

SAFETY REGULATION COMMISSION DOCUMENT  
(SRC DOC)

**SRC DOCUMENT 39**

**ASSESSMENT OF THE DEUTSCHE  
FLUGSICHERUNG GMBH (DFS)  
'CORPORATE DIRECTIVE SAFETY  
ASSESSMENT' AS A MEANS OF  
COMPLIANCE WITH ESARR 4**

<b>Edition</b>	<b>:</b>	<b>1.0</b>
<b>Edition Date</b>	<b>:</b>	<b>26 October 2009</b>
<b>Status</b>	<b>:</b>	<b>Released Issue</b>
<b>Distribution</b>	<b>:</b>	<b>General Public</b>
<b>Category</b>	<b>:</b>	<b>SRC Document</b>

## F.2 DOCUMENT CHARACTERISTICS

TITLE		
<b>SRC Document 39</b>		
<b>Assessment of the DFS ‘Corporate Directive Safety Assessment’ as a Means of Compliance with ESARR 4</b>		
<b>Document Identifier</b>	<b>Reference</b>	SRC DOC 39
srcdoc39_e1.0_ri_web	<b>Edition Number</b>	1.0
	<b>Edition Date</b>	26-10-2009
<b>Abstract</b>		
<p>This document has been developed, validated and completed by the SRC Expert Panel in charge of assessing to what extent the ‘DFS Safety Assessment Methodology’ complies with ESARR 4 “Risk Assessment and Mitigation in ATM”, Edition 1.0.</p> <p>This document comprises the outcome of these assessments and provides a view on the acceptability of the ‘DFS Safety Assessment Methodology’. It is intended to be used as a decision making tool to assist the SRC in forming its own judgement on the acceptability of the ‘DFS Safety Assessment Methodology’ as one Means of Compliance with ESARR 4.</p>		
<b>Keywords</b>		
SRC	DFS	Compliance
ESARR 4	Hazard	Acceptable
Assessment	AMC	PMC
		Safety
		Risk
<b>Contact Person(s)</b>		<b>Unit</b>
Françoise GIRARD		DG/SRU
<b>Tel</b>		
+32 2 729 51 65		

DOCUMENT INFORMATION					
Status		Distribution		Category	
Working Draft	<input type="checkbox"/>	General Public	<input checked="" type="checkbox"/>	Safety Regulatory Requirement	<input type="checkbox"/>
Draft Issue	<input type="checkbox"/>	Restricted EUROCONTROL	<input type="checkbox"/>	Requirement Application Document	<input type="checkbox"/>
Proposed Issue	<input type="checkbox"/>	Restricted SRC	<input type="checkbox"/>	ESARR Advisory Material	<input type="checkbox"/>
Released Issue	<input checked="" type="checkbox"/>	Restricted SRC Commissioners	<input type="checkbox"/>	SRC Policy Document	<input type="checkbox"/>
		Restricted SRCCG	<input type="checkbox"/>	SRC Document	<input checked="" type="checkbox"/>
		Restricted SRU	<input type="checkbox"/>	Comment / Response Document	<input type="checkbox"/>

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

### F.3 DOCUMENT APPROVAL

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

Authority	Name and Signature	Date
Quality Control (SRU)	<p style="text-align: center;"><i>« signed by Daniel Hartin »</i></p> <p style="text-align: center;">(Daniel HARTIN)</p>	26.10.2009
Chairman, Expert Assessment Panel (SRC)	<p style="text-align: center;"><i>« signed by Harry Daly »</i></p> <p style="text-align: center;">(Harry DALY)</p>	26.10.2009
Head, Safety Regulation Unit (SRU)	<p style="text-align: center;"><i>« signed by Juan Vázquez-Sanz »</i></p> <p style="text-align: center;">(Juan VAZQUEZ-SANZ)</p>	26.10.2009
Chairman, Safety Regulation Commission (SRC)	<p style="text-align: center;"><i>« signed by Jos Wilbrink »</i></p> <p style="text-align: center;">(Jos WILBRINK)</p>	26.10.2009

*(Space Left Intentionally Blank)*

## F.4 AMENDMENT RECORD

The following table records the complete history of this document.

Edition No.	Date	Reason for Change	Pages Affected
0.01	7-Feb-05	Creation – First working draft to SRU including initial contents for sections 2, 3 and 4.	All
0.02	21-Mar-05	Table 2B added. Title in central column of table 1 corrected. Executive summary completed. Removal of issue 2 (Section 3.2 is now complied with). Changes to the wording of the comments against requirements 5.1, 5.2.a, 5.2.b.ii, 5.2.b.iii, 5.2.c.iii, 5.2 note 1 & 5.2 note 2. Changes to the wording of Issue 8. Contents table corrected.	7, 8, 12, 13, 16, 18, 22, 24, 25, 28, 30, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46
0.03	10-May-05	Changes made after a meeting with DFS 3/5/2005. Executive summary changed to reflect change in issues in section 4. More detailed description of table notation added to section 3.2. Coverage changed in table 1: 3.1 & 5.3 b now "Yes", "(Mostly)" added as a descriptor to many entries – in line with changes to 3.2. "Partially" used in tables 2A & 2B instead of "-". Issue against 3.1 (old issue 1) deleted, now covered as a comment. Previous Issues 1, 4, 6 & 7 now combined and covered in issue 3. Other Issues renumbered accordingly. Table 2A, 5.1 c corrected. Additional statement from DFS added to table 2A, 5.3 b. this changes level of correspondance to "=". Additional text explaining ESARR 4 rational added to comments in table 2A A-2(1). Section 5 altered to reflect previous changes. Contents table corrected.	8, 11-21, 23, 26-29, 31, 35-46
0.04	25-May-05	Correct Chairmans name. Mitigations added to 4.8 and summarised in the Executive Summary. ESARR 4 issues added	4, 8, 44

*(Space Left Intentionally Blank)*

Edition No.	Date	Reason for Change	Pages Affected
0.05	26-Sept-05	Changes incorporated after a meeting with DFS and SRU, 20/9/2005. Executive Summary changed to remove references to ESARR 4 review. Issue 8 changed to reflect above change. Analysis section changed to explain the inclusion of pedagogic material in DFS documents and lack of direct relationship to ESARR 4. Accident changed to accident/incident throughout. Additional SAH reference added to requirement 5.1. Explanation of "technical agreements added to requirement 5.1 b. Reference to SRU as European Regulator removed from requirement 5.2 b) ii). 5.2 c) i) reviewed. Text changed to clarify the meaning of "Black Box" risk and to show "Partial" judgement is a result of not being able to review DFS supporting service manual. 5.2 (Note 1) reviewed. Downgraded to "Partial (Mostly)" and linked to Issue 3 because SAH does not cover co-ordination with external suppliers. Issue 3 changed to accommodate above changes. Section 5 – statement of compliance – changed to reflect changes made above. Contents table corrected.	9, 12, 14, 15, 19, 22, 25, 28, 32, 36, 39, 41, 43, 45, 46, 47, 48.
0.06	13-Oct-05	Changes incorporated after completion of the assessment of compliance with the executive summary and with the chapters 1, 2, 4, 6, 7, 8 of ESARR 4.	40 to 53 63 to 73
0.07	17-May-06	Changes incorporated after the AMC panel meeting on 21-Oct-05 and the assessment of Edition 2.02 of the SAH methodology which was presented after this meeting.	All
0.1	27-May-09	SRU quality review. Format changes only, no change to technical content.	All
1.0	26-Oct-09	Document formally released following RFC No. 0907.	-

*(Space Left Intentionally Blank)*

## F.5 CONTENTS

<u>Section</u>	<u>Title</u>	<u>Page</u>
<b>Foreword</b>		
<b>F.1</b>	<b>Title Page</b> .....	<b>1</b>
<b>F.2</b>	<b>Document Characteristics</b> .....	<b>2</b>
<b>F.3</b>	<b>Document Approval</b> .....	<b>3</b>
<b>F.4</b>	<b>Document Change Record</b> .....	<b>4</b>
<b>F.5</b>	<b>Contents</b> .....	<b>6</b>
<b>F.6</b>	<b>Executive Summary</b> .....	<b>7</b>
 <b>SRC Document 39 – Assessment of the DFS ‘Corporate Directive Safety Assessment’ as a Means of Compliance with ESARR 4</b>		
<b>1.</b>	<b>Introduction</b> .....	<b>9</b>
<b>2.</b>	<b>Purpose and Scope</b> .....	<b>9</b>
<b>3.</b>	<b>Analysis</b> .....	<b>10</b>
3.1	General .....	10
3.2	ESARR 4 Mandatory Provisions: Sections 3 and 5 .....	11
3.2.1	Summary Analysis .....	11
<b>4.</b>	<b>Conclusions and Recommendations</b> .....	<b>15</b>
4.1	Summary .....	15
4.1.1	Issue 1 – Management of Changes .....	15
4.1.2	Observation 1 – Bayesian Networks .....	16
4.1.3	Observation 2 – Assessment of the Effects .....	17
4.2	Detailed Analysis .....	17
4.3	ESARR 4 Mandatory Provisions: Sections 6 and 7 .....	39
4.4	ESARR 4 Advisory Sections: Executive Summary, 1, 2, 4 and 8 .....	42
<b>5.</b>	<b>Statement of Compliance</b> .....	<b>51</b>
 <b>Appendices</b>		
<b>A.</b>	<b>Terms and Definitions</b> .....	<b>53</b>
<b>B.</b>	<b>Review of the Conclusions and Recommendations of the First Assessment</b> .....	<b>64</b>

## F.6 EXECUTIVE SUMMARY

This document has been developed by the Safety Regulation Commission (SRC).

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

Complementary information has been provided by DFS:

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

SRC Document 39 comprises the outcome of this assessment and establishes the rationale for the SRC judgement on the acceptability of the ‘DFS Safety Assessment Methodology’ as a Means of Compliance with ESARR 4.

It considers all sections of ESARR 4 and includes a complete mapping between each safety requirement included in ESARR 4, Sections 3 & 5 and Appendix A, and the elements of the Proposed Means of Compliance (PMC), which are considered as meeting the intent of the requirement.

It also provides a set of conclusions and recommendations to support the final SRC judgement. The conclusions not only refer to the compliance with the totality of ESARR 4, but also, where necessary, to the compliance with part(s) of ESARR 4. The sets of conclusions and recommendations provide justifications supporting the final statement on the PMC, as well as proposed ways forward for the DFS standard to be fully compliant with ESARR 4.

In general, the DFS Safety Assessment Methodology is well thought out and thoroughly documented. The SAH, in particular, is an expansive document. A translation into English was provided for review. It contains an excellent exposition of the use of probability theory and Bayesian networks in risk assessment.

During the initial part of the assessment, a significant number of comments were generated. It was felt that many of these could be to the result of misunderstandings caused by differences in culture or errors in translation. Consequently, a meeting was arranged with DFS to discuss the comments. What emerged, for the reviewer of the first assessment, was an understanding of the DFS process and a realisation that, whilst the process itself satisfied ESARR 4, it had not been completely captured in the documentation. Since this assessment is a comparison of the DFS documentation with ESARR 4, these deficiencies have been recorded in Appendix B to this document.

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

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

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

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

The outstanding issue deals with the qualification of "changes in ATM" which appears too restrictive in the CDSA.

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

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

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

*(Space Left Intentionally Blank)*



## 1. INTRODUCTION

Under international treaties, such as the Chicago Convention, safety regulation of civil aviation is a national responsibility. Indeed, every State has complete and exclusive sovereignty over the airspace above its territory.

Each State which has signed the Chicago Convention undertakes to keep its own regulations, its air navigation equipment and operations compliant, as far as possible, with those established by the International Civil Aviation Organisation (ICAO) under the Chicago Convention.

Recent modifications<sup>1</sup> to ICAO Annex 11 requires States to assess the potential safety impacts of proposed changes<sup>2</sup> to the ATM system to show that an acceptable level of safety will be met, before implementing the proposed changes.

EUROCONTROL Safety Regulatory Requirement “Risk Assessment and Mitigation in ATM” (ESARR 4), approved by the EUROCONTROL Permanent Commission in April 2001 (Decision No. 87), strengthens those ICAO requirements and recommended practices. Its implementation and enforcement within their national legal framework becomes binding on States as from April 2004.

In that context, the EUROCONTROL Safety Regulation Commission (SRC) has the task of ensuring the uniform implementation of ESARR 4 across Europe, hence the need for SRC to recognise a number of Acceptable Means of Compliance (AMCs) to help this uniform implementation of ESARR 4.

## 2. PURPOSE AND SCOPE

The SRC Commissioner for The Federal Republic of Germany wrote to the SRC Chairman requesting that the ‘DFS Safety Assessment Methodology’ be assessed and recognised as a Means of Compliance with ESARR 4.

The purpose of this document is to contribute to the application of SRC Document 9 ‘Process for Establishing Acceptable Means of Compliance with ESARRs’, Edition 4.0. It provides the results of the SRC assessment of the ‘DFS Safety Assessment Methodology’ against ESARR 4 in order to form a view on its acceptability as a Means of Compliance to ESARR 4.

The documents compared are:

- ESARR 4, Edition 1.0 (Released Issue), dated 5<sup>th</sup> April 2001;
- ‘Corporate Directive Safety Assessment’ (CDSA), Version 1.0.1, dated 1.6.2003, reference VYK.01.
- ‘Safety Assessment Handbook’ (SAH) Volume 1: Introduction to the Methodology, Version 1.02, dated 24. November 2003,

---

<sup>1</sup> Amendment 40.

<sup>2</sup> Such as airspace re-organisation, provision of ATS procedures, introduction of new equipment, systems or facilities.

As the DFS methodology was improved during the assessment period, additional information and a released version of the SAH has been provided by DFS:

- ‘Safety Assessment Document’, template and example;
- Manual on “Assurance and Demonstration of the Safety of External Services” V1.0 (07/2003);
- ‘Safety Assessment Handbook’ Volume 1: Introduction to the Methodology, Version 2.02, dated 9 November 2005.

This document includes the factual findings of the assessment of the ‘DFS Safety Assessment Methodology’ against ESARR 4 in the form of text and tables.

In addition, it provides for a set of conclusions and recommendations with rationale. The sets of conclusions and recommendations provide some justifications supporting the final draft statement on the PMC ‘DFS Safety Assessment Methodology’.

Indeed, the document proposes in section 5 a draft statement of compliance to support the final SRC decision making process. This statement refers to the compliance with the totality of ESARR 4, and also, where necessary, to the compliance with part(s) of ESARR 4. It is intended that the SRC relies on this document to recognise/accept, or not as the case may be, the ‘DFS Safety Assessment Methodology’ as a Means to show compliance with ESARR 4 or with specific requirements/parts of ESARR 4.

### **3. ANALYSIS**

#### **3.1 General**

ESARR 4 was developed by the EUROCONTROL Safety Regulation Commission, as a harmonised safety regulatory requirement, to be enforced by all EUROCONTROL Member States<sup>3</sup>. Its main objective is to require that changes to the ATM system are implemented only after having been shown to meet tolerable safety levels.

‘DFS Safety Assessment Methodology’ was developed with the objective: *“By setting safety objectives and safety requirements, identifying and evaluating hazards and safety-related effects, and setting safety measures to reduce risk, a safety assessment is designed to ensure, by implementing required measures, and document that a system or changes thereto do not engender any unacceptable risks”*.<sup>4</sup>

The analysis, final conclusions and recommendations on the acceptability of the ‘DFS Safety Assessment Methodology’ as a means of compliance to ESARR 4 therefore reflects this statement.

---

<sup>3</sup> ECAC member states are also encouraged to enforce ESARRs at national level.

<sup>4</sup> See Paragraph 5 of ‘Corporate Directive Safety Assessment’

The ‘DFS Safety Assessment Methodology’ contains a considerable amount of tutorial material. This is to be expected, in the early stages of the introduction of a new requirement, since it is better to ensure that users understand the subject rather than simply follow a prescriptive process. Later on, when the subject is fully understood, the pedagogic material will recede into the background and play a less dominant role.

Moreover, since they are primarily a description of the DFS approach to Risk Assessment and Mitigation, the documents describing the ‘DFS Safety Assessment Methodology’ are not intended to be a concise statement of compliance with ESARR 4. Consequently, the text relating to satisfying the requirements will appear in many places. To help the reader, each requirement table has a cross-reference section (Link to SAH/CDSA) showing where each individual requirement is covered in the DFS documentation.

## **3.2 ESARR 4 Mandatory Provisions: Sections 3 and 5**

### **3.2.1 Summary Analysis**

Table 1 provides a coverage analysis of the contents of the following documents, for those mandatory provisions included in ESARR 4:

- ESARR 4, Edition 1.0 (Released Issue), dated 5<sup>th</sup> April 2001,
- ‘Corporate Directive Safety Assessment’, Version 1.0.1, dated 1.6.2003, reference VYK.01,
- ‘Safety Assessment Handbook’ Volume 1: Introduction to the Methodology, Version 2.02 dated 9 November 2005.

Table 1 only provides a summary of the coverage of the PMC with respect to ESARR 4 and references those sections of ESARR 4 that are mandatory. Where there is no text related to an ESARR 4 mandatory section, in the ‘DFS Safety Assessment Methodology’, then the “Covered by...” column will contain “No”. Otherwise the “Covered by ...” column contains a statement of the coverage. A brief description for the reason for the coverage statement is provided in the “Related Comments” column. The statement of coverage is a word i.e. “Yes” for full coverage, “Partially” for partial coverage and “No” for no coverage. The partial category is very large, since it can cover marginal coverage to very nearly complete coverage. Consequently an optional descriptor may be added e.g. (Mostly) to convey the level of coverage achieved.

The detailed findings are reproduced in tables 2A and 2B. Table 2A covers the main body of ESARR 4 while table 2B covers the appendices. Each table is constructed in the same way. Each entry in the table refers to a single requirement. The reference to the relevant paragraph in ESARR 4 is provided and the text of ESARR 4 is included.

A “Link” is provided to show where in the PMC the ESARR 4 requirement is covered and DFS have provided a “Statement” section, which explains how the requirement is covered.

A “Related Comments” section is provided and the overall “Level of Correspondence” to the ESARR 4 requirement, which is also shown in table 1 (in the “Covered by ...” column).

If the level of correspondence is “Partial” then the comments section will contain a reference to an “Issue” number. This is a pointer to section 4 where the issue of incompleteness is dealt with and suggestions are made for improving the PMC.

The section 3.2 and 3.3 address those provisions of ESARR 4 which are considered mandatory and section 3.4 addresses those provisions of ESARR 4 which are considered advisory.

**Table 1 – Coverage Analysis (Mandatory)**

ESARR 4	COVERED BY 'DFS SAFETY ASSESSMENT METHODOLOGY'	RELATED COMMENTS
<b>SECTION 5 – SAFETY REQUIREMENTS</b>		
3.1	<b>Yes</b>	The supplied material could be improved by specifically describing DFS' responsibility for services (supporting services) delivered to itself
3.2	<b>Yes</b>	Although military services are included in the guidance material (SAH) their inclusion is not made a requirement in the directive (CDSA)
5.1	<b>Partially (mostly)</b>	Hazard identification and risk assessment are dealt with in depth and are well covered. The new version of SHA V2.02 provides improvement since the first assessment. However an issue (issue 1) has been raised with regard to the notion of “changes”.
5.1 a	<b>Yes</b>	Therefore, the version 2.02 of the SAH provides (page 11) clarification with regard to the “safety analysis” performed during of the life cycle phases.
5.1 b	<b>Yes</b>	Version 2.02 of the SAH provides (page 9) clarification with scope of the safety assessment and provides an additional reference to a procedure dealing with external services.
5.1 c	<b>Yes</b>	Making the assumption that the description of this impact analysis allows to keep traceability all along the life cycle of the system and could be used at each stage as a continuous process and not only for the development of a specific project, the version 2.02 of the SAH provides (page 42) highlight the impact analysis done by the DFS in figure 19 (process description) and figure 20 (the interaction between the various elements within the system).
5.2 a	<b>Yes</b>	The derivation of safety objectives is described well.
5.2 b i)	<b>Yes</b>	Version 2.02 of the SAH, page 45, paragraph 3 identified “n to m” relations.

ESARR 4	COVERED BY 'DFS SAFETY ASSESSMENT METHODOLOGY'	RELATED COMMENTS
<b>SECTION 5 – SAFETY REQUIREMENTS</b>		
5.2 b ii)	<b>Yes</b>	<p>The assessment of the effects of hazards (accidents/incidents) is handled well, as is the assessment of the severity of the effects. However, (<b>observation 1</b>) the use of Bayesian net needs to be carefully controlled because of the level of confidence which has to be made to probabilities and experts views. Despite ways forward stated in §6.1.4. of the SAH version 2.02, they should be developed more in depth in order to guarantee the validity of the figures used in Bayesian networks.</p> <p>The assessment of the effects should be developed more in depth by providing guidance in the SAH. As required by ESARR 4, the SAH identifies several possible effects, however, only two tables describing the effect on safety in air traffic and people are developed in paragraph 6.1.3 (<b>observation 2</b>).</p>
5.2 b iii)	<b>Yes</b>	<p>The method of determining the tolerability of a hazard uses a Bayesian net, which appears to be well suited for this application. In order to emphasise the best practices dealing with Bayesian net and conditional probabilities, the AMC panel members issued an observation with regard to the use of Bayesian model.</p>
5.2 c i)	<b>Yes</b>	<p>Version 2.02 of the SAH, page 65, section 6.3.1, paragraph 2 clarifies the point.</p> <p>The document on "Assurance and Demonstration of the Safety of External Services" V1.0 (07/2003), provide the requirements for external services.</p>
5.2 c ii)	<b>Yes</b>	<p>Version 2.02 of the SAH, page 61, section 6.2.3, paragraph 3 clarifies the point.</p>
5.2 c iii)	<b>Yes</b>	<p>Version 2.02 of the SAH, page 62, section 6.2.3 paragraph 3 provides a clarification.</p>
5.2 d i) ii) iii) and iv)	<b>Yes</b>	<p>Version 2.02 of the SAH, page 78, section A2, table 3, working step 7 "Assessment of effects (severity, conditional probability, frequency)" provides a clarification.</p>
5.2 Note 1	<b>Yes</b>	<p>Version 2.02 of the SAH, pages 9 and 97 covers this item with regard to third parties.</p>
5.2 Note 2	<b>Yes</b>	<p>Bayesian networks provide a robust, probabilistic method of reasoning with uncertainty, however see observation 1.</p>
5.3 a	<b>Yes</b>	<p>DFS provided the SRU with an example of the use of RAMSYS: Handbuch der Sicherheitsbewertungen Band II V10, which covers the requirement.</p>

ESARR 4	COVERED BY 'DFS SAFETY ASSESSMENT METHODOLOGY'	RELATED COMMENTS
<b>SECTION 5 – SAFETY REQUIREMENTS</b>		
5.3 b	<b>Yes</b>	Safety requirements are traceable to the operations/functions.
Appendix A A-1 (1)	<b>Yes</b>	The DFS severity scheme has 4 categories. The most severe is clearly related to ESARR 4, although its description contains fewer examples.
Appendix A A-1 (2)	<b>Yes</b>	Agreed, the DFS method stresses that all plausible accidents and incidents should be assessed and not just those leading to severity class 1 results. However, DFS could provide additional information, in term of process, in order to provide assurance that the most probable effect of hazards under the worst case scenario is adequately taken into consideration with the Bayesian network approach (please refer to observation 1 made above in ESARR 4 Requirement 5.2 b iii).
Appendix A A-1 (3)	<b>Yes</b>	The assessment of the severity of an effect has been provided in compliance with ESARR 4. However, more guidance should be provided in order to assess the severity of effects (observation 2).
Appendix A A-2 (1)	<b>Yes</b>	The SAH provides a good clear exposition of the way a safety objective is derived. However, see observation 1 with regard to the limitation of Bayesian network.
Appendix A A-2 (2)	<b>Yes</b>	The DFS method does indeed make it clear that a 'class d' risk should be the aim for the design of any change. This is intended to give considerable headroom in the safety of the implemented systems. The concern with regard to 'class b' risks has been clarified by DFS.

*(Space Left Intentionally Blank)*

## 4 CONCLUSIONS AND RECOMMENDATIONS

### 4.1 Summary

#### 4.1.1 Issue 1 – Management of Changes

**Issue 1 (ESARR 4, requirement 5.1) – The PMC does not cover fully the requirement of ESARR4 5.1.**

Some information is provided by the PMC:

- The CDSA classifies changes into three classes according to which changes of “Class III” do not need a complete and systematic safety assessment each time the change is implemented, although only one example was provided. However, they require certain processes to be followed (e.g. checklist to be filled in). Considering that ESARR 4 does not provide additional specification on the classification of a change that is subject to a quantitative risk-based approach, this requirement is considered to be met as the CDSA describes on a global level the measures to be taken to assure that these changes do not introduce unacceptable risks at a global level<sup>5</sup>.
- Page 9 of the SAH version 2.02: “The scope of a safety assessment not only contains the elements of the DFS part of the ATM system but also has to address the system environment that may be affected by a change. This includes the consideration of all airborne and ground components that are in some way related to the safety aspects of a change. In co-operation with the national regulator and if necessary, the airspace users, it has to be assured that all affected parties are involved in the process. Similarly, the safety properties of all third-party products and services used within the DFS ATM system must be assured by conducting hazard analyses and defining and verifying safety requirements for those products and services according to the methodology described in this handbook.”

However, the CDSA does not specifically mention “All new air navigation systems”, nor does it state that airspace and flight procedure plans are considered as part of the system, consequently it might not be seen as a requirement. Therefore, certain part of the system is not covered by the safety management of changes, as it is stated in the §5 of the CDSA: “*the only modification requiring safety assessment are procedures not included and for which no provision is made in the list of aforementioned documents –in §5 and annex A of the CDSA-*” and in §5: “*this means that procedures and projects that are:*

- *fully governed by legislation,*
- *fully covered by national and international standards,*
- *fully established in DFS standards, guidelines and handbooks.*

*are not required to undergo any safety assessment”.*

These claims are too restrictive and a safety assessment is required for those changes by ESARR 4 and ICAO Annex 11, Edition 13.

<sup>5</sup> It should be taken into consideration that the procedures for changes of class II and class III were not evaluated as part of this assessment.

## Suggested Solution

It is recommended that these changes to services are included in the CDSA. DFS to clarify the scope of the change taking into account ESARRs 1 and 4.

### 4.1.2. Observation 1 – Bayesian Networks

The second assessment wishes to draw the attention of DFS to the use of a quantitative approach with regard to the “mechanics” of Bayesian networks. The quantitative results and the decision with regard to the severity class of effects rely on the validity of two main types of variables: the frequency of the hazard and/or the conditional probability of the effect.

Therefore those figures, dealing with radar failure, radio failure, human factors, etc. shall be established and validated as far as possible *a priori*.

DFS provided an example of the use of Bayesian network, however the document, which is an example (in German), has not been fully analysed. Its analysis has not been performed with a particular attention to the comparison of the result of the Bayesian approach and those of the “classical” methods of PSSA. However, it gives an idea of the process; in depth analysis could be done in a further study within EUROCONTROL.

As the Bayesian model relies on a calculation starting from a set of probability and frequencies for “basic events”, if those basic figures are not validated this could easily lead to wrong probabilities or misuse of the methodology.

In addition, it is not clear that the Bayesian Network approach fits with “the worst case scenario” which is identified as a requirement in the SAH document. This could be clarified in a methodological process description.

It should be ensured that the values used in Bayesian network is under the control of a process which, if necessary, periodically validates and improves those values (gathering of operational data, validation of expert’s panels, mathematical/statistical modelling, etc.). Such a process is referred to, but not clearly established, in the SAH (e.g. reference to guidelines, best practices or specific processes giving a framework to the use of Bayesian network)

## Suggested Solution

DFS to provide information or guidance with regard to the limitation of the use of Bayesian networks.

This observation is out of the scope of ESARR 4 and the assessment of the documentation cannot prejudge the way to use Bayesian networks during the safety assessment and mitigation process. This has to be verified by internal ANSP audit process or external NSA audit.



### 4.1.3 Observation 2 – Assessment of the Effects

In the SAH, chapter 6.1.3, the effect on the:

- air crew;
- air traffic controllers;
- aircraft functional capabilities;
- functional capabilities of the ground parts of the ATM system;
- ability to provide safety ATM services;

is identified as required by ESARR 4.

However, the SAH does not provide guidance to identify and assess hazards in each case and for each severity level. The assessment of the effects should be developed more in depth by providing guidance. The SAH only provides two tables ('effect on safety in air traffic' and 'people in air traffic') which are developed as example in paragraph 6.1.3.

Without a common basis to assess the severity of the effects on operations, the safety assessment cannot be performed in a harmonized way within DFS.

#### Suggested Solution

DFS to provide information or guidance with regard to the assessment of the severity of the effects on each domain identified in ESARR4.

## 4.2 Detailed Analysis

### Analysis

Tables 2A and 2B include detailed information resulting from the comparison between ESARR 4, Sections 3 & 5 and the 'DFS Safety Assessment Methodology'. In all cases, only the literal text of ESARR 4 has been presented and comments include a first conclusion about the level of correspondence.

The issues identified from this analysis (in table 1) are described in more detail in the following tables (2A and 2B) and solutions proposed in section 4.

### Legend

- When the provisions of the PMC document are seen as equivalent or equal to the relevant requirement of ESARR 4, the sign “ = ” is used.
- When the provisions of the PMC document are seen as encompassing as a minimum and exceeding the relevant requirement of ESARR 4, the sign “ + ” is used.
- When the provisions of the PMC document are seen as less demanding than the relevant requirement of ESARR 4, the word “*Partially*” is used. Optionally a description may be added, in parentheses, to provide a value for the coverage of ESARR 4 in the PMC e.g. (*Mostly*), (*Little*).

- When the provisions of the PMC document are seen as less demanding than the relevant requirement of ESARR 4, the sign “ - ” is used.
- When the provisions of the PMC document differ or are inconsistent with the relevant requirement of ESARR 4, the sign “ # ” is used.
- When an issue is identified in one section of the table, this issue is not raised again in other sections of the table, i.e. scope is only addressed in the table against ESARR 4, section 5.1 and not within all parts.

*(Space Left Intentionally Blank)*

**TABLE 2A : DETAILED CORRESPONDENCE ANALYSIS FOR REQUIREMENTS 3.1, 3.2, 5.1, 5.2 AND 5.3**

<p><b>ESARR 4 Requirement 3.1</b></p> <p><i>This requirement shall apply to all providers of ATM services in respect of those parts of the ATM System and supporting services, within their managerial control.</i></p>	<p><b>Level of Correspondence</b></p> <p style="text-align: center;">=</p>
<p><b>Link to SAH/CDSA:</b> CDSA, Ch. 1</p>	
<p><b>DFS Statement:</b></p> <p>CDSA Chapter 1 states that: <i>"The present guideline applies to all staff of the DFS Deutsche Flugsicherung GmbH and to all employees of the German Federal Office of Civil Aviation (Luftfahrtbundesamt) seconded to the DFS".</i></p>	
<p><b>Comments:</b></p> <p>The directive covers DFS staff and any sub contractors and indeed goes further (in Ch 5) than the claim above, in that it requires assessment for any changes to the existing Air Traffic Management System for which DFS is responsible. However it could be improved by specifically describing its responsibility for services (supporting services) delivered to itself</p>	

<p><b>ESARR 4 Requirement 3.2</b></p> <p><i>This requirement shall apply to military ATM service providers except in those cases in which military ATS or Air Defence are only and exclusively involved in the control of military aircraft, in a segregated military airspace environment.</i></p>	<p><b>Level of Correspondence</b></p> <p style="text-align: center;">=</p>
<p><b>Link to SAH/CDSA:</b> SHA Version 1.02: Ch. 1,</p>	
<p><b>DFS Statement:</b></p> <p>SAH Version 1.02 states that the need to conduct systematic risk assessments also extends to all aspects of military air traffic management, as long as they are part of the integrated civil-military ATS conducted by DFS.</p>	
<p><b>Comments:</b></p> <p>Agreed, military services are included in the guidance material (SAH) but their inclusion is not made a requirement in the directive (CDSA). Consequently it might not be seen as a requirement. It is recommended that military services are included in the CDSA.</p>	

<p><b>ESARR 4 Requirement 5.1</b></p> <p><i>An ATM service provider shall ensure that hazard identification as well as risk assessment and mitigation are systematically conducted for any changes to those parts of the ATM System and supporting services within his managerial control, in a manner which :</i></p>	<p style="text-align: center;"><b>Level of Correspondence</b></p> <p style="text-align: center;"><b>Partially (Mostly)</b></p>
<p><b>Link to SAH/CDSA:</b> CDSA, SAH Version 1.02: Ch. 1,3,7,8,9,10</p>	
<p><b>DFS Statement:</b></p> <p>DFS Safety Policy (Corporate Safety Policy and Principles) as well as SAH Version 1.02 Chapter 1 states that <i>"...All new air navigation systems - and all modifications to operational air navigation systems - shall be assessed for their safety significance before implementation, and system functions shall be classified according to their criticality.</i></p> <p><i>The safety level to be met by each system function shall be defined.</i></p> <p><i>Safety analyses shall be performed and documented in order to ensure that due consideration is given to all technical and operational aspects, and that the corresponding safety level is met", and "All new airspace and flight procedures plans, as well as all new operational procedures for air navigation services and modifications to these shall be assessed in terms of safety aspects before implementation, and all planning and procedural components classified according to their criticality.</i></p> <p><i>Safety analyses shall be performed and documented in order to ensure that all planning and procedural aspects have been duly taken into account and that the defined safety level is met..."</i></p>	
<p><b>Comments:</b></p> <p>The first assessment outlines that:</p> <ol style="list-style-type: none"> <li>1) The CDSA doesn't specifically mention all new air navigation systems nor it states that airspace and flight procedure plans are considered as part of the system</li> <li>2) Mitigation is dealt with at less depth hazard than hazard identification and risk assessment</li> <li>3) Ch 9 allows the Safety Assessment to be performed on the "design" of the system, which would not satisfy a requirement for assurance that the implemented system mitigated the risks.</li> <li>4) Ch 9 also suggests the use of a Hazard Analysis where for an implemented system an FMEA would be more appropriate.</li> <li>5) Ch 9 does not specifically address verification of the safety requirements.</li> </ol> <p>The new version of the SAH provides improvements:</p> <ul style="list-style-type: none"> <li>■ With regard to the item 2), 3), 4) 5) above, an additional paragraph is provided page 12 of the SAH 2.02, changes are made to the §6.3 and in table 3 in A2 in appendix A. They address the issue in a satisfactory way:             <ol style="list-style-type: none"> <li>i. Page 12: "It has to be pointed out that the <b>Safety Requirements</b> and the additional <b>Safety Measures</b> are the essential means for mitigating any risk <u>before</u> a change becomes operational. Therefore they are essential elements of the Safety Assessment process. While Safety Requirements are an important input for the implementation of a change (and thus are based on the system's design and architecture), Safety Measures may be necessary to further reduce risk levels after the final risk assessment ("Safety Analysis" phase) has been carried out. Safety Measures therefore are based on the actual implementation of a system, not on the system's design!"</li> </ol> </li> </ul>	

- ii. Page 63: “verification” is added in paragraph 7 , safety analysis is based on the implemented system not only on the design of system (paragraph 3 and 9),
- iii. table 3 in annex A2 : verification of safety objectives and requirement, Refinement of hazard analysis (identification of all hazards, causes, effects), based on the actual behaviour of the system after implementation

- with regard to the item 1) above, page 9 of the SAH version 2.02: “The scope of a safety assessment not only contains the elements of the DFS part of the ATM system but also has to address the system environment that may be affected by a change. This includes the consideration of all airborne and ground components that are in some way related to the safety aspects of a change. In co-operation with the national regulator and – if necessary - the airspace users it has to be assured that all affected parties are involved in the process. Similarly, the safety properties of all third-party products and services used within the DFS ATM system must be assured by conducting hazard analyses and defining and verifying safety requirements for those products and services according to the methodology described in this handbook.”

However, with regard to the item 1), the CDSA does not specifically mention “All new air navigation systems” nor does it state that airspace and flight procedure plans etc are considered as part of the system. Consequently it might not be seen as a requirement. It is recommended that these changes to services are included in the CDSA.

Therefore **(issue 1)**, certain part of the system is not covered by the safety management of changes, as it is stated in the §5 of the CDSA: “ the only modification requiring safety assessment are procedures not included and for which no provision is made in the list of aforementioned documents –*in §5 and annex A of the CDSA-*“ and in §5 : “this means that procedures and projects that are

- fully governed by legislation;
  - fully covered by national and international standards,
  - fully established in DFS standards, guidelines and handbooks ;
- are not required to undergo any safety assessment”.

These claims are too restrictive and a safety assessment is required for those changes by ESARR 4 and ICAO Annex 11, Edition 13.

*(Space Left Intentionally Blank)*

<p><b>ESARR 4 Requirement 5.1 a</b></p> <p><i>An ATM service provider shall ensure that hazard identification as well as risk assessment and mitigation are systematically conducted for any changes to those parts of the ATM System and supporting services within his managerial control, in a manner which :</i></p> <p>a) <i>addresses the complete life-cycle of the constituent part of the ATM System under consideration, from initial planning and definition to post-implementation operations, maintenance and de-commissioning;</i></p>	<p><b>Level of Correspondence</b></p> <p style="text-align: center;">=</p>
<p><b>Link to SAH/CDSA:</b> SAH Version 1.02 : Ch 4,5</p>	
<p><b>DFS Statement:</b></p> <p>SAH Version 1.02 Chapter 4 states that <i>"... a safety analysis is conducted in different phases, which are very similar to the phases of the life cycle of a system:</i></p> <div data-bbox="384 817 1209 1310" data-label="Diagram"> <pre> graph TD     A[System Definition] --&gt; B[System Design]     B --&gt; C[System Implementation]     C --&gt; D[Operation]     D --&gt; E[Decommissioning]          A --- A1[How safe does the system need to be? („Functional Hazard Analysis“)]     B --- B1[Which safety precautions are necessary? („Safety Requirements“)]     C --- C1[How safe is the system? („Safety Analysis“)]     D --- D1[How safe is the system? („Safety Analysis“)]     E --- E1[Decommissioning Safety Assessment]     </pre> </div> <p>SAH covers the whole life cycle.</p>	
<p><b>Comments:</b></p> <p>The previous assessment raised an issue with regard to the system implementation phase and operation which seemed to include respectively installation and maintenance. The second assessment takes into account the following assumptions:</p> <ul style="list-style-type: none"> <li>■ the "system implementation" includes the installation phase;</li> <li>■ the "operation" includes the maintenance.</li> </ul> <p>Therefore, version 2.02 of the SAH provides (page 11) clarification with regard to the "safety analysis" performed during those phases of the life cycle:</p> <p><i>"The completed system draft and the developed system at a later stage are subsequently subjected to a full safety analysis, which detects all remaining risks and forms the basis for the further safety measures to be taken. Hence, such a safety analysis is conducted at the end of the implementation phase but must, however, be checked and, if necessary, complemented on a regular basis during safety checks while the system is in operation. In addition, every change made to the system during its operation must be assessed in accordance with the methods described in this handbook.</i></p>	

*The Transition phase usually is regarded as part of the Implementation phase and has to be considered explicitly during the safety assessment. In some cases the transition itself will be complex (or risk bearing) enough to be counted as a change of its own. In these cases it is a good idea to conduct a separate safety assessment for the transition phase. Decommissioning a system represents a special type of change, which also must undergo a systematic risk assessment."*

<p><b>ESARR 4 Requirement 5.1 b:</b></p> <p><i>An ATM service provider shall ensure that hazard identification as well as risk assessment and mitigation are systematically conducted for any changes to those parts of the ATM System and supporting services within his managerial control, in a manner which :</i></p> <p><i>b) addresses the airborne and ground components of the ATM System, through co-operation with responsible parties; and</i></p>	<p><b>Level of Correspondence</b></p> <p><b>=</b></p>
<p><b>Link to SAH/CDSA:</b> CDSA, SAH Version 1.02 : Ch. 1,3</p>	
<p><b>DFS Statement:</b></p> <p>ESARR 4 requires a "total system approach" for the hazard identification, risk assessment and the risk mitigation strategy. The purpose of SAH Version 1.02 Chapter 5 is to outline a method to analyse hazards and risks in a holistic perspective. The method employed is the Bayesian Network approach. Bayesian Networks are also known as belief networks, causal probabilistic networks, causal nets, graphical probability networks, probabilistic cause-effect models, and probabilistic influence diagrams.</p>	
<p><b>Comments:</b></p> <p>The first assessment outlined that there are no requirements for :</p> <ul style="list-style-type: none"> <li>■ the airborne parts and the services delivered to DFS as part of the ATM services (telecom, power),</li> <li>■ technical agreements with third party service providers.</li> </ul> <p>Version 2.02 of the SAH provides (page 9) clarification with scope of the safety assessment and provide an additional reference to a procedure dealing with external services:</p> <ul style="list-style-type: none"> <li>■ The scope of a safety assessment not only contains the elements of the DFS part of the ATM system but also has to address the system environment that may be affected by a change. This includes the consideration of all airborne and ground components that are in some way related to the safety aspects of a change. In co-operation with the national regulator and, if necessary, the airspace users it has to be assured that all affected parties are involved in the process. Similarly, the safety properties of all third-party products and services used within the DFS ATM system must be assured by conducting hazard analyses and defining and verifying safety requirements for those products and services according to the methodology described in this handbook.</li> <li>■ Assurance and Demonstration of the Safety of External Services, V 1.0, DFS 2003.</li> </ul>	

<p><b>ESARR 4 Requirement 5.1 c:</b></p> <p><i>An ATM service provider shall ensure that hazard identification as well as risk assessment and mitigation are systematically conducted for any changes to those parts of the ATM System and supporting services within his managerial control, in a manner which :</i></p> <p>c) <i>addresses the three different types of ATM elements (human, procedures and equipment), the interactions between these elements and the interactions between the constituent part under consideration and the remainder of the ATM System.</i></p>	<p style="text-align: center;"><b>Level of Correspondence</b></p> <p style="text-align: center;">=</p>
<p><b>Link to SAH/CDSA:</b> SAH Version 1.02 : Ch.3,7 and Se. 4.2, 5.1</p>	
<p><b>DFS Statement:</b></p> <p>SAH Version 1.02 Chapter 7 covers guidance on how to identify hazards in a manner which addresses the whole System (human, procedures and equipment and their interactions).</p> <p>SAH Version 1.02 Chapter 3 states that " ... the term "system" should not be interpreted to strictly mean a technical (or technical air navigation services) system, rather it should be regarded as the interaction of all components, which is necessary for performing a task or a function. In this Handbook, the term "system" should always be understood in this way. ..." SHA Version 1.02 Chapter 6 and 7 does provide a detailed guidance on how to identify hazards as well as how to assess and mitigate risks systematically.</p>	
<p><b>Comments:</b></p> <p>The first assessment raised that interactions between these elements within the constituent part and interactions between the constituent part and the rest of the ATM system where are not overtly covered. In particular, the interactions between elements within the constituent part, which relate to hazards that arise during development due to design decisions made, are not clearly identified in the SAH Version 1.02.</p> <p>Making the assumption that the description of this impact analysis allows to keep traceability all along the life cycle of the system and could be used at each stage as a continuous process and not only for the development of a specific project, the version 2.02 of the SAH provides (page 42) highlight the impact analysis done by the DFS in figure 19 (process description) and figure 20 (the interaction between the various elements within the system).</p>	

(Space Left Intentionally Blank)



<p><b>ESARR 4 Requirement 5.2 a:</b></p> <p><i>The hazard identification, risk assessment and mitigation processes shall include:</i></p> <p>a) <i>a determination of the scope, boundaries and interfaces of the constituent part being considered, as well as the identification of the functions that the constituent part is to perform and the environment of operations in which it is intended to operate;</i></p>	<p style="text-align: center;"><b>Level of Correspondence</b></p> <p style="text-align: center; color: green; font-size: 2em;">+</p>
<p><b>Link to SAH/CDSA:</b> SAH Version 1.02 : Se. 4.2, 4.4, 4.5, 4.6, 7.1, 7.2, Ch. 9, 10 Ch. 7 (Introduction), Se. 7.1</p>	
<p><b>DFS Statement:</b></p> <p>SAH Version 1.02 Section 7.1 does provide guidance on how to describe the constituent part being considered in terms of processes, working steps, roles, objects, information and organisational aspects. As stated, this kind of system description defines scope, boundaries, interfaces and functions. The SAH Version 1.02 system description is also a perfect basis for hazard analysis and risk assessment and exceeds the ESARR 4 requirement.</p>	
<p><b>Comments:</b></p> <p>Agreed, the derivation of safety objectives is described well.</p>	

<p><b>ESARR 4 Requirement 5.2 b i</b></p> <p><i>The hazard identification, risk assessment and mitigation processes shall include:</i></p> <p>b) <i>a determination of the safety objectives to be placed on the constituent part, incorporating :</i></p> <p style="padding-left: 20px;"><i>i) an identification of ATM-related credible hazards and failure conditions, together with their combined effects,</i></p>	<p style="text-align: center;"><b>Level of Correspondence</b></p> <p style="text-align: center; color: blue; font-size: 2em;">=</p>
<p><b>Link to SAH/CDSA:</b> SAH Version 1.02 : Se. 4.2, 4.4, 4.5, 4.6, 7.1, 7.2, Ch. 9, 10 Ch. 5 (Introduction), 7,8</p>	
<p><b>DFS Statement:</b></p> <p>SAH Version 1.02 Chapter 7 covers guidance on how to identify ATM-related hazards in a manner which addresses the whole system. SAH Version 1.02 section 5.2 outlines how to organize hazards, causes and effect in an event tree (Bayesian Network).</p>	
<p><b>Comments :</b></p> <p>The first assessment raised issues with regard to the coverage of multiple accidents/incidents which tends to focus on the most severe accident/incident (6.1).</p> <p>The version 2.02 of the SAH provides 45 paragraph 3 identified the “n to m” relation:</p> <p>“It has to be noted, that on the one hand a group of hazards may lead to the same effect, and that on the other hand a single hazard may (and usually will) lead to various different effects. Thus, the hazard-effect relationship is not a “1-to-1 relation”, rather (technically speaking) a “n-to-m relation”!</p> <p>In addition, the example provided by DFS highlight the n:m relations in documentation.</p>	

<p><b>ESARR 4 Requirement 5.2 b ii</b></p> <p><i>The hazard identification, risk assessment and mitigation processes shall include:</i></p> <p>b) <i>a determination of the safety objectives to be placed on the constituent part, incorporating :</i></p> <p><i>ii) an assessment of the effects they may have on the safety of aircraft, as well as an assessment of the severity of those effects, using the severity classification scheme provided in Appendix A, and</i></p>	<p><b>Level of Correspondence</b></p> <p style="text-align: center;">=</p>
<p><b>Link to SAH/CDSA:</b> SAH Version 1.02 : Se. 4.2, 4.4, 4.5, 4.6, 7.1, 7.2, Ch. 9, 10 Se. 5.5, 6.1, 6.2, App. 4</p>	
<p><b>DFS Statement:</b></p> <p>All effects and causal relations between hazards and effects are presented in an event tree. SAH Version 1.02 chapter 6 covers a detailed description on how to assess the effects of hazards and how to assess the severity of those effects using the "DFS severity classification scheme". This scheme is divided into three sections. The first section describes the "effect on safety in air traffic" and contains the definitions and examples predetermined by the SRC.</p>	
<p><b>Comments:</b></p> <p>Agreed, the assessment of the effects of hazards (accidents/incidents) is handled well, as is the assessment of the severity of the effects.</p> <p>However, the SAH does not provide guidance to identify and assess hazards. The assessment of the effects should be developed more in depth by providing guidance. The SAH provides only two tables ('effect on safety in Air Traffic' and 'people in Air Traffic') which are developed as example in paragraph 6.1.3.</p> <p>Without a common basis to assess the severity of the effects on operations, the safety assessment cannot be performed in an harmonised way within DFS (observation 2).</p>	

(Space Left Intentionally Blank)

<p><b>ESARR 4 Requirement 5.2 b iii</b></p> <p><i>The hazard identification, risk assessment and mitigation processes shall include:</i></p> <p>b) <i>a determination of the safety objectives to be placed on the constituent part, incorporating :</i></p> <p><i>iii) a determination of their tolerability, in terms of the hazard's maximum probability of occurrence, derived from the severity and the maximum probability of the hazard's effects, in a manner consistent with Appendix A;</i></p>	<p style="text-align: center;"><b>Level of Correspondence</b></p> <p style="text-align: center;">=</p>
<p><b>Link to SAH/CDSA:</b> SAH S Version 1.02e. 4.2, 4.4, 4.5, 4.6, 7.1, 7.2, Ch. 9, 10 Se. 6.3, 6.4, 7.3, App. 4</p>	
<p><b>DFS Statement:</b></p> <p>The calculus on how to determine the hazards maximum probability using a Bayesian network has a long history in statistics. SHA Version 1.02 section 7.3 covers basic guidance on how to derive quantified safety objectives from the identified hazards. SHA Version 1.02 section 7.3 shows that safety objectives are thus requirements on the maximum frequency of the identified hazards. This frequency results from the severity classes of all effects, their conditional probabilities and the maximum permissible frequencies according to the "DFS-Risk-Matrix". SAH Version 1.02 Appendix 4 covers the derivation of the "DFS-Risk-Matrix" from the European safety minimum.</p>	
<p><b>Comments:</b></p> <p>Agreed, the method of determining the tolerability of a hazard uses a bayesian net, which appears to be well suited for this application.</p> <p>However (<b>observation 1</b>) the use of Bayesian net needs to be carefully controlled because of the confidence which have to be made to probabilities and experts views. Despite ways forward stated in §6.1.4. in SAH version 2.02, they should be developed more in depth in order to guarantee the validity of the figures used in Bayesian networks.</p>	

(Space Left Intentionally Blank)

<p><b>ESARR 4 Requirement 5.2 c i</b></p> <p><i>The hazard identification, risk assessment and mitigation processes shall include:</i></p> <p>c) <i>the derivation, as appropriate, of a risk mitigation strategy which :</i></p> <p style="padding-left: 40px;"><i>i) specifies the defences to be implemented to protect against the risk-bearing hazards,</i></p>	<p style="text-align: center;"><b>Level of Correspondence</b></p> <p style="text-align: center;">=</p>
<p><b>Link to SAH/CDSA:</b> SAH Version 1.02 : Se. 4.2, 4.4, 4.5, 4.6, 7.1, 7.2, 7.3, Ch. 8, 9, 10</p>	
<p><b>DFS Statement:</b></p> <p>SAH Version 1.02 Chapter 10 specifies several possibilities how to place safety measures against risk bearing hazards.</p>	
<p><b>Comments (Issue 3):</b></p> <p>The first assessment showed that the requirement for risk mitigation strategy shall be improved in order to avoid the point where, in a contract to external supplier for instance, the component is treated as a “black box”. This could lead to a risk that unspecified behaviours remain undisclosed and their contribution to the resulting emergent properties may cause an accident/incident. Neither the CDSA nor the SAH cover the management of contracts in sufficient detail for this risk to be mitigated.</p> <p>The version 2.02 of the SAH provides page 65 in 6.3.1 paragraph 2 clarify the point:</p> <p><i>“During this step care must be taken to analyse the system components as they are after the change has been implemented. This includes the analysis of the behaviour of and possible hazards resulting from those components supplied by third parties. It has to be ensured that those parts behave exactly as required and will not cause additional hazards.”</i></p> <p>In addition a process applied to external suppliers is identified as a reference in appendix A.8.</p>	

(Space Left Intentionally Blank)

<p><b>ESARR 4 Requirement 5.2 c ii</b></p> <p><i>The hazard identification, risk assessment and mitigation processes shall include:</i></p> <p>c) <i>the derivation, as appropriate, of a risk mitigation strategy which :</i></p> <p><i>ii) includes, as necessary, the development of safety requirements potentially bearing on the constituent part under consideration, or other parts of the ATM System, or environment of operations, and</i></p>	<p><b>Level of Correspondence</b></p> <p style="text-align: center;">=</p>
<p><b>Link to SAH/CDSA:</b> SAH Version 1.02 : Se. 4.2, 4.4, 4.5, 4.6, 7.1, 7.2, 7.3, Ch. 8, 9, 10</p>	
<p><b>DFS Statement:</b></p> <p>SAH version 1.02 Chapter 8 requires the preparation of safety requirements.</p>	
<p><b>Comments:</b></p> <p>The first assessment raised that defences may stem from other parts of the ATM system, therefore requirements would have to be written for them as well. This aspect is not covered.</p> <p>The version 2.02 of the SAH page 61 in 6.2.3 paragraph 3 clarifies the point:</p> <p><i>“It shall be noted that safety defences may also stem from other parts of the ATM system and thus requirements would have to be written for them as well. In every case the system environment has to be considered and take into account when defining safety requirements.”</i></p>	

(Space Left Intentionally Blank)

<p><b>ESARR 4 Requirement 5.2 c iii</b></p> <p><i>The hazard identification, risk assessment and mitigation processes shall include:</i></p> <p>c) <i>the derivation, as appropriate, of a risk mitigation strategy which :</i></p> <p><i>iii) presents an assurance of its feasibility and effectiveness</i></p>	<p><b>Level of Correspondence</b></p> <p style="text-align: center;"><b>=</b></p>
<p><b>Link to SAH/CDSA:</b> SAH Version 1.02 issue : Se. 4.2, 4.4, 4.5, 4.6, 7.1, 7.2, 7.3, Ch. 8, 9, 10</p>	
<p><b>DFS Statement:</b></p> <p>SAH Version 1.02 includes various statements confirming validation of safety requirements (see section 4.5, chapter 9 and 10.</p>	
<p><b>Comments:</b></p> <p>It has been raised during the previous assessment that the risk mitigation strategy will be to have a process which identifies the requirements (safety) for the measures to be taken to mitigate the risks. For this strategy, the individual requirements will have to be feasible i.e. they must be implementable and verifiable. For the strategy to be effective, the set of safety requirements have to mitigate the whole risk. The references given above in the SAH didn't cover the point.</p> <p>The version 2.02 of the SAH page 62 in 6.2.3 paragraph 3 provides a clarification:</p> <p><i>"It goes without saying that it is to be carefully ascertained whether or not safety requirements have been met before the system is put into operation (and, for that matter, before a new procedure is operationally approved). Therefore, during the second phase of a safety assessment, plausible arguments have to be provided that all the safety requirements are feasible, i. e. that they are actually implementable and verifiable. To ensure this, acceptance criteria shall be available which refer to these requirements. It must be checked whether these criteria are met before the operational approval is issued Currently, there are no set methods for determining safety requirements. However, some general rules can be stated:</i></p> <ul style="list-style-type: none"> <li>• <i>Safety requirements are required measures which are suitable to fulfil the safety objectives formulated within the framework of the Functional Hazard Analysis.</i></li> <li>• <i>Safety requirements are a special type of user requirements, and it must equally be possible to turn them into concrete acceptance criteria, i.e. to verify them before commissioning the system. The definition of acceptance criteria also ensures the feasibility of the requirements."</i></li> </ul>	

(Space Left Intentionally Blank)

<p><b>ESARR 4 Requirement 5.2 d</b></p> <p><i>The hazard identification, risk assessment and mitigation processes shall include:</i></p> <p>d) <i>verification that all identified safety objectives and safety requirements have been met</i></p> <p style="padding-left: 20px;">i) <i>prior to its implementation of the change,</i></p> <p style="padding-left: 20px;">ii) <i>during any transition phase into operational service,</i></p> <p style="padding-left: 20px;">iii) <i>during its operational life, and</i></p> <p style="padding-left: 20px;">iv) <i>during any transition phase till decommissioning.</i></p>	<p style="text-align: center;"><b>Level of Correspondence</b></p> <p style="text-align: center;">=</p>
<p><b>Link to SAH/CDSA:</b> CDSA Ch 7, Appendix F, SAH Version 1.02 : Se. 4.2, 4.4, 4.5, 4.6, 4.9, 7.1, 7.2, Ch. 9, 10</p>	
<p><b>DFS Statement:</b></p> <p>SAH Version 1.02 chapter 4 and 9 requires a risk assessment and mitigation process. This process includes the verification that all identified safety objectives and safety requirements have been met (see SHA chapter 9, last page and CDSA Appendix F). CDSA chapter 7 states that "<i>The modification under assessment may not be implemented or brought into effect prior to final clearance of the safety assessment documented by the signatures referred to in Section 6.2.</i>"</p>	
<p><b>Comments:</b></p> <p>The first assessment showed that the translation provided of the CDSA (Appendix F) didn't not contain any material specifically related to the verification of either the safety requirements or safety objectives, and this activity was not well described in the SAH.</p> <p>The safety properties of the implementation are verified via the use of the baysian network. The justification of claims made in the baysian network are recorded by the RAMSYS tool and associated with each element of the network. The DFS safety requirements are verified by application of the SSA process. All of this is brought together and completely documented at the end of the project by application of the safety analysis process.</p> <p>The version 2.02 of the SAH page 78 in A2 table 3, working step 7 "Assessment of effects (severity, conditional probability, frequency)" provides a clarification with regard to the process:</p> <ul style="list-style-type: none"> <li>■ <i>Objective : to collect all information required for risk assessment. Verification of safety objectives and safety requirements;</i></li> <li>■ <i>Result : complete Bayesian event network, including verification of safety objectives. By application of acceptance criteria, verification of safety requirements.</i></li> </ul>	

(Space Left Intentionally Blank)

<p><b>ESARR 4 Requirement 5.2 (Note 1)</b></p> <p><i>It is considered as essential that the activities depicted in a), b), c) and d) are fully co-ordinated between those parties responsible for developing and implementing the safety requirements bearing on the constituent parts of the ATM System). See 5.1 (b) above.</i></p>	<p style="text-align: center;"><b>Level of Correspondence</b></p> <p style="text-align: center;">=</p>
<p><b>Link to SAH/CDSA:</b> CDSA, Ch. 6 (Introduction, Se. 6.2, App. 2)</p>	
<p><b>DFS Statement:</b></p> <p>CDSA Chapter 6 specifies roles, responsibility and tasks in conducting a Safety Assessment. Section 6.2 states "... As a general rule, all organisational units affected by the modification subject to assessment should be involved in conducting the safety evaluation. These include not only the operating unit (for technical system elements) but also all current and future users, represented where appropriate by one or more representative units. A safety assessment that does not involve internal users is not permitted. ..."</p>	
<p><b>Comments:</b></p> <p>The CDSA provides an adequate set of requirements for co-ordinating the hazard identification, risk assessment and mitigation processes for development within DFS but it does not adequately cover co-ordination with external parties.</p> <p>The version 2.02 of the SAH page 9 and in page 97 covers item with regard to the third parties.</p>	

<p><b>ESARR 4 Requirement 5.2 (Note 2)</b></p> <p><i>It is recognised that a combination of quantitative (e.g, mathematical model, statistical analysis) and qualitative (e.g. good working processes, professional judgement) arguments may be used to provide a good enough level of assurance that all identified safety objectives and requirements have been met.</i></p>	<p style="text-align: center;"><b>Level of Correspondence</b></p> <p style="text-align: center;">=</p>
<p><b>Link to SAH/CDSA:</b> SAH: Ch. 5</p>	
<p><b>DFS Statement:</b></p> <p>Bayesian networks provide a robust, probabilistic method of reasoning with uncertainty. BN is the best known method to cover quantitative and qualitative arguments in a single model. However, an observation has been raised (observation 1) with regard the control of the use of Bayesian networks.</p>	
<p><b>Comments:</b></p> <p>Agreed, Bayesian networks provide a robust, probabilistic method of reasoning with uncertainty. However the use of Bayesian networks for reasoning in the presence of uncertainty has not been described in any detail. That uncertainty is being dealt with in any way at all may go "over the head" of a reader! DFS has stated that the whole section on baysian networks has been rewritten in version 2 of the SAH and covers this issue (please refer to the observation made above in ESARR 4 Requirement 5.2 b iii).</p>	



<p><b>ESARR 4 Requirement 5.3 a)</b></p> <p><i>The results, associated rationales and evidence of the risk assessment and mitigation processes, including hazard identification, shall be collated and documented in a manner which ensures:</i></p> <p>a) <i>that correct and complete arguments are established to demonstrate that the constituent part under consideration, as well as the overall ATM System are, and will remain, tolerably safe including, as appropriate, specifications of any predictive, monitoring or survey techniques being used;</i></p>	<p style="text-align: center;"><b>Level of Correspondence</b></p> <p style="text-align: center;">=</p>
<p><b>Link to SAH/CDSA:</b> SAH Version 1.02 , Ch. 11</p>	
<p><b>DFS Statement:</b></p> <p>SAH Version 1.02 describes the use of a documentation and collating tool (RAMSYS) which is used to conduct a safety assessment and document its result in a unified way.</p>	
<p><b>Comments:</b></p> <p>There is no evidence that requirement 5.3 a) has been met. It is difficult to find text that supports the consideration of a “correct and complete argument”. Moreover it is not clear what the meaning of “...specifications of any predictive, monitoring or survey techniques...” is in the DFS context and therefore it is difficult to establish if this clause of 5.3 a) has been satisfied.</p> <p>For the second assessment the DFS provides the SRU with an example of the use of RAMSYS:Handbuch der Sicherheitsbewertungen Band II V10, which covers the requirement.</p>	

<p><b>ESARR 4 Requirement 5.3 b)</b></p> <p><i>The results, associated rationales and evidence of the risk assessment and mitigation processes, including hazard identification, shall be collated and documented in a manner which ensures:</i></p> <p>b) <i>that all safety requirements related to the implementation of a change are traceable to the intended operations/functions.</i></p>	<p style="text-align: center;"><b>Level of Correspondence</b></p> <p style="text-align: center;">=</p>
<p><b>Link to SAH/CDSA:</b> SAH Version 1.02 , Ch. 4.3, 7.3, 7.4, 11</p>	
<p><b>DFS Statement:</b></p> <p>As shown in SAH Version 1.02 (Fig 5, pp 14 &amp; 15), safety requirements have to be derived from safety objectives and safety criticality. These, in turn, are directly linked with hazards and system components, which, in turn, are linked with system functions, processes and work steps (Ref: SAH CH 7.3 &amp; 7.4). Thus, each requirement is always traceable to operations/functions. Moreover, the SAH describes the use of a documentation and collating tool (RAMSYS – SAH Ch 11) which is used to conduct a safety assessment and document its result in a unified way.</p>	
<p><b>Comments:</b></p> <p>Agreed.</p>	

**TABLE 2B – DETAILED CORRESPONDENCE ANALYSIS FOR APPENDIX A**

<p><b>ESARR 4 Requirement A-1 (1)</b>  <i>The severity of the effects of hazards in that environment of operations shall be determined using the classification scheme shown in <b>Figure A-1</b></i></p>	<p><b>Level of Correspondence</b>  =</p>
<p><b>Link to SAH/CDSA:</b> SAH: Ch. 6</p>	
<p><b>DFS Statement:</b>                  The Severity Classification Scheme used by DFS contains the definitions and examples predetermined by EUROCONTROL or equivalent to those. The risk classification scheme defined in SAH section 6.4 is fully consistent with the risk classification in ESARR 4.</p>	
<p><b>Comments:</b>                  The DFS severity scheme has 4 categories. The most severe is clearly related to ESARR 4 although its description contains fewer examples.                  The other three categories all relate to infringements of separation although their descriptions do not use the same words as are used in ESARR 4 so it is difficult to judge if the boundaries will be the same. It would be of benefit if there were a description of the meaning of the DFS categories of separation infringement (A – C) in the SAH.</p>	

<p><b>ESARR 4 Requirement A-1 (2)</b>  <i>As there is no such scheme today as an accident/incident causation model, the severity classification shall rely on a specific argument demonstrating the most probable effect of hazards, under the worst case scenario.</i></p>	<p><b>Level of Correspondence</b>  =</p>
<p><b>Link to SAH/CDSA:</b> SAH Version 1.02 : Se. 6.1, Se. 7.2</p>	
<p><b>DFS Statement:</b>                  SAH Version 1.02 clearly states in Chapter 6: “<i>The question which must be asked is: "What can happen <b>in the worst-case scenario</b>, but under <b>plausible and realistic conditions</b>, if the hazard does actually occur?" (We also call this the “reasonably pessimistic” approach.)</i>” Additionally, the DFS methodology requires not only the “most probable” effect to be analysed, but also other effects that may be less probable but could possibly result in a higher risk.</p>	
<p><b>Comments:</b>                  Agreed, the DFS method stresses that all plausible accidents and incidents should be assessed and not just those leading to severity class 1 results.                  However, DFS could give more information, in term of process, in order to provide assurance that the most probable effect of hazards under the worst case scenario is adequately taken into consideration with the Bayesian network approach (please refer to the observation made above in ESARR 4 Requirement 5.2 b iii).</p>	

<p><b>ESARR 4 Requirement A-1 (3)</b></p> <p>In order to deduce the effect of a hazard on operations and to determine its severity, the systematic approach/process shall include (but not be restricted to) the effects of hazards on the various elements of the ATM System, such as:</p> <ul style="list-style-type: none"> <li>■ Effect of hazard on air crew, (e.g. workload, ability to perform his/her functions);</li> <li>■ Effect of hazard on the Air Traffic Controllers, (e.g. workload, ability to perform his/her functions);</li> <li>■ Effect of hazard on the aircraft functional capabilities;</li> <li>■ Effect of hazard on the functional capabilities of the ground part of the ATM System;</li> <li>■ Effect of hazard on the ability to provide safe Air Traffic Management Services; (e.g. magnitude of loss or corruption of Air Traffic Management Services/functions).</li> </ul>	<p style="text-align: center;"><b>Level of Correspondence</b></p> <p style="text-align: center;">=</p>
<p><b>Link to SAH/CDSA:</b> SAH Version 1.02 : Se. 6.2.2</p>	
<p><b>DFS Statement:</b></p> <p>While the severity classification scheme may be somewhat generic, the description and examples given in SAH Version 1.02 , Chapter 6 clearly demonstrate, that the DFS methodology requires the effects of hazards on air crew, ATCOs, aircraft functional capabilities etc. to be assessed during all three stages of the Safety Assessment process.</p>	
<p><b>Comments:</b></p> <p>The first assessment raised that the five categories of effects listed in the requirement were not included in SAH 1.02 and neither are they expanded upon.</p> <p>The version 2.02 of the SAH page 47 gives a partial solution to this issue:</p> <p><i>“While assessing the severity of an effect, various aspects have to be taken into accounts. Among those are the effect is the:</i></p> <ul style="list-style-type: none"> <li>• <i>air crew (e. g. workload, ability to perform the necessary functions)</i></li> <li>• <i>air traffic controllers (e. g. workload, ability to perform the necessary functions)</i></li> <li>• <i>aircraft functional capabilities</i></li> <li>• <i>functional capabilities of the ground parts of the ATM system</i></li> <li>• <i>ability to provide safety ATM services (e. g. magnitude of loss of corruption of ATM services/functions).</i></li> </ul> <p><i>The following table provides some examples of effects and hazards, which – in the worst case – may lead to such effects.”</i></p> <p>However, despite this paragraph in SAH is compliant with ESARR 4, there remains a need to further develop guidance in order to assess the severity of such effects <b>(observation 2)</b>.</p>	

<p><b>ESARR 4 Requirement A-2 (1)</b></p> <p><i>Safety objectives based on risk shall be established (1) in terms of the hazard's maximum probability of occurrence, derived both from the severity of its effect, according to <b>Figure A-1</b> and from the maximum probability of the hazard's effect, according to <b>Figure A-2</b>.</i></p>	<p style="text-align: center;"><b>Level of Correspondence</b></p> <p style="text-align: center;">=</p>
<p><b>Link to SAH/CDSA:</b> SAH: Se. 7.3</p>	
<p><b>DFS Statement:</b></p> <p>This is exactly the way Safety Objectives are derived by the DFS methodology. This is described in SAH.</p>	
<p><b>Comment:</b></p> <p>The SAH provides a good clear exposition of the way a Safety Objective is derived. In the case of DFS this involves apportioning the TLS given in ESARR 4. In the defined method of apportioning accident/incident frequencies to systems and their components, DFS has taken advantage of the principle of conservative design. DFS has started this apportionment process by calculating the annual accident rate for Germany as a whole from: the ESARR 4 TLS, knowledge of the number of aircraft using German airspace and the time for which they remain in German airspace. This seems to be a very rational way of defining the national risk budget. Furthermore, if the ECAC ATM Strategy for 2000+ is used as the fundamental objective, this value should not need to change over time.</p> <p>Such an apportionment process is anticipated by ESARR 4: "(Note: Figure A-2 only refers to an overall safety performance of ATM at ECAC and national level and is not directly applicable to the classification of individual hazards. To achieve this, a method of apportionment of the overall probability to the constituent parts of the ATM system may need to be developed. This apportionment may be done per phase of flight and/or, per accident types.)"</p> <p>During the first assessment, a need was identified to make consistent the target defined for design and the achieved target in operation. It appears that the scope of the safety target for design and the scope of achieved safety target in operation are not the same, the latest includes many more elements in its calculation which cannot be easily isolated, e.g. training, controller's experience, etc. The second figure (achieved safety level) is aiming at monitoring the overall system, as required by Annex 11 §2.26, and not at providing objective for building new systems or for implementing the changes. Further work within the SRU has the objective of clarifying this difference between safety target for design and achieved safety level.</p> <p>The second issue raised by the first assessment is that for the model to be practical data to validate must be available in a reasonable timeframe. The rationale of this issue was that the least conservative target level of safety for a level "d" risk is one accident every 15,000 years, which seemed unmeasurable.</p> <p>One accident every 15,000 years for such a risk is a way to express a frequency of acceptable occurrence of a hazard depending of the severity of the effect, which is the result of the derivation of the <math>1.55 \cdot 10^{-8}</math> established for the highest class of risk in ESARR 4, for the design of system and accepted by the SRC. Several assumptions have been made which lead to a distribution which meets the hypothesis required by ESARR 4. The apportioned values are calculated using of this distribution.</p> <p style="text-align: right;">cont...</p>	

However, (observation 1) the second assessment wishes to draw the attention of DFS to the use of a quantitative approach with regard to the “mechanics” of Bayesian networks. The quantitative results and the decision with regard to the severity class of effects rely on the validity of two main types of variables: the frequencies of the hazard and/or the conditional probability of the effect.

Therefore, those figures, dealing with radar failure, radio failure, or any other subsystem failure, human factors, etc. shall be established and validated as far as possible *a priori*, otherwise as the model relies on a calculation, it could easily lead to wrong probabilities. It should be ensured that the values used in Bayesian network is under the control of a process which, if necessary, periodically validates and improves those values (gathering of operational data, validation of expert’s panels, mathematical/statistical modelling, etc.). Such a process is referred to, but not clearly established, in the SAH.

ESARR 4 requires that “*the severity classification shall rely on a specific argument demonstrating the most probable effect of hazards, under the worst case scenario*”. The methodology detailed in SHA deals with this requirement in §6.1.3 (Assessing the severity of effects). However, it is not clear, in terms of process, that this approach is totally taken into account in Bayesian network.

On the basis of the documents provided for the assessment, the process described by DFS doesn’t contradict ESARR 4 and appears compliant. With regard to the use of Bayesian networks, it would be an improvement to provide complementary information in order to ensure that their use is validated, supported by qualitative arguments (as it could be done by a PSSA phase), under control of experts and cannot be misused.

(Space Left Intentionally Blank)

<p><b>ESARR 4 Requirement A-2 (2)</b></p> <p><i>As a necessary complement to the demonstration that these quantitative objectives are met, additional safety management considerations shall be applied so that more safety is added to the ATM system whenever reasonable.</i></p>	<p style="text-align: center;"><b>Level of Correspondence</b></p> <p style="text-align: center;">=</p>
<p><b>Link to SAH/CDSA:</b> SAH: Se. 6.4, App. A.4</p>	
<p><b>DFS Statement:</b></p> <p>As shown by the DFS Risk Matrix and explained in Appendix A.4, DFS has introduced the concept of “tolerable” risks (risk class “c”). Those risks span a range of two orders of magnitude in the frequency of occurrence between the Safety Minimum defined by ESARR 4 and the Safety Level DFS considers “acceptable”. That means, that enough precautions have been taken to ensure that the overall accident/incident probability introduced by total number of risks is always much lower than the ECAC Safety Target. In fact, safety objectives are derived in a way to ensure that all risks are “acceptable” instead of “tolerable”.</p>	
<p><b>Comment:</b></p> <p><b>At the first assessment it was established that</b> the DFS method does indeed make it clear that a class d risk should be the aim for the design of any change. During the AMC panel meeting, it was raised that class b could, in certain cases, be tolerated for a limited period of time in order to ensure that process is justified and documented, the following paragraph is added in version 2.02: <i>“Risks of classes a and b are unacceptable. The difference between both classes is that class “a” risks cannot – under any circumstances – be tolerated, while class “b” risks can be tolerated for a limited period of time, provided it can be proven that it is not possible to reduce the risk. However, the DFS Board of Managing Directors is always required to make a conscious and <u>documented decision in each case</u>”</i></p>	

(Space Left Intentionally Blank)

### 4.3 ESARR 4 Mandatory Provisions: Sections 6 and 7

#### Analysis

Table 2 Coverage Analysis – Mandatory Provisions provides for a coverage analysis of the contents of the following documents, for those mandatory provisions included in ESARR 4:

- CDSA
- SAH
- DAR

In table 2 the following abbreviation is used when both documents are addressed: DAM (DFS Assessment Methodology)

#### Legend

- When the provisions of CDSA and SAH are seen as equivalent or equal to the relevant requirement of ESARR 4, the sign “ = ” is used.
- When the provisions of CDSA and SAH are seen as encompassing a minimum and exceeding the relevant requirement of ESARR 4, the sign “ + ” is used.
- When the provisions of CDSA and SAH are seen as less demanding than the relevant requirement of ESARR 4, the sign “ - ” is used.
- When the provisions of CDSA and SAH differ or are inconsistent with the relevant requirement of ESARR 4, the sign “ # ” is used.

#### Summary of Initial Conclusions

- Annex F of the CDSA specifies exemptions for the implementation of most parts of the FHA and SSA specified. In this case the usefulness of the implementation of the SSA in this case should be revisited.
- The DAR provided for assessment is in German.

*(Space Left Intentionally Blank)*

ESARR 4	Covered by DAM	Coverage	Related comments
SECTION 6- IMPLEMENTATION			
6.1	NA	-	<p>Section 6.1 of ESARR 4 specifies that <i>“The provisions of this requirement are to become effective within three years from the date of adoption by the EUROCONTROL Commission”</i>.</p> <p><b>INITIAL CONCLUSION:</b></p> <p>This statement is not part of this assessment.</p>
SECTION 6- EXEMPTIONS			
7	YES  (-)	CDSA  Chapter 5 (para 2 and 6)  Chapter 8	<p>Section 7 of ESARR 4 specifies that there are no exemptions (<a href="#">see issue 1</a>).</p> <p>(=) CDSA chapter 5 paragraph 2 specifies that <i>“A safety assessment is always required within the DFS if changes are made to the existing Air Traffic Management System, for which the DFS is responsible.”</i> In addition in paragraph 6 the following statement is mentioned <i>“The only modifications requiring safety assessment are procedures not included and for which no provision is made in the list of aforementioned documents”</i>. This statement requires further explanation.</p> <p>(=) CDSA specifies the classification of changes in chapter 8. According to this classification, changes that take place are regularly need <i>“a complete and systematic safety assessment once by way of an example in accordance with the procedure set out in the Safety Assessment Handbook”</i>.</p> <p style="text-align: right;">cont ...</p>



ESARR 4	Covered by DAM	Coverage	Related comments
SECTION 6- EXEMPTIONS			
7	YES  (-)	CDSA Chapter 5 (para 2 and 6)  Chapter 8	<p>(-) Annex F of CDSA provides exemptions for the implementation of the complete and systematic safety assessments. The safety assessment can only be tailored on the basis of agreed safety arguments.</p> <p><b>INITIAL CONCLUSION:</b> (See issue 1)</p> <p>The DAM classifies changes into three classes according to which changes of “Class III” do not need a complete and systematic safety assessment each time they change is implemented but only once by way of an example. However, they require certain processes to be followed (e.g. checklist to be filled in). Considering that ESARR 4 does not provide additional specification on the classification of a change that is subject to a quantitative risk-based approach this requirement is considered to be met as CDSA describes on a global level the measures to be taken to assure that these changes do not introduce unacceptable risks at a global level.</p> <p>It should be taken into consideration that the procedures for changes of class II and class III were not evaluated as part of this assessment, as no material was provided.</p> <p>Annex F provides exemptions for the implementation of the complete and systematic safety assessments. There is no relationship with the classification provided in chapter 8.</p>

*Table 1 Coverage Analysis – Mandatory Provisions (Chapters 6 and 7)*

*(Space Left Intentionally Blank)*

#### 4.4 ESARR 4 Advisory Sections: Executive Summary, 1, 2, 4 and 8

##### Analysis

Table 3 Coverage Analysis – Advisory Provisions provides coverage analysis of the contents of the following two documents, for those advisory sections/material included in ESARR 4:

- CDSA
- SAH

The following abbreviation is used when both documents are addressed: **DAM** (DFS Assessment Methodology)

##### Legend

- When the provisions of CDSA and SAH are seen as equivalent or equal to the relevant requirement of ESARR 4, the sign “=” is used.
- When the provisions of CDSA and SAH are seen as encompassing a minimum and exceeding the relevant requirement of ESARR 4, the sign “+” is used.
- When the provisions of CDSA and SAH are seen as less demanding than the relevant requirement of ESARR 4, the sign “-” is used.
- When the provisions of CDSA and SAH differ or are inconsistent with the relevant requirement of ESARR 4, the sign “#” is used.

*Note: The following initial conclusions are derived from Table 3 Coverage Analysis – Advisory Provisions*

##### Summary of Initial Conclusions

- The relationship of the three phases (FHA, PSSA and SSA) with the phases described in Figure 3 are a bit confusing.
- The term “safety analysis” is used in different meanings. In page 10 the sentence above the figure and in the figure (Figure 3).
- It is assumed that “System Analysis” is referred to as “SSA”. If so, the description in chapter 9 covers only part of the SSA activities.
- More emphasis is put on the earlier phases of the life cycle (e.g. activities during system definition and design than on activities during transition). There is more detailed information concerning the required activities for the safety assessment in the DFS PMH specified. Nevertheless this document was not in the scope of this assessment.

ESARR 4	Covered by DAM	Coverage	Related comments
SECTION 1-SCOPE			
1.1	YES (=)	CDSA Chapter 5 (para 2 and 6) Chapter 7 Chapter 8 Annex F  SAH Chapter 5 and 6	<p>Section 1.1 of ESARR 4 specifies that <i>“This requirement concerns the use of a quantitative risk based-approach in Air Traffic Management when introducing and/or planning changes to the ATM System.”</i></p> <p>(=) CDSA chapter 5 paragraph 2 specifies that <i>“A safety assessment is always required within the DFS if changes are made to the existing Air Traffic Management System, for which the DFS is responsible.”</i> In addition, in paragraph 6 the following statement is mentioned <i>“The only modifications requiring safety assessment are procedures not included and for which no provision is made in the list of aforementioned documents”</i>. This statement requires further explanation.</p> <p>(=) CDSA specifies in chapter 7 that the safety assessments need to be conducted in accordance with the SAH. SAH provides guidance for the usage of and approach combining qualitative and quantitative elements. (see also requirement 5.2 (Note 2)):</p> <p>(=) CDSA specifies in chapter 8 the classification of changes. According to this classification changes, that regularly take place regularly need <i>“a complete and systematic safety assessment once by way of an example in accordance with the procedure set out in the Safety Assessment Handbook.”</i></p> <p>(=) CDSA provides only general information on the procedures to be implemented in case of a change of class II or class III. The objectives or the content of the checklist referred to in chapter 8.3 is not defined in the <b>DAM</b>.</p> <p>(-) Annex F of CDSA provides exemptions for the implementation of the complete and systematic safety assessments. The safety assessment can only be tailored on the basis of agreed safety arguments (issue 1).</p> <p style="text-align: right;">cont ...</p>

ESARR 4	Covered by DAM	Coverage	Related comments
SECTION 1-SCOPE			
1.1	YES (=)	CDSA Chapter 5 (para 2 and 6) Chapter 7 Chapter 8 Annex F  SAH Chapter 5 and 6	<p><b>INITIAL CONCLUSION:</b></p> <p>The DAM classifies changes into three classes according to which changes of “Class III” do not need a complete and systematic safety assessment each time the change is implemented but only once by way of an example. However, they require certain processes to be followed (e.g. checklist to be filled in).</p> <p>Considering that ESARR 4 does not provide additional specification on the classification of a change that is subject to a quantitative risk-based approach this requirement is considered to be met, as CDSA describes the measures to be taken to assure that these changes do not introduce unacceptable risks on a global level.</p> <p>It should be taken into consideration that the procedures for changes of class II and class III were not evaluated as part of this assessment as no material was provided.</p> <p>Annex F provides exemptions for the implementation of the complete and systematic safety assessments. There is not relationship with the classification provided in chapter 8.</p>
1.2	YES (=)	SAH Chapter 3 (para 2 and Figure 2) Chapter 3 (para 5, 6) Chapter A.3 (page 74)	<p>Section 1.2 of ESARR 4 specifies that “<i>This requirement covers the human, procedural and equipment (hardware, software) elements of the ATM System as well as its environment of operations.</i>”</p> <p>(=) Chapter 3 paragraph 2 of SAH gives the three elements that need to be considered. On the next page (paragraph 5 and 6) the environment is also considered.</p> <p>(=) In the sentence “<i>Each of the systems operated by DFS (engineering, organisation, procedures) could lead to safety risks for the environment or the company itself</i>” different descriptions for the elements are used.</p> <p><b>INITIAL CONCLUSION:</b></p> <p>SAH uses the term “object” for what is called “equipment” in ESARR 4.</p> <p>The list provided in paragraph 2 does not mention “environment”. As this information is provided in a subsequent paragraph this requirement is considered to be met.</p>

ESARR 4	Covered by DAM	Coverage	Related comments
SECTION 1-SCOPE			
1.3	YES (-)	CDSA Annex F  SAH Chapter 3 (para 6) Chapter 4  DAR	<p>Section 1.3 of ESARR 4 specifies that “<i>This requirement covers the complete life-cycle of the ATM System, and, in particular, of its constituent parts.</i>”</p> <p>(=) In chapter 3 of SAH it is specified that “<i>the systematic assessment of safety must be conducted over the entire life cycle of a system.</i>”</p> <p>(=) Chapter 4 provides a list of the DFS phases of the life cycle of a system and a high level mapping with the phases and activities of the safety.</p> <p>(-) Annex F of CDSA specifies that “<i>safety assessment generally begins very early on in the planning and development cycle of a new process, new technical system or modification of existing processes and systems</i>”. Nevertheless, for certain exemptions not all phases of the life cycle have to be covered (issue 1).</p> <p><b>INITIAL CONCLUSION:</b></p> <p>The process and the activities required for safety assessment are only mapped on a very high level. More emphasis is put on the earlier phases of the life cycle (e.g. activities during system definition and design than on activities during transition).</p> <p>The exemption described in Annex F is in contradiction to the statement of this requirement.</p>
1.4	YES (+)	SAH Chapter 1 Chapter 3	<p>Section 1.4 of ESARR 4 specifies that “<i>This requirement does not address the assessment of introducing and/or planning organisational or management changes to the ATM service provision.</i>”</p> <p>(+) SAH includes “organisation” in addition to the procedure in the list of the elements in chapter 3 and 5.</p> <p><b>INITIAL CONCLUSION:</b></p> <p>As the requirement of ESARR 4 explicitly specifies that organisational or management changes are not considered, the scope of PMC is considered wider than ESARR 4 explicitly requires.</p>

ESARR 4	Covered by DAM	Coverage	Related comments
SECTION 2-RATIONALE			
2.1	NA	-	<p>Section 2.1 of ESARR 4 specifies that “<i>The increasing integration, automation and complexity of the ATM System requires a systematic and structured approach to risk assessment and mitigation, including hazard identification, as well as the use of predictive and monitoring techniques to assist in these processes.</i>”</p> <p><b>INITIAL CONCLUSION:</b></p> <p>This section does not specify a requirement but a rationale. Therefore this statement is not part of this assessment.</p>
2.2	NA	-	<p>Section 2.2 of ESARR 4 specifies that “<i>Errors in the design, operation or maintenance of the ATM System or failures in the ATM System could, through a decrease in safety margins, result in, or contribute to, a hazard to aircraft. Increasingly, more reliance and therefore a greater safety burden, is being placed upon all parts of the ATM System. In addition, the increased interaction of ATM across State boundaries requires that a consistent and more structured approach be taken to the risk assessment and mitigation of all ATM System elements throughout the ECAC States.</i>”</p> <p><b>INITIAL CONCLUSION:</b></p> <p>This section does not specify a requirement but a rationale. Therefore this statement is not part of this assessment.</p>
2.3	NA	-	<p>Section 2.3 of ESARR 4 specifies that “<i>In addition, and in certain cases, the implementation of ESARR 3 (Use of Safety Management Systems by ATM Service Providers) also necessitates the provision of more specific requirements to be used. ESARR 4 provides such detailed requirements, hence developing further sections 5.2.4 and 5.3.4 of ESARR 3.</i>”</p> <p><b>INITIAL CONCLUSION:</b></p> <p>This section does not specify a requirement but a rationale. Therefore this statement is not part of this assessment.</p>

ESARR 4	Covered by DAM	Coverage	Related comments
SECTION 2-RATIONALE			
2.4	NA	-	<p>Section 2.4 of ESARR 4 specifies that “Accordingly, a harmonised approach to the identification, assessment and management of risk is a necessary step in ensuring high levels of ATM safety across the ECAC area.”</p> <p><b>INITIAL CONCLUSION:</b></p> <p>This section does not specify a requirement but a rationale. Therefore this statement is not part of this assessment.</p>
SECTION 4-SAFETY OBJECTIVE			
4.1	YES (=)	SAH	<p>Section 4.1 of ESARR 4 specifies that “Within the overall objective of ensuring safety, the objective of this requirement is to ensure that the risks associated with hazards in the ATM System are systematically and formally identified, assessed, and managed within safety levels, which as a minimum, meet those approved by the designated authority.”</p> <p>(=) SAH provides guidance on how to assess and manage hazards within the safety levels.</p> <p>(=) SAH provides some guidance on the identification of hazards.</p> <p>(=) with regard to the risk classification scheme DFS claims that the figures have been approved by the Ministry of Transport.</p> <p><b>INITIAL CONCLUSION:</b></p> <p>The requirement is only partly fulfilled as:</p> <ul style="list-style-type: none"> <li>- the guidance provided for the identification of hazards is not very detailed and</li> <li>- it is not clear whether the figures provided in SAH (Table 1, 2 and 3) with regard to the risk classification scheme have been approved by the designated authority.</li> </ul>

ESARR 4	Covered by DAM	Coverage	Related comments
SECTION 8-ADDITIONAL MATERIAL			
8.1.1	Yes (=)	6.3.5	<p>Section 8.1.1 of ESARR 4 specifies that <i>“For existing parts of the ATM System, an analysis based on available historical data, such as safety occurrence (i.e. accident, incident, ATM specific occurrence) statistics, human errors, equipment faults, mostly based on system safety monitoring and occurrence reporting schemes may contribute evidence to the safety assurance process, hence complementing the safety analysis depicted in section 5 of this requirement.”</i></p> <p><b>INITIAL CONCLUSION:</b></p> <p>SAH 2.02 refers to experience in several places without providing exact information on how this information was gathered for instance in 6.3.5: Safety monitoring and improvement and revision of the safety assessment.</p>
8.2.1	NA	-	<p>Section 8.2.1 of ESARR 4 specifies that <i>“EATMP SAM SAF ET1.ST03.1000-MAN- (Ed 1.0) is considered as a useful guidance when implementing this safety regulatory requirement. The applicability of the methodology would need to be specified at the beginning of any risk assessment and mitigation process.”</i></p> <p>and</p> <p><i>“(Note: Future revisions of that document are also to be foreseen, to encompass assessment of the human, equipment and procedures elements and develop further the system safety assessment process beyond the Functional Hazard Assessment).”</i></p> <p><b>INITIAL CONCLUSION:</b></p> <p>Even the DAM refers to EATMP SAM on page A7 this statement is not related to the evaluation of the DAM.</p>
8.2.2.1	NA	-	<p>Section 8.2.2.1 of ESARR 4 specifies that <i>“The safety objectives allocated to each hazard drive the determination of specific means to attain the proper level of confidence in the success of implementing the mitigation strategies and related safety requirements.”</i></p> <p><b>INITIAL CONCLUSION:</b></p> <p>This statement formulated more as a rationale than a requirement. Therefore this statement is not part of this assessment.</p>



ESARR 4	Covered by DAM	Coverage	Related comments
SECTION 8-ADDITIONAL MATERIAL			
8.2.2.2	Yes (=)	5.7	<p>Section 8.2.2.2 of ESARR 4 specifies that “<i>These means may include a set of different levels of constraints being set on specific software elements of the ATM System.</i>”</p> <p><b>INITIAL CONCLUSION:</b></p> <p>The rationale for the establishment for safety criticality in SAH 2.02 page 34 to 36 takes into account the constraints on specific software elements of the ATM System.</p>
8.2.3.1	YES (=)	SAH Chapter 4.6	<p>Section 8.2.3.1 of ESARR 4 specifies that “<i>Safety monitoring and data collection mechanisms could be specifically developed as an enabling tool to the validation of the safety assumptions and requirements as identified during the risk assessment and mitigation processes, including hazard identification, as well as the assessment of the safety added value of the programme. For example, such mechanisms could be used for the validation of theoretical data such as Mean Time Between Failures) and models (such as fault tree, reliability flow charts) used in the safety assessment and safety assurance processes.</i>”</p> <p>(=) In chapter 4.6 SAH specifies that the continuous activities have to take place to monitor the validity of the safety analysis. In this chapter, a reference to the “safety monitoring and improvement” sub-process is also mentioned.</p> <p><b>INITIAL CONCLUSION:</b></p> <p>SAH specifies that safety monitoring must take place. Nevertheless no guidance is provided in <b>DAM</b> on how these activities should be done. Complimentary information could help obtain better data in monitoring.</p>
8.2.3.2	NA	-	<p>Section 8.2.3.2 of ESARR 4 specifies that “<i>In addition, safety monitoring and data collection mechanisms consistent with the provisions of ESARR 2(11), could also be developed as enabling tools to define global safety indicators in order to control and monitor the safety levels reached in operation by the ATM System.</i>”</p> <p><b>INITIAL CONCLUSION:</b></p> <p>As ESARR 2 is out of scope of this assessment this requirement has not been assessed.</p>

ESARR 4	Covered by DAM	Coverage	Related comments
SECTION 8-ADDITIONAL MATERIAL			
8.2.3.3	YES (=)	SAH 2.02 Chapter 4 6.3.5  DAR	<p>Section 8.2.3.2 of ESARR 4 specifies that "Safety monitoring should therefore be seen as a complementary means of qualification before and during operational use."</p> <p>(=) safety monitoring is described in 6.3.5: "The process of regular (i.e. continuing or cyclical) monitoring of the safety of a system is called "safety monitoring and improvement."</p> <p>At DFS, the "safety controlling" sub-process carries out this function. Apart from identifying deviations, this function also initiates measures which restore a safe status (safety improvement)."</p> <p>(=) DAR states the evidence that has to be provided for the operational and technical acceptance (example see 6).</p> <p><b>INITIAL CONCLUSION:</b></p> <p>SAH specifies that safety monitoring must take place, but it is unclear whether these activities are to start before or after transition. No guidance is provided on how these activities should be done.</p> <p>DAR lists required document for the acceptance of a system but it only refers to activities before the transition and it does not specify if safety monitoring is required to produce the required evidence.</p>
8.3			See Terms and Definitions

Table 2 Coverage Analysis – Advisory Provisions

<sup>6</sup> Nachweis, dass eine Sicherheitsbewertung durchgeführt wurde und ein Sicherheitskonzept vorliegt.  
 Nachweis, dass alle identifizierten Sicherheitsrisiken durch geeignete Maßnahmen auf ein akzeptables Niveau (gemäß Risikotabelle der DFS) reduziert wurden.

## 5. STATEMENT OF COMPLIANCE

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

- ESARR 4 Section 3.1)
- ESARR 4 Section 3.2)
- ESARR 4 Section 5.1.a) (within the limitation of the interpretation of “any changes”)
- ESARR 4 Section 5.1.b) (within the limitation of the interpretation of “any changes”)
- ESARR 4 Section 5.1.c) (within the limitation of the interpretation of “any changes”)
- ESARR 4 Section 5.2 a)
- ESARR 4 Section 5.2.b.i)
- ESARR 4 Section 5.2.b.ii) (observation 1 : use of Bayesian network)
- ESARR 4 Section 5.2.b.iii) (observation 1 : use of Bayesian network)
- ESARR 4 Section 5.2.c.i)
- ESARR 4 Section 5.2.c.ii)
- ESARR 4 Section 5.2.c.iii)
- ESARR 4 Section 5.2.d)
- ESARR 4 Section 5.2 Note 1
- ESARR 4 Section 5.2 Note 2 (observation 1 : use of Bayesian network)
- ESARR 4 Section 5.3.a)
- ESARR 4 Section 5.3.b)
- ESARR 4 Appendix A-1 (1)
- ESARR 4 Appendix A-1 (2) (observation 1 : use of Bayesian network)
- ESARR 4 Appendix A-1 (3) (observation 2 : need for guidance to assess the severity of effects)
- ESARR 4 Appendix A-2 (1)
- ESARR 4 Appendix A-2 (2)

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

- ESARR 4 Section 5.1

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

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

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

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

*(Space Left Intentionally Blank)*

## APPENDIX A – TERMS AND DEFINITIONS

Term	ESARR 4 Definition	DAM Definition	Comment
<b>A</b>			
<b>Accident</b>	<p>An occurrence associated with the operation of an aircraft which takes place between the time any person boards the aircraft with the intention of flight until such time as all such persons have disembarked, in which:</p> <p>a) a person is fatally or seriously injured as a result of:</p> <ul style="list-style-type: none"> <li>- being in the aircraft, or</li> <li>- direct contact with any part of the aircraft, including parts which have become detached from the aircraft, or</li> <li>- direct exposure to jet blast,</li> </ul> <p>except when the injuries are from natural causes, self-inflicted or inflicted by other persons, or when the injuries are to stowaways hiding outside the areas normally available to the passengers and crew; or</p> <p>b) the aircraft sustains damage or structural failure which:</p> <ul style="list-style-type: none"> <li>- adversely affects the structural strength, performance or flight characteristics of the aircraft, and</li> <li>- would normally require major repair or replacement of the affected component</li> </ul> <p>except for engine failure or damage, when the damage is limited to the engine, its cowlings or accessories; or for damages limited to propellers, wing tips, antennas, tires, brakes, fairings, small dents or puncture holes in the aircraft skin; or</p> <p>c) the aircraft is missing or is completely inaccessible.</p>	No definition provided	There are no contradictions except that non-aviation examples are used.

Term	ESARR 4 Definition	DAM Definition	Comment
<b>Assessment</b>	An evaluation based on engineering, operational judgement and/or analysis methods.	No definition provided	No contradiction identified
<b>ATM Service Provider</b>	An organisation responsible and authorised to provide ATM service(s).	No definition provided	Not used (except when mentioning text from another source)
<b>ATM Service</b>	A service for the purpose of ATM.	No definition provided	Not used (except when mentioning text from another source)
<b>ATM System</b>	ATM System is a part of ANS System composed of a Ground Based ATM component and an airborne ATM component.	No definition provided	Footnote 18 in SAH does not include humans.
<b>ATM</b>	The aggregation of ground-based (comprising variously ATS, ASM and ATFM) and airborne functions required to ensure the safe and efficient movement of aircraft during all appropriate phases of operations.	No definition provided	No contradiction identified
<b>Assumption</b>	Statement, principle and/or premises offered without proof.	No definition provided	No contradiction identified
<b>C</b>			
<b>Cause</b>		Situation or event resulting in a hazard in terms of a causal connection.	Not defined in ESARR 4
<b>CNS/ATM</b>	The aggregation of functions used in provision of CNS services and used by ATM.	No definition provided	No contradiction identified
<b>CNS system</b>	All the hardware and software that make up a function, tool or application that is used to provide one or more air traffic management services. The CNS system is an enabler to the provision of ATM services.	No definition provided	No contradiction identified

Term	ESARR 4 Definition	DAM Definition	Comment
<b>Commercial Air Transport</b>	The operation of an aircraft in one or more stages on a scheduled or non-scheduled basis, which is available to the public for remuneration or hire (technical stops are counted in ICAO's statistics).	No definition provided	Not used (except when mentioning text from another source or referring to other related documentation)
<b>Criticality</b>		(also called Safety Criticality) Indication of the influence of a system or a system component on safety, determined on the basis of the severity and the conditional probability of the effects resulting from hazards.	Not defined in ESARR 4
<b>D</b>			
<b>Designated authority</b>	The competent body designated by State authority, responsible for aviation safety regulation.	No definition provided	Not used (except when mentioning text from another source)
<b>Direct (ATM system contribution to accident / Incident)</b>	Where at least one ATM event or item was judged to be DIRECTLY in the causal chain of events leading to an accident or incident. Without that ATM event it is assumed that the occurrence would not have happened.	No definition provided	Not used
<b>E</b>			
<b>Effect</b>		Situation or event resulting from a hazard in terms of a causal connection. Safety assessments only consider "negative effects", i.e. impairments to the life or health of persons or to the material or functional qualities of objects.	Not defined in ESARR 4

Term	ESARR 4 Definition	DAM Definition	Comment
<b>Environment of operations</b>	The environment of operations consists of the physical and institutional characteristics of the airspace within which operations occur. The environment includes ATM services being provided, technologies used, airspace organisation, ambient conditions and people.	No definition provided	Not used (except when mentioning text from another source)
<b>Error</b>	A mistake in specification, design, or implementation or an occurrence arising as a result of incorrect action or decision by personnel operating or maintaining the system (flight crew, Air Traffic Controller, service provider or maintenance personnel).	No definition provided	No contradiction identified
<b>F</b>			
<b>Failure</b>	The inability of any element of the Air Traffic Management System to perform its intended function or to perform it correctly within specified limits.	No definition provided	Not used
<b>Failure Condition</b>	A condition having an effect on the aircraft and/or its occupants, either directly or indirectly through loss of separation, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational (density of air traffic, TMA etc...) or environmental conditions.	No definition provided	Not used



Term	ESARR 4 Definition	DAM Definition	Comment
<b>Frequency</b>		<p>If in <math>n</math> independent repetitions of a situation <math>S</math>, a specific event <math>E</math> occurs precisely <math>h_n(E)</math> times, then <math>h_n(E)</math> is called the (absolute) <b>frequency</b> of event <math>E</math>.</p> <p>The quotient <math>H_n(E) = h_n(E)/n</math> is called the <b>relative frequency</b> of event <math>E</math>.</p>	Not defined in ESARR 4
<b>Functional hazard analysis (FHA)</b>		First phase of a safety assessment. Assessment of hazards on a functional level, definition of safety objectives and safety criticality.	Not defined in ESARR 4
<b>G</b>			
<b>General Aviation Operation</b>	An aircraft operation other than a commercial air transport operation or aerial work operation.	No definition provided	Not used
<b>H</b>			
<b>Hazard</b>	Any condition, event or circumstance which could induce an accident.	Situation or event which could potentially have a negative effect.	There is a difference as the <b>DAM</b> has a wider scope. It also addresses negative effects for the company.
<b>I</b>			
<b>Inadequate separation</b>	In the absence of prescribed separation minima, a situation in which aircrafts were perceived to pass too close to each other for pilots to ensure safe separation.	No definition provided	Not used

Term	ESARR 4 Definition	DAM Definition	Comment
<b>Incident</b>	An occurrence other than an accident, associated with the operation of an aircraft, which affects or could affect the safety of operation.	No definition provided	In SAH not 8 states: "Incidents" in this case are taken to mean, inter alia, aircraft proximities or infringement of separation minima"  The definition ESARR 4 has a wider scope.
<b>L</b>			
<b>Target Level of Safety (or safety level or safety minima)</b>	A level of how far safety is to be pursued in a given context, assessed with reference to an acceptable or tolerable risk.	No definition provided	Not used
<b>Loss of safety margins</b>	All situations where an aircraft is too close to something else (e.g. another aircraft, ground, obstacle, restricted area, meteorological anomalies) and the ability to recover from the hazardous situation is jeopardised.	No definition provided	Not used
<b>M</b>			
<b>Methodology specialist</b>		An expert in the application of a specific systematic method. In this case: an expert in the methodical execution of safety assessments.	Not defined in ESARR 4
<b>Mitigation (or risk mitigation)</b>	Steps taken to control or prevent a hazard from causing harm and reduce risk to a tolerable or acceptable level.	No definition provided	No contradiction identified
<b>O</b>			
<b>Operational expert</b>		A person with many years of experience in the use of a system, e.g. an air traffic controller or a flight data manager.	Not defined in ESARR 4

Term	ESARR 4 Definition	DAM Definition	Comment
<b>P</b>			
<b>Probability</b>		<p>The probability that an event <math>A</math> or an event <math>B</math> occurs is a number <math>p(A)</math> or <math>p(B)</math> for which the following is true:</p> <ul style="list-style-type: none"> <li>• <math>0 \leq p(A) \leq 1</math> or <math>0 \leq p(B) \leq 1</math>.</li> <li>• If event <math>A</math> is certain to occur, then <math>p(A) = 1</math>.</li> <li>• If the occurrence of event <math>A</math> is impossible, then <math>p(A) = 0</math>.</li> </ul> <p>If events <math>A</math> and <math>B</math> are mutually exclusive, the probability that either event <math>A</math> or event <math>B</math> will occur can be determined as follows:  <math>p(A \cup B) = p(A) + p(B)</math></p>	Not defined in ESARR 4
<b>Procedures (Refer to Operational ATC procedures in ESARR 2)</b>	Written procedures and instructions used by ATC personnel in the pursuit of their duties directly in connection with the provision of the ATM services.	No definition provided	The term is used in both senses "Operation Procedures" and "Safety or Project Management" procedures.

Term	ESARR 4 Definition	DAM Definition	Comment
<b>R</b>			
<b>Risk</b>	The combination of the overall probability or frequency of occurrence of a harmful effect induced by a hazard and the severity of that effect.	An indication of the impact presented by a hazard. A risk arises from a hazard in connection with one of its possible effects. It is assessed in terms of the severity and the relative frequency of these effects.	Different Definition, the word “impact” is not a “a combination of the overall probability or frequency of occurrence of a harmful effect”.
<b>Risk class</b>		A set of risks – defined by their severity and frequency – which are regarded as being equivalent.	Not defined in ESARR 4
<b>Risk Assessment</b>	Assessment to establish that the achieved or perceived risk is acceptable or tolerable.	No definition provided	No contradiction identified
<b>Risk Mitigation</b>	See “Mitigation”.	No definition provided	
<b>Risk matrix</b>		The risk matrix indicates the risk class to which a risk – defined by its severity and frequency – is assigned.	Not defined in ESARR 4
<b>S</b>			
<b>Safety</b>	Freedom from unacceptable risk of harm.	The expectation that a system – under defined conditions – will not enter into a state which could endanger human life or health, the environment or equipment. A system is called safe when all risks which could result from the hazards have been reduced to an acceptable degree by suitable measures.	The definition in <b>DAM</b> is different than the definition in ESARR 4.

Term	ESARR 4 Definition	DAM Definition	Comment
<b>Safety analysis</b>		Third phase of the safety assessment. Proof of the achieved safety level by consistent analysis and assessment of the remaining risks. Description of safety measures aimed at reducing risks.	Not defined in ESARR 4
<b>Safety assessment</b>		All steps that are necessary to establish and provide proof of the required safety level of a system. A safety assessment comprises the functional hazard analysis, the definition of safety requirements and the safety analysis, including the preparation of safety measures.	Not defined in ESARR 4
<b>Safety Assurance</b>	All planned and systematic actions necessary to provide adequate confidence that a product, a service, an organisation or a system achieves acceptable or tolerable safety.	No definition provided	No contradiction identified
<b>Safety measure</b>		<p>Safety measures are elements, processes or special working procedures for the reduction of risks. These measures are classified on the basis of their intention. Measures exist for</p> <ul style="list-style-type: none"> <li>- prevention, i.e. for attempting to prevent the occurrence of hazards and effects;</li> <li>- tolerance, i.e. to permit the services of the system to be offered even if hazards or effects occur;</li> <li>- reduction, i.e. to reduce the frequency of hazards or the severity of the resulting effects.</li> </ul>	Not defined in ESARR 4

Term	ESARR 4 Definition	DAM Definition	Comment
<b>Safety Minima</b>	Refer "to target level of safety".	No definition provided	No contradiction identified
<b>Safety objective</b>	A safety objective is a qualitative or quantitative statement that defines the maximum frequency or probability at which a hazard can be expected to occur.	Determination of the maximum frequency at which an identified hazard may be expected to occur.	The definition in ESARR 4 is wider.
<b>Safety level</b>	Refer to 'target level of safety'.	No definition provided	
<b>Safety requirement</b>	A risk mitigation means, defined from the risk mitigation strategy, that achieves a particular safety objective. Safety requirements may take various forms, including organisational, operational, procedural, functional, performance, and interoperability requirements or environment characteristics.	No definition provided	No contradiction identified
<b>Separation minima infringement</b>	A situation in which prescribed separation minima were not maintained between aircrafts.	No definition provided	Not used
<b>Safety Monitoring</b>	A systematic action conducted to detect changes affecting the ATM System with the specific objective of identifying that acceptable or tolerable safety can be met.	No definition provided	In chapter 4.6 SAH the following statement is provided: "The process of regular (i.e. continuing or cyclical) monitoring of the safety of a system is called "safety monitoring and improvement"."  As the ESARR 4 addresses the monitoring with regard to changes to the system.
<b>Severity</b>	Level of effect/consequences of hazards on the safety of flight operations (i.e. combining level of loss of separation and degree of ability to recover from the hazardous situation).	Classification of the "negative impact" of an effect. The "classification scheme for the effects of hazards" distinguishes between 5 levels of severity.	No contradiction identified
<b>Severity Class</b>	Gradation, ranging from 1 (most severe) to 5 (least severe), as an expression of the magnitude of the effects of hazards on flight operations.	No definition provided	Not used

<b>Term</b>	<b>ESARR 4 Definition</b>	<b>DAM Definition</b>	<b>Comment</b>
<b>Supporting services</b>	Systems, services and arrangements, including Communication, navigation and Surveillance services, which support the provision of an ATM service.	No definition provided	Not used (except when mentioning text from another source)
<b>System</b>	A combination of physical components, procedures and human resources organised to perform a function.	All technical and/or organisational and/or other top-level functions, processes and elements necessary for the independent execution of a set of tasks. [PMH] A system comprises persons, procedures and technology.	Footnote 18 in SAH does not include humans.
<b>T</b>			
<b>Target Level of Safety (or 'safety level' or 'safety minima')</b>	A level of how far safety is to be pursued in a given context, assessed with reference to an acceptable or tolerable risk.	No definition provided	Not used
<b>V</b>			
<b>Validation</b>	Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled (usually used for internal validation of the design).	No definition provided	Not used
<b>Verification</b>	Confirmation by examination of evidence that a product, process or service fulfils specified requirements.	No definition provided	Not used (except when mentioning text from another source)

*Table 3 Mapping Terms and Definition*

## APPENDIX B – REVIEW OF THE CONCLUSIONS AND RECOMMENDATIONS OF THE FIRST ASSESSEMENT

This section summarises those issues that could jeopardise the acceptability of the 'DFS Safety Assessment Methodology' version 1.02 i.e. its use as a means of showing compliance with ESARR 4 and which has been improved by DFS in version 2.02.

This section also includes a number of suggestions, to DFS, derived from this assessment, in order to facilitate the potential development of a future release of 'DFS Safety Assessment Methodology' that is more fully compliant with ESARR 4.

This section includes the result of the assessment of the last release of DFS

### B.1 Issue 1 – Mitigation Topics

**ISSUE 1 – The PMC** does not cover mitigation adequately.

- Hazard identification and risk assessment are dealt with in depth and are well covered, however, mitigation (which includes showing that the requirements are satisfied) is dealt with at less depth (Requirement 5.1).

#### Suggested Solution

DFS stated that the topic of mitigation is dealt with more clearly in version 2 of the SAH. They have also restructured the document so that a more appropriate balance is evident.

#### DFS Improvement

- SAH Version 2.02 provides corrections to this issue.
- Chapter 3, Page 9, the scope of ATM has been redefined accordingly, including a clarification of the process and external services.
- Chapter 6.3, Page 63 of the SAH
- Annex 2, Page 78 in the SAH

### B.2 Issue 2 – Transitions Inadequately Covered

**ISSUE 2 – The PMC** does not adequately address transitions in the lifecycle.

- The transition phases of the life cycle are inadequately covered (Requirement 5.1.a).
- The DFS safety objectives and safety requirements are verified and completely documented at the end of the project by application of the safety analysis process. However, this activity is not described adequately in the SAH (Requirement 5.2.d).



### Suggested Solution

Transitions are not well described, largely due to historic reasons. However it is considered good practice in DFS to provide a separate safety case for transitions of any significance. The way DFS have previously described the process has not specifically included any transition phases and to add one now might cause confusion and would introduce inconsistent models. However DFS will emphasis that this is required in the text of the SAH.

Since transitions are not well described it is clear that the verification of transition requirements will similarly be inadequately described.

- DFS to include specific text in the SAH to describe how transitions and transition requirements are included in the current process.

### DFS Improvement

- SAH Version 2.02 provides corrections to this issue.
- Chapter 4, page 11.

## B.3 Issue 3 – Coverage of Interactions

### ISSUE 3 – The PMC:

- does not adequately cover constituent interactions.
- does not adequately cover supporting services/external parties.
- provides for weak control of RAM for outsourced components.
- does not describe the requirements to be established for external defences.
- There is inadequate coverage of components, services and parties outside the scope of the management of the ATS e.g. airborne components and technical agreements with third party service providers (Requirement 5.1.b and 5.2 Note 1).
- While the three types of element are well covered, interactions between elements are not overtly covered. In particular, the interactions between elements within the constituent part, which relate to hazards that arise during development due to design decisions made, are not clearly identified in the SAH (Requirement 5.1.c).
- There is a risk that defences will not be fully specified for components that are developed by an external supplier (Requirement 5.2.c.i).
- There is good coverage of safety requirements that bear on the constituent part however, those needed to define defences stemming from rest of the ATM system are less well covered (Requirement 5.2.c.ii).

## Suggested Solution

The common thread running through all the observations made above is that when performing a risk assessment, the risks associated with services supplied to the ANSP and used by him in providing an Air Traffic Service, must be taken into account. Typically such services include the provision of Telecommunications, electrical power supply and CNS services. Less obviously they also include the services of a third party organisation in supplying components to the specification of the ANSP and in maintaining the system.

This interpretation is supported by requirement 3.1, which specifically mentions “supporting services” and requirement 5.1.b, which talks about addressing airborne (including spatial) and ground components “through co-operation with responsible parties”.

The ATM system can be considered to consist of all components and services directly related to the delivery of an ATM service (Ref: Note in ESARR 4, A-1, pp13). It therefore includes those services, used primarily for ATM purposes and those services whilst not intended primarily for ATM are nonetheless needed in the provision of the air traffic service e.g. telecommunications and electrical power supply. The services not owned and managed by the ANSP are called “supporting services” and ESARR 4 reinforces this distinction with the phrase “within their managerial control” to demonstrate the separation of responsibilities of the ANSP from any third party supplier of services.

Clearly the ANSP cannot control the risks associated with the services, used in providing the air traffic service but which are owned by a third party. However the ANSP must know what these risks are and mitigate them within the system he uses to deliver the air traffic service. These requirements have been put into ESARR 4 to make it clear that whilst an ANSP is not responsible for the management of the supporting services he is responsible for their use.

Normally an ANSP would discharge this responsibility by forming third party agreements with the suppliers. However some third party suppliers are not open to such agreements because they may be governmental organisations. Moreover the behaviour of the support service may be regulated but outside of the control of an ANSP e.g. the radio fit in an aircraft, the navigational performance of the aircraft. The ANSP still needs to know the behaviour of such services in order to perform a valid risk assessment. ESARR 4 covers this with the stipulation in 5.1 b, that the risk of such services is addressed “through co-operation with responsible parties”. Thus ESARR 4 intends the ANSP to seek out the behavioural specifications for such services even though he cannot choose not to use them or has no control over them.

The difficulties faced in the practical development of systems, where components may be bought “off the shelf” or subcontractors used for their implementation and manufacture, are that behaviours may be introduced by the implementation i.e. the component does more than was specified for it. The risk assessment must seek out such additional behaviours and/or place management controls on suppliers such that they contribute to the risk assessment and mitigation process.

ESARR 4 stresses (in 5.1.c) that the behaviours resulting from the interactions of both the components of the constituent part and its interactions with the rest of the ATM system are to be considered within the risk assessment and mitigation process. Clearly these interactions cannot be known unless the behaviours of all of the supporting services and the components of the constituent part are known. Moreover it is not sufficient just to know the design intent for the components, their actual behaviour must be known.

Whilst DFS are aware of these issues and in practice work towards accommodating them, the SAH does not provide specific guidance on how to fully address them.

The DFS method does not describe how additional behaviours are identified and controlled. It does not even admit that they may exist i.e. it is a design centred approach. There is nothing wrong with this it is just incomplete.

DFS would surely not fail to notice that defences might be available in the ATM system outside the constituent part. However the use of such defences would demand that requirements were written for their properties. Little guidance is given on these issues in the SAH. Consequently it may be worth adding a paragraph or two explaining that defences may stem from other parts of the ATM system and thus requirements would have to be written for them as well.

A handbook, which was prepared for ESARR 3 conformance, contains missing material on the identification of supporting services/external parties and the control of suppliers. It has not been translated and was not part of the review. However DFS propose that it should be included in the review and will get a translation and deliver it to the PMC review meeting.

Interactions between all elements of the constituent part and interactions between the constituent part and the rest of the ATM system are assessed using the RAMSYS tool. DFS agreed that this was not covered in the SAH and undertook to include an explanation in a later version of the SAH. The tool was not assessed.

- DFS to update SAH to include guidance on the use of external defences.
- DFS to provide a copy of the handbook for review.
- DFS to include specific guidance on the use of RAMSYS to assess interaction between all elements of the constituent part and between the constituent part and the rest of the ATM system.

### **DFS Improvement**

- SAH Version 2.02 provides corrections to this issue.
- Chapter 3 page 9
- Annex 8 page 97 , reference to external service provision
- Chapter 6.1.1 page 42
- Chapter 6.3.1 page 65
- Chapter 6.2.3 page 61

## B.4 Issue 4 – Coverage of Combined Effects

**ISSUE 4 – The PMC** does not adequately cover the cumulative effects of hazards.

- While coverage of hazard identification is good as is the coverage of the effect of a single hazard on a single accident/incident, the coverage of cumulative effects is less good and tends to focus on the most severe accident/incident (Requirement 5.2.b.i).

### Suggested Solution

The issue particularly refers to the one to many relationships between accidents/incidents and hazards. DFS agreed that this is not well dealt with in the SAH but do it. They will bring an example to the meeting to illustrate how cumulative effects are handled.

- DFS to provide an example of the assessment of cumulative effects for review.

### DFS Improvement

- Version 2.02 provides corrections to this issue.
- Chapter 6.1.2 page 45.

## B.5 Issue 5 – Validation of Risk Mitigation Strategy

**ISSUE 5 – The PMC** does not describe how validation is to be performed.

- The SAH describes the intent to verify the successful implementation of the risk mitigation strategy but does not describe how it is validated before it is implemented (Requirement 5.2.c.iii).

### Suggested solution

In general DFS rely on the principle of independent views of the processes used and their results ("Plausibility" in CDSA 6.2.1) and of the expertise of the players to establish the validity of those processes. The criteria used are those that have developed over time and have been subjected to the scrutiny of argument within DFS. They have not been written down. Furthermore, DFS would not wish to make specific efforts to capture all the criteria but would accept that a more organic process of capturing them as their use develops was within their scope of activities.

As part of the development of defences, their effects are inserted into the RAMSYS model and thus there is control over their implementation. The model itself is reviewed and hence there is a notion of validation in that the model is judged to be either plausible or implausible.

A third document "Richtlinie für Abnahmen und Freigaben von FS-technischen- oder Technischen Einrichtungen (Freigabe-Richtlinie)" (in German) included in the review pack contains text about assessing the validity of the measures as part of the operational release procedures. DFS agreed it would be better to include this text in the SAH.

- DFS to include validation guidance for the risk mitigation strategy in the SAH.

#### **DFS Improvement**

- Version 2.02 provides corrections to this issue.
- Chapter 6.2.3 page 62.

### **B.6 Issue 6 – Argumentation**

**ISSUE 6 – The PMC** does not provide justification that complete and correct arguments will be made.

- The description of the tool used (RAMSYS) is insufficient and therefore does not provide adequate justification that correct and complete arguments for the safety of the system will be established. Moreover, it is unlikely that RAMSYS could provide all of the necessary arguments (Requirement 5.3.a).

#### **Suggested Solution**

DFS claims that RAMSYS does do all that are required. A description of the use of the tool that justifies this is not in the current document, neither is it in version 2 of the SAH. DFS are prepared to put such a description in the SAH at a later date. DFS state that the bayesian network is the argument and that verification is performed during the safety analysis process. The bayesian net does provide the framework of an argument in that it shows why the ATM system is safe given that the properties of the network hold. However the properties of the basic building blocks of the network: the hazards, the arrival rate of causes and the conditional probabilities linking causes to hazards and hazards to accidents and incidents, need to be verified and this relies on different kinds of arguments and evidence e.g. arguments and evidence that all hazards have been identified.

- DFS to include a description of the use of the RAMSYS tool in the SAH and to update the SAH to include justification that complete and correct arguments will be provided for any system.

#### **DFS Improvement**

- DFS provides an example (in German) of their documentation, however this documentation is an example of the use of Bayesian Network (see observation 1)

*(Space Left Intentionally Blank)*

## B.7 Issue 7 – Effects Analysis

**ISSUE 7 – The PMC** does not include the effects categories.

- The five categories of effects may well be considered in the DFS system; however, they are not specifically mentioned in the SAH (Requirement Appendix A-1 (3)).

### Suggested Solution

As DFS acknowledge the severity classification scheme is “somewhat generic” and the five effects categories are not mentioned. It is important that guidance is given on the range of accidents/incidents that can result from a hazard in such a way that ensures as complete an analysis as possible. DFS claim that they do in fact always consider the effects mentioned in Appendix A-1 (3) and there is general supporting text that shows they consider a wide range of effects. However the SAH contains neither the list in Appendix A-1 (3) nor does it expand upon the list or rephrase it. DFS have accepted that issue 2 of the SAH does not improve the situation but that more information would be included at a later date.

- DFS to update the SAH to include more information on the categories of effects to be included in the effects analysis.

### DFS Improvement

- SAH Version 2.02 provides corrections to this issue.
- Chapter 6.1.3 page 47
- Annex 2 page 78

However, it remains an observation because some guidance is missing to support the assessment of the severity of effect.

## B.8 Issue 8 – Validation of TLS

**ISSUE 8 – The PMC** provides a means of apportioning the TLS that may not be amenable to validation.

- The SAH provides a good clear exposition of the way a Safety Objective is derived. However, this is necessary but insufficient condition for satisfying the requirement because another necessary condition is that the risk budget allocated to a system change must be correctly derived from the TLS in ESARR 4. There is some doubt about the practicality of the DFS scheme for deriving the system level TLS. (Requirement Appendix A-2 (1)).

*(Space Left Intentionally Blank)*

## Suggested Solution

While the apportionment model is well defined and appears rational, it is acknowledged to be arbitrary (Appendix 4, Pg 3, 2nd paragraph) and therefore has not been validated. Acquiring the data to validate the model poses the greatest difficulty for DFS. While there is much design data available to show that the target risks are being set at level d, there can be little data that shows what the actual achieved accident rates are. This is because the least conservative target level of safety for a level d risk is one accident every 15,000 years. Clearly this is not measurable in any reasonable timescale. DFS need to describe how the model will be validated. This will probably require additional parts to the model, which can be verified, together with a constructive argument linking these parts to the overall system TLS. These parts and the argument will need to be described.

Whilst it can be argued that DFS has not fully meet the requirement in Appendix A-2, it should also be noted that a method of validly and practically apportioning a quantitative target level of safety has not yet been assessed as acceptable by the SRC and consequently to criticise DFS for a failure to meet them may be premature.

Other issues relating to apportionment in ESARR 4 are:

- The appendix makes it clear that the TLS is for the whole of ECAC airspace and for all ATM. It also notes that an apportionment process may need to be developed. However it sets no requirements for the apportionment process or the validity of the resultant apportioned TLS. This may be deliberate in terms of the process but ESARR 4 should make it clear that any resulting apportioned TLS should be valid.
- The TLS applies to the total ATM system in ECAC airspace. The ESARR 4 Risk Assessment and Mitigation process relates to changes to that system. For any single change only a small portion of the TLS is available to the system being changed. The requirements in ESARR 4 are not contradictory in this respect, however they do not mention it. This has been a source of some confusion during the creation of this report. It has also been raised in conversations on ESARR 4 with UK ANSPs. It might improve ESARR 4 if a note were added to identify this issue and to clearly state the intent of ESARR 4.

- DFS to describe the means of validating the apportionment model.
- RTF should resolve the ESARR 4 issues e.g. to establish whether more guidance is needed or whether ESARR 4 needs changing.

## Comment of SRU with Regard to Issue 8

- ESARR4 is dealing with risk classification scheme (RCS) for design of changes or new systems; the TLS is related to Annex 11. It is dealing with the service provision. The scope of those figures is different.
- DFS defined a risk classification scheme which has been calculated on the basis of the level 1 risk. The value of level 1 risk has been decided on a common agreement by the SRC. On going work is aiming to regulate and to validate at European level the definition and the use of a risk classification scheme.
- RTF has been replaced by coordination group. The presentation of the progress of the mandate of RCS will be presented to coordination group.
- It remains an observation with regard the use of Bayesian network.