system elements, taking proper consideration of the various SPR generated that might affect the system. See also section 8.2.

The WG identified that certain EUROCAE working groups had already extended the guidance presently available in ED-78A on the linkages between such documentation. For example, WG-51/SC-186 indicated the relationships schematically in the diagram below [29].



ADS-B applications: from Standardisation to Operations

FIGURE 1: RELATIONSHIP BETWEEN SPR AND OTHER REGULATORY DOCUMENTS

The WG considered that the issue of relating ED-78A documents for OSED etc with certification material has not been sufficiently described with ED-78A, but there were sufficient examples of how the issue had been successfully addressed in a consensus manner by a number of users of ED-78A. It would therefore be possible to produce additional guidance material.

3.9 DEFINITION OF SAFETY TARGETS WITHIN THE OSED STAGE

It was noted to the WG that if Safety Targets could be defined within ED-78A, and furthermore, defined at OSED stage, it may be possible to define a consistent Safety Target for all applications. See also section 4.6.

The WG felt that the issue of setting and harmonizing safety targets was outside the scope of ED-78A, which appears to be the position of the original authors of ED-78A. ED-78A goes no further than the consensus position available at the time of publication in using the idea of a risk based approach to defining safety objective bands of a qualitative nature.

The WG felt that there are various other groups that are also addressing this issue, such as EASA rulemaking groups and SESAR Joint Undertaking through the SESAR Safety Reference Material, and it would be inappropriate to address this issue specifically within ED-78A.

The WG considered that the issue of setting safety targets within ED-78A has not been sufficiently described in ED-78A, but there were insufficient examples of how the issue had been successfully addressed in a consensus manner by a number of users of ED-78A. It was also felt that there are other groups already looking at this issue, for example the SJU SRM, EASA Safety Assessment Task Force¹ (SATF) [31] and FAA SMS Manual. The WG would therefore not recommend the production of additional guidance material, or pointers to the existing material.

3.10 GUIDANCE ON COLLECTION OF ENVIRONMENTAL CHARACTERISTICS

It was noted to the WG that the OSED was intended to identify the essential environmental characteristics that would be necessary during the SPR stage. The following specific aspects were noted to the WG; the first, on how to ensure that the essential traffic characteristics were collected, secondly, how to provide a set of environmental characteristics that sufficiently captured the largest sub set of implementation scenarios and, thirdly, how to ensure that the environmental characteristics were correctly captured.

The WG identified various EUROCAE documents in which the essential characteristics of environment considerations had been developed, and also identified some mechanisms, such as integration task forces (from ADS-B work) which are presently in use to agree sets of environment criteria. Various EUROCAE documents also identified methods of capturing Environmental requirements, (for example ED-165 Section A-5; ED-122 Section 2.3 and ED-120 – Chapter 3).

The WG identified that description of information to be collected in the OSED relating to environmental characteristics is limited to section C3.2, which is primarily focused on Data Link and has been considerably expanded by application of ED-78A.

The WG considered that the collection of environmental characteristics has not been sufficiently described in ED-78A, but there are sufficient examples of how the issue had been successfully addressed in a consensus manner by a number of users of ED-78A. It would therefore be possible to produce additional guidance material, or pointers to the existing material.

3.11 NEW SYSTEMS THAT REMOVE EXISTING FUNCTIONALITY

It was noted to the WG that some intended new systems were designed to replace, rather than augment existing systems. It was noted that the present description of the OSED did not account for the possibility that the removal of existing systems might remove some functionality which the new system did not explicitly intend to replace. No specific examples were given, but examples considered might include the replacement of ILS with MLS, which would mean that back beam guidance was no longer available².

¹ The SATF was part of EASA Rule Making Task ATM.001 and ATM.004 and continues under EASA Rule Making Task 0469 and 0470

² In some countries, an ILS localizer is used to provide a 'back beam' radiation pattern that facilitates take off guidance for aircraft. Although an MLS is intended to replicate ILS functionality, the 'back beam' pattern is not available.

The WG felt that this was a usual limitation of the safety approach taken in determination of the scope of the change; the SPR is only intended to argue for the safety of the new functionality in the system and is not a safety argument for the entire system. An emphasis must be put on the objective of safety of the change to identify all the functionality affected.

The WG considered that ED-78A did not provide any guidance on the identification of functions removed when a new system is assessed, but that the addition of this point would be possible when discussing the scope of the OSED.

3.12

SUMMARY OF OSED SECTION

The WG recommends that EUROCAE should consider the production of an additional guidance document to address the following issues to capture the experience gained in the application of ED-78A;

- [Rec 3](#) To provide pointers to existing material relating the OSED to ICAO Operational Requirements and service descriptions. See sections 3.1 Linkage of OSED with 'Operational usage', 3.2 Linkage of OSED descriptions with ICAO (and other organizations) service descriptions.
 - [Rec 4](#) To provide pointers to existing material relating to defining Environmental Characteristics. See sections 3.10 Guidance on collection of environmental characteristics.
 - [Rec 5](#) To provide pointers to existing material relating to defining Operational Descriptions to account for service level, functional or physical implementations at a granularity level commensurate with stakeholders needs. See section 3.3 Interactions with other systems.
 - [Rec 6](#) To provide pointers to existing material to aid in the definition of the boundaries of the Operational System under consideration to reinforce the consideration and identification of what is not included in the OSED analysis. See sections 3.4 Partial implementations, 3.11 New systems that remove existing functionality.
 - [Rec 7](#) To provide pointers to existing material relating defining the actors to be part of the SPR See sections 3.7 Emphasis on core team activities.
 - [Rec 8](#) To provide pointers to existing material defining the relationship between OSED, SPR and Interop to certification material. See sections 3.5 OSED maturity, 3.6 OSED level of acceptance by stakeholders, 3.8 Relationship of OSED – SPR – Interop with other EUROCAE material MOPS etc .
 - [Rec 9](#) To provide pointers to existing material reinforcing that ED-78A is only for the coordinated requirement definition stage. See sections on 3.7 Emphasis on core team activities
 - [Rec 10](#) To provide pointers to existing material reinforcing the iterative nature of the OSED – SPR step. See sections on 3.6 OSED level of acceptance by stakeholders, 3.5 OSED maturity.
- The WG recommends that EUROCAE should consider the possibility of further activities to address the lack of existing guidance and existing experience for the following issues.
- [Rec 11](#) To provide guidance on the conduct of an SPR without all members of the 'core team' available. See section on 3.7 Emphasis on core team activities.

CHAPTER 4

OSA

This Chapter describes and explains issues identified by WG-91 in the area of the OSA (Operational Safety Assessment).

4.1 ITERATION OF OSA AND OSED.

It was noted by the WG that the OHA needs to have the OSED (a first working version) as an input that is not always “on time” available. See also CHAPTER 3.

Additional guidance could describe the iterative process between OHA and OSED to produce initial (or interim) version of the SPR. Then the SPR will be consolidated for its official issue.

Based on the first version of the OSED, the Functional Breakdown consists in decomposing the top level function/operation in main sub-functionalities that are assessed in non-nominal modes (with each potential failure mode assessed along with the mitigations) and analyzed to determine the associated effects. Each sub-functionality may be also subdivided but the level of granularity is to be defined depending on the SPR project based on the need of the stakeholders.

The results of the OHA can then provide a first list of operational hazards that will be used to validate or to improve the OSED through the description of necessary functional and operational mitigations of the hazards, as part of the maturity process of the OSED.

Hazards shall be identified at an appropriate level (operational, logical or physical level) that ensures all stakeholders share a common risk picture of the proposed change. The appropriate level is one that allows a coordinated sharing of the risk between stakeholders. This might generally correspond to the operational level. This guidance can include the methods and experience used by present stakeholders.

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, although there was insufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A, the WG could identify additional guidance. It would therefore be possible to produce additional guidance material based on present material.

4.2 DEPTH OF OSA

OSA are always end-to-end assessments, so SOs and SRs should be specified to Aircraft, AO, ATSP and other providers. This means that the ASOR must possess the minimum quality and granularity level ensuring that meaningful SOs and SRs can be derived.

The granularity level also depends on the fact that certain CNS/ATM system elements may be already in operation, requiring some more refinement in specification (e.g.: for INTEROP purposes). See for example 4DTRAD extensions to LINK2000+.

Preliminary checks (on prototypes, through trials or evaluations) for achievability of Safety Objectives and the safety requirements identified by the chosen risk mitigation can be conducted, for example, using bottom-up verification (and validation Iterative process) of basic causes.

The Users of ED-78A questioned how far in the system decomposition the allocation of safety performance requirements should go. The WG felt that OSA should then consider the stakeholder interface level only and the implementation will have to be considered in each involved domain.

The boundaries of safety assessment should be clearly defined in terms of systems, operations or procedures that are potentially impacted by the change and that are to be put under scrutiny by the assessment process.

Granularity level per domain will depend on the project (new technology, linked or not with existing MOPS or MASPS or new Operation).

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was sufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. It would therefore be possible to produce additional guidance material based on present material.

4.3 COMPLETENESS AND ADEQUACY OF HAZARD IDENTIFICATION AND CLASSIFICATION

It was noted to the WG that guidance is requested on how to ensure investigation of hazards and effects is correct and complete. This may include the case of determination of the probability of occurrence of effects once the hazard occurs, when relevant (i.e.: when in combination with some external events).

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was insufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. It would therefore not be possible to produce additional guidance material based on present material.

4.4 NECESSARY INFORMATION REQUIRED IN SPR

A need is expressed to how the SPR identified the necessary information that will allow each domain to perform their local safety analysis in relation to the applicable regulation. Note that CS 25.1309 (and associated AMC 25.1309) is the applicable regulation to Airborne domain. ANSPs are required to perform a local safety case in accordance with EC REG 1035/2011. For both aircraft and ground domain the basis for compliance is the published international SPR standard.

The WG identified that inclusion of guidance on the inclusion in the SPR of the necessary information to allow the domains to determine design assurance levels (DAL) at Functional/Domain level is missing in the current ED-78A. Safety qualitative assessment should include Assurance level allocation, considering independence and dissimilarity principle. See also section 8.9.

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, although there was insufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A, the WG could identify the necessary guidance. It would therefore be possible to produce additional guidance material based on present material

4.5 SEVERITY CLASSIFICATION SCHEME: TABLE 4-1 OF ED-78A

For the severity classifications, it was noted to the WG to consider:

- EC REG 1035-2011 and CS 25.1309 definitions as that present ranking for effect on operations, occupants and air crew all come directly from CS 25.1309.
- That the ANSP severity classification has been revised in CR 1035 Annex II paragraph 3.2.4 since the publication of ED-78A.
- EUROCONTROL-SAM provides a scheme for effects on the ATM system operations (controllers, flight crew, airborne and ground system), while taking into account severity indicators. In practice, each time a combination of causes occurs that may lead to a hazard, then not always the hazard will develop as in reality some internal or external mitigation means (IMM/EMM) may prevent or reduce the effects of the hazard. It is noted that this possible solution is part of the SAM and applied in some of the published EDs and DOs.

- Once the classification of all effects of the Operational Hazard is established, then the worst credible effect can be determined. The safety objective associated with the worst credible effect is used as basis for deriving the safety requirements. SAM also explicitly allows other approaches, i.e. to establish safety objectives for all effects of a hazard and then pick the most stringent one. It is to be noted that some concerns regarding the worst credible effect notion are overcome with ARP4754 safety approach which is presently used within the aircraft domain.

The WG felt that this issue was incorrectly addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was sufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. It would therefore be possible to produce additional guidance material based on present material.

4.6

TOLERABILITY OF RISK WITHIN ED-78A

It is noted that current figure 4-1 in ED-78A Safety Objective (SO)/Severity Class (SC) relationship is directly issued from CS25.1309 guidance, which describes the safety assessment process of aircraft systems and is considered as regulatory document for the airborne domain. No equivalent regulatory document exists for ground domain although ED-125 has been used in practice.

The qualitative combined SO/SC values are used as a risk matrix to determine whether the combined SO/SC result for the hazard concerned is at acceptable or unacceptable level of risk.

However, due to the safety evolutions that have taken place in the last decade, it is noted that the current Figure 4-1 is not sufficient.

Therefore, guidance on the development of a qualitative Risk Classification Scheme (RCS) has been developed in SAM (FHA Chapter 3 Guidance E) and ED-125 at the overall ATM level (called safety targets) for all five severity classifications. Similar RCSs have been defined in the FAA SMS.

With this method of RCS elaboration each RFG group has to define its own ad-hoc RCS based on compliance with these overall RCS.

Despite these initiatives, it is acknowledged that a widely acceptable and practical RCS to be commonly applied by ANSPs and airframe/avionics manufacturers and in standardisation bodies remains a difficult undertaking. It is to be noted that FAA SMS solution allows a "common RCS".

It is understood that discussions around the establishment and use of a quantitative RCS are ongoing in various groups (e.g. EASA task force and SESAR-SRM). To date no final solution has been agreed.

The WG felt that this issue was incorrectly addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was insufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. It would therefore not be possible to produce additional guidance material based on present material.

4.7 ALLOCATION OF SAFETY OBJECTIVE AND REQUIREMENT (QUALITATIVE AND QUANTITATIVE ASPECTS)

It was noted to the WG that there is also the need for clear guidance concerning the allocation of the safety objectives to each involved contributor (domain).

Allocation of SOs, using Fault trees, has been successfully applied in published EDs/DOs for ADS-B and AIS/MET applications. A similar technique is being applied by WG-78/SC-214 for the SPR on data communications.

In addition, the following methods have been noted as methods of deriving safety objectives although the WG noted that there is no consensus on their use across all domains:

- by use of a functional / logical model of services involved
- by use of an Accident / Incident model using barriers (such as the SJU SRM)
- by use of a relative performance approach (such as that used by EUROCONTROL CASCADE in ADS-B-NRA, ADS-B-RAD ADS-B-APT and ATSA-VSA Preliminary Safety Cases [32], [33], [34] and associated EUROCAE ED-160 [30], ED-161 [35], ED-163 [28].

It was also noted to the WG that ED-78A provides only qualitative safety objectives.

The WG felt that this issue was incorrectly addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was insufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. It was also felt that there are other groups already looking at this issue, for example the SJU SRM, EASA SATF and FAA SMS Manual. It would therefore not be appropriate at this time to produce additional guidance material based on present material.

4.8 HUMAN ERROR CONTRIBUTION

The WG noted that this issue relates to both the OPA and OSA parts of the analysis.

It was noted to the WG that the OPA developed by WG-76 allocates performance requirements between technical systems and human. Accounting for the human part was one of the most contentious issues in WG-76. At present the RCP concept does not give guidance on the particular elements included.

It was noted to the WG that there is a need for guidance on how to consider “human error contribution to the hazards” for each domain and to provide the necessary assurance for humans and procedures. It was noted by the WG that CS25.1302 applicable to airborne requires this for flight crew and aircraft procedures and that guidance material (AMC 25.1302) is available.

It is noted that various EUROCAE/RTCA SPR publications on the standardization of ADS-B applications exist (e.g. ED-160 (ATSA-VSA); ED-195 (ASPA-FIM) [36]) that applied human error contribution and derived qualitative human safety requirements based on the human error contribution for ground and aircraft domain. It also provides background material and evaluations around the topic of human errors.

The interim draft SPR material from WG-78/SC-214 uses the same background material for the appliance of human error contributions for the aircraft and ground domain.

The WG noted however that the issue of using ‘Human error rate’ is contentious in some parts of the ATM Domain. Although used in various ways in various documents, the WG indicated that there is no consensus agreement on the approaches used.

Reference for controllers:

Human Reliability Assessment (CARA) Development for EUROCONTROL; Q07/22268NC – Deliverable D1-1: Technical Basis; Gibson; September 2008 [37];

CARA User Manual, v1.3; Kilner, Gibson; March 2010 [38].

Reference for flight crew:

System Safety for the 21 Century, Richard A. Stephans [39].

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was insufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A for pilots and controllers. It would therefore not be possible to produce additional guidance material based on present material.

4.9 FORMAT OF OUTPUT EVIDENCE

It was noted to the WG that as a number of OSED, SPR and Interop have to be provided by EUROCAE/RTCA committee developing the international SPR standard documents and by SESAR groups for the development of the prototype systems in support of validation.

Examples are:

- ED-160 (Safety, Performance and Interoperability Requirements Document for Enhanced Visual Separation on Approach;
- ED-159 (Safety, Performance and Interoperability Requirements Document for ATSA-ITP) [40]

The ED-160 and ED-159 documents cover OSED + OPA + OSA + INTEROP, while the following two documents only contain OSED + OPA + OSA.

The INTEROP material associated with these SPRs is published in separate documents, ED-100A [[41], ED-110B [42] respectively.

- ED-122 (Safety, Performance Standard for Air Traffic Data Link Services in Oceanic/Remote airspace)
- ED-120 (Safety, Performance Standard for Air Traffic Data Link Services in Continental airspace)

Note that experience has shown that most published material is OSED + SPR. The Interoperability is published as a separate document.

It was noted that guidance material could be updated on the basis of the experience found in these publications.

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was sufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. It would therefore be possible to produce additional guidance material based on present material.

4.10 ITERATIVE PROCESS FOR THE SPR DOCUMENT

It was noted to the WG that there should be a process to refine the safety objective and risk mitigation in case of deviation to the requirement provided by the first issue of the SPR.

ED-78A, in its focus on the coordinated requirement coordination is clear that the derived requirements should be verified and validated by the core team. (See 4.1.2.2 of ED-78A) The WG noted that this could be achieved by the Validation loop during the development of the SPR document.

Trials step results can help to complete the final assessment of the objectives/requirements that will be allocated to each domain, before publishing the SPR as official document.

This process can also be used when an individual domain cannot meet the SPR requirement and requires a rebalancing. Such problems may be solved by rebalancing (this step is done during the Validation of the SPR document) OR redesign (when the requirement is not met).

However, when the SPR is issued, there is no “SPR or Operation Owner” and each domain has to negotiate the acceptability of any deviation with his supervisory authority.

It was noted that guidance could be given on how an update of the next release of a standard document should be issued (e.g. ED-100 vs. ED-100A or by issuing a change to the existing document (ED-120, change 1 and change 2) and what determines the difference in publication.

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was sufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. It would therefore be possible to produce additional guidance material based on present material.

4.11 IDENTIFIED SOURCES OF GUIDANCE MATERIAL

The WG, in the production of this Chapter, has identified the following candidate material to address the issues highlighted. The WG does not mean to indicate that all the material contained in these references is recommended for inclusion in updated guidance material. In some cases the WG has identified which particular issue could be addressed by the reference material.

TABLE 1: INDICATION OF WHICH REFERENCE DOCUMENTS ADDRESS WHICH ISSUES

	Airborne Framework				ATM Framework		
	ARP 4761	ARP 4754	AMC 1309	AMC 1302	SAM, SAME SRM	ED-125	CARA
(1) Clear definition (OSD) (Para 4.1)		X	X		X		
(2) Functional breakdown (Para 4.1)	X	X			X		
(3) Severity (Para 4.5)		X	X	X criticality	X	X	
(4) Risk (RCS) (Para 4.6)			X		X	X	
(5) Safety Objectives (Para 4.7)	X	X	X		X	X	
(6) Human Error (Para 4.8)				X qualitative			X quantitative
(7) Evidence (Para 4.9)					X		
(8) Iterative Process (Para 4.10)		X			X		

4.12 SUMMARY OF OSA SECTION

The WG recommends that EUROCAE should consider the inclusion of additional guidance within an updated ED-78A to address the following issues to capture the experience gained in the application of ED-78A;

[Rec 12](#) Updated definition of severities. See section 4.5 Severity classification scheme: Table 4-1 of ED-78A.

The WG recommends that EUROCAE should consider the production of an additional guidance document to address the following issues to capture the experience gained in the application of ED-78A;

[Rec 13](#) Guidance to allow the SPR to be used for domain approval processes. See section 4.4 Necessary Information Required In SPR.

[Rec 14](#) Guidance on the iterative process between the OSD and OSA. See section 4.1 Iteration of OSA and OSD.

- [Rec 15](#) *Format of output evidence. See section 4.9 Format of Output evidence.*
- [Rec 16](#) *Guidance on how to update an SPR. See section 4.10 Iterative process for the SPR document*
- [Rec 17](#) *Iteration of OSA and OSED to identify common hazard definitions. See section 4.1 Iteration of OSA and OSED.*
- [Rec 18](#) *Guidance on the level of system decomposition in the OSA. See section 4.2 Depth of OSA.*

The WG recommends that EUROCAE should consider the possibility of further activities to address the lack of existing guidance and existing experience for the following issues.

- [Rec 19](#) *Guidance on completeness of hazard identification and adequacy of severity classification. See section 4.3 Completeness and adequacy of hazard identification and classification.*
- [Rec 20](#) *Development of a common Risk Classification scheme. See section 4.6 Tolerability of Risk within ED-78A.*
- [Rec 21](#) *Allocation of Safety Objectives and derivation of safety requirements. See section 4.7 Allocation of safety objective and requirement (qualitative and quantitative aspects).*
- [Rec 22](#) *Guidance on Human Error aspects in risk mitigation. See section 4.8 Human error Contribution.*

CHAPTER 5

OPA

This Chapter describes and explains issues identified by WG-91 in the area of the OPA.

5.1 NEEDS TO BE LINKED TO EXISTING STANDARDS

It was noted that the OPA needs to be linked to other standards to provide assurance that such standards are being complied with. Particular examples noted include ICAO RCP, RNP, RSP etc and the Eurocontrol Surveillance standard.

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was sufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. It would therefore be possible to produce additional guidance material based on present material.

5.2 IS OPA NOW PART OF SAFETY ASSESSMENT?

It was noted by the WG that the separate concept of the OPA has now been included within the scope of safety assessment, for the SAME Broader approach, the SJU SRM 'success' approach (figure 5 of input 5) and within the early work of the EASA SATF rulemaking task. The OPA task is now more commonly considered part of the safety assessment of 'normal' operations.

It was also noted by the WG that the aspects of hazard identification, setting of safety requirements, and derivation of safety requirements were now accepted to be common to both OPA and OSA considerations.

Historically, safety assessments have been limited to an examination of internal system failures. They have tended to assess how reliable the ATM system needs to be to ensure that the system is adequately protected against internal failures. This restricted view of safety has been sufficient since ATM systems have gradually evolved and it has been adequate to rely on the assumption that the ATM system is intrinsically safe when no failure occurs. Given the radical nature of SESAR concepts, the development of new technologies and the increasing use of automation, this assumption is no longer valid.

The SESAR safety methodology continues to require that safety assessments examine internal system failures (termed "failure based approach") but additionally requires the consideration of the "success based approach". The success based approach determines the functionality and performance needed to be incorporated into the design to ensure that when the system is working as intended it is able to provide the necessary safety benefit. Furthermore even an extremely small deterioration in ATM functionality and performance could have an effect on this safety benefit. Therefore, it is clear that ATM safety assessment needs a success approach as well as the current, failure approach. The SRM document presents a broader approach to safety assessment that is based on success/failure rather than only concentrating upon failures. In essence, it is a far more integrated approach that combines the safety aspects of the OPA and OSA into the safety assessment framework

The WG noted that there was insufficient consensus at present on this issue. However the WG also noted that SAME, that extends Safety Assessment to the 'success' approach, has been approved by the EUROCONTROL Safety Team. Furthermore the SRM has been accepted by the SJU for cross domain activities.

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was insufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. It would therefore not be possible to produce additional guidance material based on present material.

5.3 ACCEPTABILITY OF OPA CLAIMS

It was further noted that the RCP has been accepted by WG-76 because nothing better could be identified, and it was felt necessary to comply with the TORs to produce the SPR. This acceptance was also made with other reservations, notably when considering text like "*an RCP is specified ... for a given region...*". The question arose as to whether there was sufficient evidence that this claim represented an argument for the acceptability of the RCP in the OPA. Furthermore, sentences like "*the RCP is independent of the technology used and applicable to voice and data communications*" raises the issue of having the same figures for both voice and data. The OPA was conducted separately from the OSA and the RCP value derived on the basis of expert judgment. See Annex C of ED-175 0.

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was insufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. It would therefore not be possible to produce additional guidance material based on present material.

5.4 OPA GUIDANCE ON USE OF RCP CONCEPT

ED-78A provides OPA guidance on how performance requirements should be based on the RCP concept from the OSED for CDPLC services. This guidance was based on the existing scope of ED-78A. In this concept, an RCP specification is specified in terms of Availability, Integrity, Continuity and Time parameters that are needed to define the performance of the CPDLC transactions. Present material can be found at ED-78A, section 2.2.3 and 4.1.3, Annex C/Para 3.1.5, C3.2.2 and Annex F – OPA guidance

Since ED-78A was published, for Continental CPDLC operations, ED120/DO290 (Continental SPR standard) has been developed (published in May 2004) and is used as compliance reference for the EC Implementing Rule 29/2009. For Oceanic/Remote ADS-C and CPDLC operations, ED-122/DO-306 (Oceanic SPR standard) is used as compliance reference for air-and ground implementers.

For both of these documents, the methodology to establish performance requirements used the OPA section of ED-78A.

However, since the publication of these SPR standards, further advances, and lessons learnt from LINK2000+ and Oceanic operations have taken place.

The further improvements are being applied by EUROCAE WG-78/RTCA SC-214 in their SPR development for the next generation data link (SESAR/NEXTGEN) and are discussed in the following items

5.4.1 New performance specification

ED-78A limits the performance specifications to Required Communications Performance (RCP) for the Controller–Pilot Data link Communications application (CPDLC). At the time of ED-78A development, the Required Surveillance Performance (RSP) was not mature and thus excluded from the document (see section 1.2 - Scope). However, ED-78A has since been used for surveillance services and flight information services and thus requires specifications for surveillance and FIS performance. ICAO/OPLINKP is working on an update of ICAO Doc 9869 - Manual on Required Communications performance (RCP).

The surveillance services are obtained through the Automatic Dependent Surveillance-Contracted (ADS-C) application. The flight information services are obtained through the Data-link Flight Information Services (D-FIS) application. The surveillance services make use of the RSP (Required Surveillance Performance) concept. This concept has been applied within ED-122/DO-306 to specify ADS-C based performance. The flight information services will make use of the RIP (Required Information Performance) concept. For RIP, discussions are ongoing within WG-78/SC-214 and ICAO whether Flight Information services should have a performance specification or not.

With the future of NextGen (USA) / SESAR – 4D Trajectory Based Operations (4DTBO) and other Continental data communication plans, the draft 'WG-78/SC-214' SPR incorporates the RSP specifications for Trajectory based operations and other ATC Communications (e.g. provision of MET data, air – or ground speed, etc...).

In addition, the draft 'WG-78/SC-214' SPR includes the Required Information service Performance (RIP) in support of D-OTIS (ATIS, VOLMET, NOTAM), D-RVR and D-HZWX (SAR, SIGMET) services.

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was sufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. It would therefore be possible to produce additional guidance material based on present material. It was considered by the WG that RSP and RIP concept should become part of ED-78A.

5.4.2 New Guidance on Performance Parameters

The RCP/RSP/RIP performance parameters, used for CPDLC, ADS-C and FIS applications, are expressed by Time, Continuity, Availability and Integrity.

Experience in ED-120 and ED-122 indicated that the definitions of these should be clarified.

5.4.2.1 Uplink expiration Time

Timing should contain the 99% value rather than the timing associated with the expiration time. The expiration time should be derived in the OSA as the time-out of particular transactions (e.g. clearance expiration time as used as in some Data Link applications for CPDLC) means that an abnormal state has occurred. And as one example, a consequent safety requirement would become that the controller gets an indication that the transaction has become operationally invalid and that he should return to alternative procedures.

5.4.2.2 Verification and demonstration of timing performance

It is common engineering practice to address time performance by 2 engineering values: 99% and 95%. The 99% operations are stretched operations, while 95% operations are considered nominal operations.

5.4.2.3 Availability RCP

The Availability RCP is in fact for a single aircraft and so is best labelled as A^{AIRCRAFT}.

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was sufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. It would therefore be possible to produce additional guidance material based on present material.

5.4.2.4 Determining Continuity and Availability

The concept of QOPL_{UIT} (Quantitative Operational Performance Level) and QOPL_{LOS} could be removed as they were neither used in the WG-78/SC-214 work nor in the ED-122/DO-306 (Oceanic SPR). Simply deriving Availability and Continuity has proved sufficient.

5.4.2.5 Allocation of time:

The end-to-end time must be allocated to the elements, being part of the end-to-end chain as the derived performance requirements are used as basis for service level agreements between CSP, ATSP and AO.

ED-78A (Annex F) applies an arithmetic sum for budgeting the RCTP timing to the aircraft system, CSP and ATSU. This approach has been shown to be simplistic as technical and human delays are independent and specifying delays, using an arithmetic sum, produce unnecessarily stringent requirements to the technical elements and humans.

Statistical analysis from Oceanic and Continental CPDLC operations (LINK2000+) shows that technical/human delays behave according to a statistical distribution curve, for example Exponential or 'Burr' distributions.

The time allocations should be described according to the statistical approach.

Note that validations in WG-78/SC-214 are currently being carried out to verify which statistical approach fits best with the statistical data collected from CPDLC operations.

5.4.2.6 **Aircraft time**

The WG felt that ED-78A should be updated to mention that it is desirable for the airborne element of the total system end to end time to be a standardised value for RCP, RSP and RIP concepts and that the aircraft time element should be independent from the airspace. However, it does not mean that the aircraft time must be the same for RCP, RSP and RIP.

5.4.2.7 **ACSP (Aeronautical Communication Service Provider) time**

The WG felt that ED-78A should be updated to capture experience in the allocation of ACSP times that shows they are mainly determined by the typical technologies used in different airspaces. For example Continental Data Link operations use line-in-sight systems, while in Oceanic airspace the technology used is the much slower SATCOM.

ED-78A Annex F provides detailed information that should be updated on the basis of the applications made by WG-78/SC-214 SPR standardisation work. For example, RCP/RSP/RIP specifications are denoted in multiplications of 60 (i.e. RCP120, RSP180, etc). Moreover, for reasons of manageability by end-users and certification authorities, the number of RCP, RSP, and RIP specifications should be limited to no more than three (e.g. RCP120/RCP240/RCP400). And these RCP should be associated with defined Operational Environments (see ED-175 C4 page 150 for illustration).

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was sufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. It would therefore be possible to produce additional guidance material based on present material.

5.5 **OPA LINKAGE WITH OSA**

The document makes the linkage with safety through QSPL (Quantitative Safety Performance Level) parameters. However, as QSPL is not used in practice, the OSA linkage needs to be updated.

5.5.1 **Continuity**

ED-78A should be updated to indicate that the Continuity figure which is linked with the expiration time should be derived within the OSA as it denotes an abnormal case. For an illustration, see the formula derived in ED-175 C.4.1.2 page 152). In practice, the 99.9% continuity is associated with the expiration time value.

Extra guidance can be included in ED-78A to show that published SPRs (ED-120, ED-122) as well as the WG-78/SC-214 SPR draft specifies a functional safety requirement that the controller needs to be alerted when the transaction has become operationally invalid (Timer expires as this represents the moment at which the transaction has become operationally invalid).

5.5.2 **Availability**

The present guidance in ED-78A can be updated as the Availability parameter is driven from efficiency and safety perspective. For illustration see the formula used in ED-175 C.4.1.3 page 153). However, the linkage does not need to use $QOPL_{LOS}$ and $QSPL_{LOS}$.

This is true for availability of service provision (ATSU and ACSP) and Availability of aircraft.

5.5.3 Integrity

The present guidance in ED-78A could be updated as there is no notion of integrity used in OPA. Such criteria are only derived from the OSA.

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was sufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. It would therefore be possible to produce additional guidance material based on present material.

5.6 SUMMARY OF OPA SECTION

The WG recommends that EUROCAE should consider the inclusion of additional guidance within an updated ED-78A to address the following issues to capture the experience gained in the application of ED-78A;

[Rec 23](#) *New performance specifications of RSP and RIP (Required Information Performance). See section 5.4.1 New performance specification.*

[Rec 24](#) *New guidance on the definition and specification of OPA parameters. See sections 5.4.2 New Guidance on Performance Parameters and 5.5 OPA Linkage with OSA*

The WG recommends that EUROCAE should consider the production of an additional guidance document to address the following issues to capture the experience gained in the application of ED-78A and allow the use of ED-78A beyond its present scope of application;

[Rec 25](#) *Linking of OPA to existing national and international standards. See section 5.1 Needs to be linked to existing standards*

The WG recommends that EUROCAE should consider the possibility of further activities to address the lack of existing guidance and existing experience for the following issues.

[Rec 26](#) *The new approaches to deriving the required normal performance parameters from Safety work. See section 5.2 Is OPA now part of safety assessment?*

[Rec 27](#) *Defining the acceptability of claims for safety. See section 5.3 Acceptability of OPA claims.*

CHAPTER 6

INTEROPERABILITY

No issues were identified by WG-91 in the area of Interoperability.

CHAPTER 7

TRANSITION / OPERATIONS

This Chapter describes and explains issues identified by WG-91 in the area of the Transition - Operations.

7.1 ISSUES RELATING TO COORDINATED ENTRY INTO SERVICE

It was noted to the WG that there should be some available examples of successful introduction into services of multiple domain projects, i.e. RVSM and ADS-B and guidance could be given on how to use ICAO and its regional panels, and RFG for coordination purposes.

The WG noted that ED-78A already provides guidance in this area in chapter 6 but noted that this section is extremely small.

The WG considered that the guidance on coordinated entry to service has not been sufficiently described with ED-78A, and there are several examples of how this item has been addressed in a consensus manner by a number of users of ED-78A. However the WG felt that these examples did not describe all possible scenarios. It would therefore not be possible to produce additional guidance material based on published material.

7.2 ISSUES RELATING TO OPERATIONS

It was noted to the WG that there could be guidance given on the responsibility for monitoring by stakeholders and the methods used for operational feedback necessary to identify in-service problems and to allocate responsibility for addressing the issue, particularly where multiple stakeholders are involved. In effect, there should be allocated responsibilities identified on how to handle a change to the SPR (or other document) that occurs during the life of the system, for example if a problem with a requirement is found when a stakeholder implements of a system and as a result cannot meet the SPR.

The WG identified the example of EUROCAE ED-110B/RTCA DO-280B Interoperability Requirements for ATN Baseline 1 (Interop ATN B1) [42]. In this example, the in-service use identified a discrepancy in the standards relating to identification of the ATN Application "Version Number" parameter. This led to a submission to ICAO to address the issue.

The WG felt that this was an issue that was insufficiently addressed by ED-78A but that there were sufficient examples of how the issue had been successfully addressed. It would therefore be possible to produce additional guidance material.

7.3 EVIDENCE FOR APPROVAL

It was noted to the WG that evidence for approval and the associated approval plans could make use of the information collected in the SESAR standardisation / regulatory roadmaps and could make use of information used in interoperability mandates requiring system fitment.

The WG was unable to find any examples of how these documents had been used in conjunction with ED-78A, but recognized that this was an area that was in active development with EASA and the EC.

The WG felt that this was an issue that was insufficiently addressed by ED-78A but that there were insufficient examples of how the issue had been successfully addressed. It would therefore not be possible to produce additional guidance material based on present material.

7.4 TRANSITION HAZARDS

It was noted to the WG that guidance was requested on how to handle hazards arising from the transition from an existing mode of operation to a new mode of operation. This particularly applies to how the new system might affect the functionality of other systems. One example given to illustrate the issue is for the addition of ADS-B surveillance data to a radar display system. In this example, the specific characteristics of ADS-B data would need to be considered as regards how any existing ground safety nets might make use of this data.

The WG identified that this topic was out of scope of ED-78A as it was linked to the safety of the existing service rather than the change to the service.

The WG felt that this was an issue that was insufficiently addressed by ED-78A but that there were insufficient examples of how the issue had been successfully addressed. It would therefore not be possible to produce additional guidance material based on published material.

7.5 RISKS ASSOCIATED WITH MULTIPLE CHANGES

It was noted that stakeholders need to consider the implications when a combination of changes are developed into a single change, for example multiple ADS-B applications using a single aircraft 'box'. The key issue here is to get assurance that no additional risks would emerge from combining individual changes, that might have an impact on the other stakeholders (i.e. are the individual changes independent in their effects on the whole system).

This was recognized as being not just a limitation of ED-78A, but a more general issue with the scope of safety analysis which tends to be focused on the derivation of safety requirements for the change being considered.

It was recognized by the WG that the SPR generated by ED-78A was never intended to be the entire safety argument for the implementation of a change by an ANSP or for an aircraft manufacturer. There are already arrangements in place for the ANSP and the aircraft manufacturer to take the SPR (and indeed multiple SPR) for the change, and to include the safety analysis of how this change affects the remaining ATM or aircraft system. For example, an aircraft manufacturer would also need to justify, amongst other things, the effect of the change on other aircraft components. The ANSP would also provide an argument for how the new system will be used in the overall provision of services. These are generally controlled through the operational approvals given to both domains.

One example of successful integration is the case where various ATSA-xxx services affect the same target system. In such an example, the MOPS was used to collect the safety requirements and so ensure that the resulting system met all the requirements of the individual applications and certified accordingly.

The WG felt that this was an issue that was insufficiently addressed by ED-78A but that there were insufficient examples of how the issue had been successfully addressed. It would therefore not be possible to produce additional guidance material based on published material.

7.6 SUMMARY OF TRANSITIONS - OPERATIONS SECTION

The WG recommends that EUROCAE should consider the production of an additional guidance document to address the following issues to capture the experience gained in the application of ED-78A.

[Rec 28](#) How to update standards to address deficiencies found during operations. See sections on 7.2 Issues relating to Operations.

The WG recommends that EUROCAE should consider the possibility of further activities to address the lack of existing guidance and existing experience for the following issues.

[Rec 29](#) How to use ED-78A generated material in the certification / approval of changes to systems. See sections on 7.3 Evidence for approval and 7.1 Issues relating to Coordinated entry into service.

- [Rec 30](#) *How stakeholders should consider the implications of multiple changes. See section on 7.5 Risks associated with multiple changes.*
- [Rec 31](#) *How stakeholders should consider the effect of the new system on their existing system. See section on 7.4 Transition hazards.*

CHAPTER 8

CERTIFICATION

This Chapter describes and explains issues identified by WG-91 in the area of the Coordinated Approval & Certification Planning.

8.1 **LINKAGE OF SPR WITH 'COORDINATED APPROVAL & CERTIFICATION PLANNING'**

It has been noted that the SPR should capture both the requirements and the allocation of these requirements to the oversight organizations.

ED-78A identifies the intended use of an SPR, and that is developed using an OSA and an OPA. These two documents already refer to Stakeholder identification.

Moreover, ED-78A indicates: "SPR provides traceability from each requirement to its source".

The working group noted that it would be neither feasible nor convenient to identify into an SPR or ED-78A, specific details of oversight organizations. Indeed, present guidance provided concerning traceability of requirements to each source can be considered enough, as each stakeholder has its oversight competent authority.

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was insufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. It would therefore not be possible to produce additional guidance material based on present material.

8.2 **LINKAGE OF MOPS & MASPS WITH 'COORDINATED APPROVAL & CERTIFICATION PLANNING'**

It has been noted to the WG that the relationship between OSED, SPR and IR documents and the MASPS and MOPS document should be better integrated to allow existing material to be collected in a new analysis, and to allow the production of new MASPS and MOPS. It also has been noted that existing MOPS and MASPS should be used and coordinated with other domain activities. It was further noted by the WG that there is a preference in the FAA for MASPS as well as OSED / SPR / INTEROP documents but the European view is that OSED/SPR/INTEROP replaces MASPS.

ED-78A identifies that "the production of MOPS and MASPs is not part of this guidance material". However, it does not preclude it.

The WG noted that the development phase should be based in on SPR, IR, OSED. For the certification phase, it could be useful to use MOPS and MASPS when it is possible; however it is not strictly needed. The WG identified the following example where MOPS or MASPS have not been developed from SPR, as for ATN B1 Data Link (ED-110B and ED-120). Indeed, ATN B1 Data link is supported over VDL Mode 2, which has an existing MOPS (ED-92A). It is noted that SPR and IR do not refer explicitly to this MOPS within their texts, however, VDL Mode 2 MOPS (ED-92A) exists and it is referred during the certification processes of ATN B1 Data Link installations.

The WG felt that this issue was sufficiently addressed in ED-78A at present and clearly within the scope of ED-78A. Furthermore, there are some evidences of how the issue had been successfully addressed by a user of ED-78A (WG-51/SC-186, related to ASA MOPS). The WG considers that existing ED-78A guidance is adequate.

However, the WG considers that ED-78A could recommend to develop (or update) MOPS and MASPS, when possible. During the development of a new SPR/IR, such WG should take into account that if MOPS are also developed after SPR/IR, these MOPS will facilitate the certification of airborne domain. Indeed, the existence of MOPS or MASPS may facilitate the creation of E-TSO/TSO.

8.3 LINKAGE OF APPROVAL PLANNING WITH ‘COORDINATED APPROVAL & CERTIFICATION PLANNING’

It is noted that:

- it is not clear how material generated following ED-78A guidance applies to the certification structure;
- regulators should be part of the planning phase;
- the connection with applicable requirements should be identified.

ED-78A reference to the approval planning describes clearly the intent of this phase: “Approval planning is the process of ..., establishing the approval basis, proposing the means of compliance, and identifying tasks and schedules for the approval of a new or modified element ...”. “Approval planning provides early involvement and commitment of the applicant and the approval authority ...”.

This section emphasizes that the Approval planning phase is intended to formalize the agreements between stakeholders, including the approval authorities.

The WG notes that the material generated following ED-78A should be agreed with the approval authorities during the Approval planning, in particular, with regards to the means of compliance and the tasks for such approval. ED-78A clearly provides guidance on the involvement of authority in the planning phase which is generic enough to include new or modified CNS/ATM systems.

Concerning the connection with the applicable requirements, the agreement of the approval basis with the approval authorities should include any other applicable requirements.

The WG felt that this issue was sufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was sufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. It would therefore not be necessary to produce additional guidance material based on present material.

8.4 VALIDATION OF SPR AND SYSTEM DESIGN

Regarding validation aspects, it is noted that there is a lack of guidance regarding validation methods for interoperability requirements. It is also noted that ED-78A should be aligned with EOCVM V3 and V4 (European Operational Concept Validation Methodology) [43]. It is noted that guidance does not provide any indication on how validation could or should be conducted, in particular for various types of requirements such as human performance, training, maintenance requirements etc. Further, it is noted that there is no guidance about how to ensure that all mitigations are properly validated.

ED-78A refers to validation within the scope of qualification of a system element.

ED-78A does not refer to validation within the scope of the development phase. It refers to “*requirements consistency and requirements discrepancy*”, which are two subjects which could/should be considered under requirements validation scope.

The WG noted that this phase could also include the end to end system test that validates that the requirements can be achieved. In this case the system is taken to mean all the system parts of the individual domains. For example, for data link, to include the ANSP, the CSP and the aircraft systems. The SPR planning activities would need to define the responsibilities for the domains in such tests. In particular it is likely that a lead domain would need to have responsibility for this, as is the case in the SESAR scenarios.

Regarding EOCVM, the WG notes that ED-78A is intended to provide guidance for the approval of the provision and use of an ATS, without identifying a detailed methodology.

The WG notes that ED-78A does not provide enough information concerning validation. Indeed, validation is considered only as part of the qualification, when validation can also be considered as part of the development phase. As an example, ARP 4754 (Certification of Highly Integrated or Complex Systems) includes the validation concept as part of the development.

The WG also noted that EUROCAE is considering whether a version of documents, perhaps to be called an “Initial Standard”, should be issued to be used as a common reference for validation activities. The “Initial Standard” version would then be replaced by a validated standard after the validation activities.

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was sufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. The WG notes that guidance can be proposed to existing documentation where requirements validation and verification are used, as referred ARP 4754, which is intended for the development of airborne complex systems. The WG also notes that guidance can be developed for the validation of the SPR phase.

8.5 MULTI-DOMAIN TESTING FOR VERIFICATION PURPOSES IN CERTIFICATION

ED-78A does refer to this aspect in 5.2.1.2.e), Verification objectives. ED-78A indicates that for the verification of operational, performance and interoperability implementation, test plans and procedures including success criteria must be considered.

The need for end to end testing may be dependent on the system implemented and the approval basis. Additionally, end to end system test plans are also referred to during the Approval planning phase, where the related approval plans are identified. During this phase, the need of end to end system tests, and the responsible organization of such tests should be identified and agreed with the approval authority.

The WG has found examples regarding end to end system testing. However, end to end testing was understood as referred to within ED-78A, as part of the SPR/IR verification objectives scope. Indeed, such verification tests should identify (when needed) the boundary requirements to be demonstrated by each domain when performing their testing phase before enter into service (e.g. for certification).

The WG felt that this issue was sufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was sufficient evidence of how the issue had been successfully addressed by a user of ED-78A. It would therefore not be necessary to produce additional guidance material.

The WG considered that any end to end testing to be performed after definition of SPR/IR, may be much more difficult and costly, and have clearly to identify such needs. The demonstration of requirements may not need complete end to end testing.

8.6 ARP4754

It is noted that ED-79 / ARP 4754 should be identified as not being effective at determining shared mitigation means.

ED-78A does not refer to ED-79/ARP 4754.

The original use of ARP 4754 was intended for complex systems installed on aircraft. With this, the analysis is performed by a single responsible organization (aircraft TC holder) of the multiple aircraft-level functions. Within this scope, mitigation means are evaluated within the overall aircraft.

The use of ED-79/ARP 4754 beyond the scope of complex systems installed on aircraft shall be adequately justified during the Approval planning phase and agreed with the authorities.

The WG considers that ED-78A cannot provide guidance to use ED-79/ARP 4754 beyond the scope of complex systems installed on-board aircraft. However, its use is recommended as it is being extensively used for airborne systems design, providing a proven approach for systems development.

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was sufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. The WG recommends that ED-79 should be referred in ED-78A, as well as providing new guidance concerning the possible use of ED-79 on the development of multi-domain ATS services.

8.7 DEVIATIONS DURING IMPLEMENTATION OR OPERATIONS

It was noted to the WG that guidance is needed on coordination necessary between system elements when a system element cannot meet the necessary SPR or IR.

ED-78A does refer briefly to corrective actions identified during entry into service.

However, ED-78A does not provide detailed guidance when a system element may not comply with SPR or IR.

The WG has not identified any additional guidance regarding this issue. However, the WG confirms the need to have additional guidance when a system element cannot meet the necessary SPR or IR, even if there is no present guidance.

During entry in service, the domains will need to provide assurance to the regulators that the requirements have been met. In the OPA and the OSA, it is therefore necessary to identify which of the requirements identify the minimum performance requirement necessary to meet nominal performances (derived in the OPA activities) and minimum performance necessary to provide the mitigation in non nominal modes (in the OSA Part).

Similarly, where the requirements are conditional on environments of application, this should be clearly indicated.

The WG felt that this issue was insufficiently addressed in ED-78A at present but is clearly within the scope of ED-78A, and although there was insufficient evidence of how the issue had been successfully addressed by users of ED-78A, the WG itself could make proposals. The WG recommends that ED-78A should be updated to indicate clearly how to manage proposed deviations to performances indicated in SPR or IR, after the definition of such standards. For example, during the definition of SPR / IR, it could be identified which requirements are purely safety related performances, and which of them are operational or efficiency requirements. This would allow an easier assessment of potential deviations to SPR or IR by any of the domains.

With regards to potential performance deviations found during the in service operation of the equipment, the WG considers that this is a maintenance issue, where the definition of each domain shall identify the appropriate maintenance tasks to maintain their respective domain within the required performances of SPR / IR.

8.8 TRANSITION CRITERIA

It is noted that element J (transition criteria identification) is too specific to the data link example, and there are other transition criteria examples that can be given.

ED-78A indicates that transition criteria are defined as one of the objectives for development. It does not provide any more detailed guidance concerning this aspect.

The WG is unable to identify existing guidance regarding the definition of transition criteria from existing SPR.

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was insufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. The WG notes that it is not needed to provide detailed guidance, as the transition criteria identification is dependent on the new ATM/CNS system proposed, and it should be established during the Objectives for development phase. Indeed, the guidance provided is not specific with Data Link.

8.9 DEVELOPMENT ASSURANCE LEVELS

It is noted that ED-78A section 5.1.1 talks of "Development Assurance Levels", and if "Development Assurance" is effectively defined in the glossary, the corresponding scale (to identify the levels) is not mentioned. Reference to existing guidance on the assignment of design assurance levels could be provided as discussed below.

ED-78A defines "Development Assurance" as: "All those planned and systematic actions performed to minimize generic errors during development and implementation, and provide confidence that the system is suitable for its intended use". However, it does neither refer to any definition of levels, nor an identification of them.

The WG identified guidance in the following document, from the aircraft domain, where the levels are defined and identified: ED-79/ARP 4754 "Certification considerations for highly-integrated or complex aircraft systems". These levels correspond to software development levels identified in ED-12B/DO-178B, and Complex Electronic Hardware development levels in ED-80/DO-254 [45]

Additionally, different "Development Assurance Levels" can be found from other domains, which are similar to those from the aircraft domain. ED-109/DO-278 [46] (Guidelines For Communication, Navigation, Surveillance, And Air Traffic Management (CNS/ATM) Systems Software Integrity Assurance) defines the levels for ATM ground systems domain. It provides 6 levels, 5 of them corresponding to the 5 levels identified in ED-12B/DO-178B [44] (1=A, 2=B, 3=C, 5=D, 6=E). One intermediate level is added (4) which does not correspond to any airborne software DAL, but is between DAL C and DAL D. Also, the Eurocontrol EATMP Software Task Force defined the EUROCONTROL EATMP Software Assurance Levels (ESARR 6). Additionally, there exists ED-153 [47] "Guidelines for ANS Software Safety Assurance" to provide a standard to comply with EC Regulation 482/2008 [48].

Additionally, the concept of "Development assurance" is within safety analysis where quantitative analyses are not adequate, and qualitative analysis is to be performed, as for the development of software, or the management of processes (including human factor evaluation).

The WG noted that existing guidance concerning the Development Assurance Levels (DAL) can be provided, however it is dependent on the domain to be applied to, and it is not harmonized.

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was sufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. The WG recommends that a harmonized concept for "Development Assurance" and 5 corresponding levels (as used within the existing domains) should be proposed in ED-78A, to be used during the development of SPR, allowing coherent safety objectives for all the related domains. Indeed, the certification of airborne domain requires to provide function DAL in order to perform their safety assessments as part of their showing of compliance with CS-25.1309 requirement.

8.10

REAL APPROVAL PROCESS

It is noted that it should be checked if there is some feed back for the application of ED-78A in an actual approval process.

The WG notes that ED-78A has been used during the definition of several SPR and IR, citing as examples the following: SPR for Continental data link (ED-120), SPR for Oceanic and Remote Data Link (ED-122), SPR for AIS and MET data Link services (ED-175), IR for ATN B1 Data link (ED-110B).

The WG notes that ED-78A has been used to develop SPR and IR, for certain ATM/CNS systems.

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was sufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. No further guidance on this issue could be found from existing material.

8.11

EASA-SES

It is noted to the WG that there is no present guidance on the arrangements between SES and EASA for pan European changes.

ED-78A provides adequate guidance concerning Approval Planning, in order to ensure that all stakeholders of a certain new ATM/CNS system reach adequate agreements. However, it should be understood that ED-78A guidance only requires that these agreements are to be considered within the limits of the applicable regulations.

ED-78A does not therefore need to provide guidance on specific arrangements between EASA and SES. The necessary arrangements are within the scope of competences of EASA as defined by the European Regulations, principally by Regulation (EC) No. 216/2008 [49].

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly within the scope of ED-78A, and furthermore, there was insufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. The WG considers that ED-78A should not refer to the European Regulations. No additional guidance can be recommended on this issue.

8.12

APPROVAL

It was noted to the WG that the approvals issued to parts of the CNS/ATM should be coordinated to ensure that the approval status of the total CNS/ATM system could be identified by regulators and domain owners.

ED-78A does not provide detailed information concerning the boundaries of the scope of the approval.

ED-78A does not clarify by whom and how the scope of the approval should be managed. However, this activity should be defined during the Approval Planning phase, as it may be dependent on the regulators environment and Authorities involved.

The WG felt that this issue was insufficiently addressed in ED-78A at present and clearly outside the scope of ED-78A, and furthermore, there was insufficient evidence of how the issue had been successfully addressed in a consensus manner by a user of ED-78A. The WG considers that there are not examples to produce additional guidance on this subject.

8.13

SUMMARY OF CERTIFICATION SECTION

The WG recommends that EUROCAE should consider the inclusion of additional guidance within an updated ED-78A to address the following issues to capture the experience gained in the application of ED-78A;

[Rec 32](#) *Identify the need for the SPR to identify the information necessary for the aircraft stakeholders to identify DAL. See section 8.9 on (Cert – Design Assurance levels)*

The WG recommends that EUROCAE should consider the production of an additional guidance document to address the following issues to capture the experience gained in the application of ED-78A and allow the use of ED-78A beyond its present scope of application;

[Rec 33](#) *Identify the safety requirements from the efficiency requirements to allow easier management of potential deviations in domains. See section on 8.7 8.7 Deviations during implementation or operations(Cert – Deviations during implementation or operation)*

The WG recommends that EUROCAE should consider the possibility of further activities to address the lack of existing guidance and existing experience for the following issues.

[Rec 34](#) *Guidance on the activities to be followed if a safety requirement is identified as deficient during operations. See section 8.7 Deviations during implementation or operations (Cert – Deviations)*

[Rec 35](#) *Specific guidance on liaison with oversight organisations. See section 8.1 Linkage of SPR with 'Coordinated Approval & Certification Planning'(Cert – Linkage of SPR with 'coordinated approval and certification planning')*

[Rec 36](#) *The use of ARP4754 for qualification of ground elements of the ATM system. See sections 8.4 Validation of SPR and system design and 8.6 ARP4754(Cert – Validation of SPR and system design)(cert – ARP 4754)*

[Rec 37](#) *The development of harmonized concept of 'development assurance. See section 8.9 Development Assurance Levels on Cert – Design Assurance levels)*

[Rec 38](#) *Validation of SPR. See section 8.4 Validation of SPR and system design(Cert – validation of SPR and system design)*

The WG recommends that EUROCAE should facilitate and inform other organisations in the production of additional guidance material for the following issues.

[Rec 39](#) *Guidance on the linkage between certification activities and generation of certification material. See sections on 8.2 Linkage of MOPS & MASPS with 'Coordinated Approval & Certification Planning', 8.3 Linkage of Approval planning with 'Coordinated Approval & Certification Planning', 8.5 Multi-domain testing for verification purposes in certification, 8.8 Transition criteria, 8.10 Real approval process, 8.11 EASA-SES, 8.12 Approval.*

CHAPTER 9

TRAINING PACKAGE

The WG was not able to provide adequate resource to the issue of a training package due to lack of suitable input.

The WG identified that EUROCONTROL already provides training on the EUROCONTROL Safety Assessment Methodology through a number of individual courses, in particular the SAF Safety Assessment group of courses. These courses incorporate elements of the ED-78A approach.

The WG identified that these courses, which have been given to a large number of European ATM Safety Practitioners could be developed and focused to further enhance the usage of ED-78A.

Informal approaches to the Institute of Air Navigation Services, who develop and deliver this training, indicate that they would be willing to provide delivery mechanisms and infrastructure for the delivery of such course, but would require additional support in the development and delivery of the courses.

CHAPTER 10

RATIONALE AND RECOMMENDATIONS

10.1

RATIONALE

To enable future planning of activities recommendations have been split into the following forms.

LEVEL 1: Update ED-78A now within same scope
WG-91 recommends that EUROCAE should consider the update of ED-78A to address the following issues; <i>to be used where</i> <i>it has been identified that ED-78A is deficient,</i> <i>where an agreed approach can be practically demonstrated</i> <i>and where the issue is within the existing ED-78A scope.</i>
LEVEL 2: Prepare application note to provide additional Guidance
WG-91 recommends that EUROCAE should consider the production of an additional guidance document to address the following issues to capture the experience gained in the application of ED-78A and allow the use of ED-78A beyond its present scope of application; <i>to be used where</i> <i>it has been identified that ED-78A is deficient,</i> <i>where an approach has been practically demonstrated.</i>
LEVEL 3: Consider reopening ED-78A for new material
WG-91 recommends that EUROCAE should consider the possibility of further activities to address the lack of existing guidance and existing experience for the following issues. <i>to be used where</i> <i>it has been identified that ED-78A is deficient,</i> <i>where an approach has been practically demonstrated</i> <i>and where the issue would increase the scope of ED-78A beyond Data communications used for ATS.</i>
Level 4: Other organisations to produce material
WG-91 recommends that EUROCAE should facilitate and inform other organisations in the production of additional guidance material for the following issues. <i>to be used where</i> <i>the WG has identified the ED-78A as deficient</i> <i>where an approach has not been practically demonstrated</i> <i>where another organisation than EUROCAE is identified as having authority over the issue</i>