



**ACCEPTABLE MEANS OF COMPLIANCE AND GUIDANCE MATERIAL  
TO COMMISSION REGULATION (EU) XXXX/XXX**

**(Assessment of changes to functional systems by service providers in ATM/ANS and  
the oversight of these changes by competent authorities)**

**DRAFT**

**FOR INFORMATION PURPOSES ONLY**



## Table of contents

<b>ACCEPTABLE MEANS OF COMPLIANCE AND GUIDANCE MATERIAL TO COMMISSION REGULATION (EU) No XXX/XXXX.....</b>	<b>10</b>
GM1 to Article 5 Service Providers and Article 6(2) Oversight capabilities.....	10
MANAGEMENT, ASSESSMENT, ASSURANCE AND OVERSIGHT OF CHANGES TO FUNCTIONAL SYSTEMS..	10
<b>APPENDIX I: GENERAL GUIDANCE MATERIAL RELATED TO CHANGES TO FUNCTIONAL SYSTEMS ..</b>	<b>16</b>
1.    DEFINITIONS.....	17
1.1.    SAFETY SUPPORT ASSURANCE AND SAFETY ASSURANCE.....	17
1.2.    SPECIFICATION OF THE CHANGED SERVICE .....	18
1.3.    ARCHITECTURE OF FUNCTIONAL SYSTEMS .....	18
1.4.    CONCEPT OF SAFETY RISK .....	19
2.    UNDERLYING MODELS OF CHANGE MANAGEMENT .....	20
2.1.    FUNCTIONAL SYSTEM.....	20
2.1.1.Functional system model .....	20
2.1.2.    Organisation model of service providers.....	24
2.2.    CHANGES TO FUNCTIONAL SYSTEMS.....	29
2.2.1.    Change to functional system and its assessment.....	29
2.3.    SERVICES, INFORMATION AND THE RESPONSIBILITY FOR SAFETY .....	57
2.4.    MULTI-ACTOR CHANGES .....	62
2.4.1    Multi-actor changes — General.....	62
2.4.2    Change affecting multiple service providers and aviation undertakings — Forms of dependencies .....	62
2.4.3    Changes affecting multiple service providers and aviation undertakings — Examples .....	65
2.4.4    Changes affecting multiple service providers — Multi-actor changes involving safety support assessment and assurance .....	66
2.4.5    Changes affecting multiple ATSPs — Example of overarching safety argument .....	68
3.    PROCESS VIEWS.....	71
3.1.    SERVICE PROVIDER CENTRIC VIEW.....	71
3.1.1.    Change to functional system and its assessment.....	71
3.2.    SERVICE PROVIDER — COMPETENT AUTHORITY INTERACTION VIEW .....	79
3.2.1.    Interactions between service providers and competent authorities during the change process .....	79



3.3.	MULTI-ACTOR VIEW .....	89
4.	SAFETY ASSESSMENT AND SAFETY SUPPORT ASSESSMENT .....	95
4.1.	MODEL OF AN ARGUMENT .....	95
4.2.	LIFECYCLE OF THE CHANGE FOR EQUIPMENT AND ASSURANCE.....	98
4.3.	DEGRADED MODES OF OPERATION .....	99
5.	RISK ANALYSIS AND EVALUATION .....	103
5.1.	RISK ANALYSIS IN TERMS OF SAFETY RISK.....	103
5.1.1.	Hazards and accidents .....	103
5.1.2.	Severity schemes .....	107
5.1.3.	Combining severity schemes .....	114
5.1.4.	Validating risk analyses.....	116
5.2.	RISK EVALUATION SCHEMES .....	120
5.2.1.	Risk evaluation schemes.....	120
6.	RISK-BASED SELECTION MODEL .....	121

**ACCEPTABLE MEANS OF COMPLIANCE AND GUIDANCE MATERIAL TO ANNEX I — DEFINITIONS OF TERMS USED IN ANNEXES II TO XIII ..... 130**

**ACCEPTABLE MEANS OF COMPLIANCE AND GUIDANCE MATERIAL TO ANNEX II — REQUIREMENTS FOR COMPETENT AUTHORITIES — SERVICES PROVISIONS AND ATM NETWORK FUNCTIONS (Part-ATM/ANS.AR) ..... 131**

SUBPART B — MANAGEMENT (ATM/ANS.AR.B) .....	131
AMC1 ATM/ANS.AR.B.015(a)(8) Record keeping .....	131
RECORD KEEPING FOR FUNCTIONAL SYSTEMS CHANGE MANAGEMENT PROCEDURES.....	131
SUBPART C — OVERSIGHT, CERTIFICATION, AND ENFORCEMENT (ATM/ANS.AR.C).....	131
AMC1 ATM/ANS.AR.C.010(a) Oversight .....	131
CHANGES TO THE FUNCTIONAL SYSTEM .....	131
GM1 ATM/ANS.AR.C.030 Approval of change management procedures for ATM/ANS functional systems	131
GENERAL.....	131
AMC1 ATM/ANS.AR.C.030(a) Approval of change management procedures for functional systems .....	132
MEANS AND METHOD OF SUBMITTING PROCEDURES.....	132
AMC1 ATM/ANS.AR.C.030(b) Approval of change management procedures for functional systems .....	132
APPROVAL OF PROCEDURES .....	132
AMC1 ATM/ANS.AR.C.035(a) Decision to review the notified change to the functional system .....	132



MEANS AND METHOD OF SUBMITTING NOTIFICATION OF CHANGES TO FUNCTIONAL SYSTEMS.....	132
GM1 ATM/ANS.AR.C.035(c) Decision to review the notified change.....	133
OTHER SELECTION CRITERIA .....	133
<b>ACCEPTABLE MEANS OF COMPLIANCE AND GUIDANCE MATERIAL to ANNEX III — COMMON REQUIREMENTS FOR SERVICE PROVIDERS (Part-ATM/ANS.OR) .....</b>	<b>135</b>
SUBPART A — GENERAL COMMON REQUIREMENTS (ATM/ANS.OR.A).....	135
AMC1 ATM/ANS.OR.A.045(a) Changes to the functional system.....	135
NOTIFICATION DATA .....	135
GM1 ATM/ANS.OR.A.045(a) Changes to the functional system.....	135
NOTIFICATION DATA .....	135
GM2 ATM/ANS.OR.A.045(a) Changes to the functional system.....	136
ROUTINE CHANGES .....	136
GM3 ATM/ANS.OR.A.045(a) Changes to the functional system.....	137
MEANS OF NOTIFICATION.....	137
GM4 ATM/ANS.OR.A.045(a) Management of change to a functional system .....	139
REGISTER OF NOTIFIED CHANGES.....	139
GM5 ATM/ANS.OR.A.045(a) Management of change to a functional system .....	140
EXAMPLE OF NOTIFICATION FORM FOR AN AERODROME FLIGHT INFORMATION SERVICES (AFIS) PROVIDER.....	140
AMC1 ATM/ANS.OR.A.045(a)(3) Changes to the functional system .....	141
NOTIFICATION TO USERS OF THE SERVICE.....	141
GM1 ATM/ANS.OR.A.045(a)(3) Changes to the functional system .....	141
DEDICATED PUBLICATION FOR PROPOSED CHANGES .....	141
AMC1 ATM/ANS.OR.A.045(b) Changes to the functional system .....	141
MODIFICATION OF A NOTIFIED CHANGE .....	141
AMC1 ATM/ANS.OR.A.045(d) Changes to the functional system .....	142
ENTRY INTO OPERATIONAL SERVICE OF A CHANGE SELECTED FOR REVIEW .....	142
GM1 ATM/ANS.OR.A.045(c); (d) Changes to the functional system .....	142
TRANSITION INTO OPERATION.....	142
GM2 ATM/ANS.OR.A.045(c); (d) Changes to the functional system .....	142
CHANGES IMPLEMENTED PRIOR TO RECEIVING APPROVAL .....	142
AMC1 ATM/ANS.OR.A.045(e) Changes to the functional system.....	142



CHANGES AFFECTING MULTIPLE SERVICE PROVIDERS — OVERARCHING SAFETY ARGUMENT.....	142
GM1 ATM/ANS.OR.A.045(e) Changes to the functional system .....	142
CHANGES AFFECTING MULTIPLE SERVICE PROVIDERS AND AVIATION UNDERTAKINGS — GENERAL.....	142
GM2 ATM/ANS.OR.A.045(e) Changes to the functional system .....	143
AFFECTED STAKEHOLDERS — SERVICE PROVIDERS AND AVIATION UNDERTAKINGS.....	143
GM3 ATM/ANS.OR.A.045(e) Changes to the functional system .....	143
CHANGE AFFECTING MULTIPLE SERVICE PROVIDERS AND AVIATION UNDERTAKINGS — COORDINATION.....	143
GM1 ATM/ANS.OR.A.045(e)(2) Changes to the functional system .....	144
CHANGE AFFECTING MULTIPLE SERVICE PROVIDERS AND AVIATION UNDERTAKINGS — ASSUMPTIONS AND RISK MITIGATIONS .....	144
GM4 ATM/ANS.OR.A.045(e) Changes to the functional system .....	144
COORDINATION WITH AFFECTED AVIATION UNDERTAKINGS.....	144
GM1 ATM/ANS.OR.A.045(f) Changes to the functional system .....	145
LACK OF COORDINATION .....	145
SUBPART B — MANAGEMENT (ATM/ANS.OR.B).....	145
GM1 ATM/ANS.OR.B.005(a)(4) Management system .....	145
IDENTIFICATION OF CHANGES TO FUNCTIONAL SYSTEMS .....	145
AMC1 ATM/ANS.OR.B.005(d) Management system .....	146
REACTION TO UNDERPERFORMANCE OF FUNCTIONAL SYSTEMS.....	146
AMC1 ATM/ANS.OR.B.010(a) Change management procedures.....	147
GENERAL.....	147
GM1 ATM/ANS.OR.B.010(a) Change management procedures.....	147
GENERAL.....	147
GM2 ATM/ANS.OR.B.010(a) Change management procedures.....	149
EXAMPLE OF COMPLIANCE MATRIX FOR CHANGE MANAGEMENT PROCEDURES APPROVAL .....	149
GM3 ATM/ANS.OR.B.010(a) Change Management Procedures.....	151
LIAISON WITH THE COMPETENT AUTHORITY .....	151
AMC2 ATM/ANS.OR.B.010(a) Change management procedures.....	151
REGISTER OF NOTIFIED CHANGES.....	151
SUBPART C — SPECIFIC ORGANISATIONAL REQUIREMENTS FOR SERVICE PROVIDERS OTHER THAN AIR TRAFFIC SERVICES PROVIDERS.....	151
GM1 ATM/ANS.OR.C.005(a)(1) Safety support assessment and assurance of changes to the functional system.....	151



GENERAL..... 151

GM2 ATM/ANS.OR.C.005(a)(1) Safety support assessment and assurance of changes to the functional system ..... 152

    PROVISION OF SAFETY SUPPORT ASSESSMENTS BY COMPOUND PROVIDERS ..... 152

GM3 ATM/ANS.OR.C.005(a)(1) Safety support assessment and assurance of changes to the functional system ..... 152

    SAFETY SUPPORT ASSESSMENT ..... 152

GM4 ATM/ANS.OR.C.005(a)(1) Safety support assessment and assurance of changes to the functional system ..... 153

    SCOPE OF THE CHANGE..... 153

GM3 ATM/ANS.OR.C.005(a)(1) Safety support assessment and assurance of changes to the functional system ..... 154

    TRAINING..... 154

GM4 ATM/ANS.OR.C.005(a)(1) Safety support assessment and assurance of changes to the functional system ..... 154

    INTERACTIONS..... 154

AMC1 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system ..... 154

    FORM OF ASSURANCE..... 154

GM1 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system ..... 154

    SPECIFICATION ..... 154

GM2 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system ..... 155

    ASSURANCE LEVELS..... 155

AMC2 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system ..... 155

    COMPLETENESS OF THE ARGUMENT..... 155

GM3 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system ..... 155

    COMPLETENESS OF THE ARGUMENT..... 155

GM4 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system ..... 159

    SAFETY SUPPORT REQUIREMENTS..... 159



AMC3 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system .....	159
DETERMINATION OF THE SPECIFICATION OF THE CHANGED SERVICE .....	159
AMC4 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system .....	160
DETERMINATION OF THE OPERATIONAL CONTEXT FOR THE CHANGE .....	160
AMC1 ATM/ANS.OR.C.005(b)(1) Safety support assessment and assurance of changes to the functional system .....	160
VERIFICATION .....	160
GM1 ATM/ANS.OR.C.005(b)(1) Safety support assessment and assurance of changes to the functional system .....	160
NO SAFETY SUPPORT REQUIREMENTS AT SYSTEM LEVEL .....	161
GM1 ATM/ANS.OR.C.005(b)(1) Safety support assessment and assurance of changes to the functional system .....	161
VERIFICATION .....	161
AMC1 ATM/ANS.OR.C.005(b)(2) Safety support assessment and assurance of changes to the functional system .....	162
MONITORING .....	162
GM1 ATM/ANS.OR.C.005(b)(2) Safety support assessment and assurance of changes to the functional system .....	162
MONITORING OF INTRODUCED CHANGES .....	162

## **ACCEPTABLE MEANS OF COMPLIANCE AND GUIDANCE MATERIAL TO ANNEX III — SPECIFIC REQUIREMENTS FOR THE PROVISION OF AIR TRAFFIC SERVICES (PART-ATS) ..... 163**

SUBPART A — ADDITIONAL ORGANISATION REQUIREMENTS FOR THE PROVISION OF AIR TRAFFIC SERVICES (ATS.OR) .....	163
GM1 ATS.OR.205(a)(1) Safety assessment and assurance of changes to the functional system .....	163
GENERAL .....	163
GM2 ATS.OR.205(a)(1) Safety assessment and assurance of changes to the functional system .....	163
SCOPE OF THE CHANGE .....	163
GM3 ATS.OR.205(a)(1) Safety assessment and assurance of changes to the functional system .....	164
TRAINING .....	164
GM4 ATS.OR.205(a)(1) Safety assessment and assurance of changes to the functional system .....	164
DESCRIPTION OF THE SCOPE — MULTI-ACTOR CHANGE .....	164
GM1 ATS.OR.205(b)(1)(iii) Safety assessment and assurance of changes to the functional system .....	164



INTERACTIONS.....	164
AMC1 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system .....	164
FORM OF ASSURANCE.....	164
GM1 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system .....	164
SAFETY CRITERIA .....	164
GM2 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system .....	165
ASSURANCE LEVELS.....	165
AMC2 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system .....	165
COMPLETENESS OF THE ARGUMENT .....	165
GM3 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system .....	165
COMPLETENESS OF THE ARGUMENT .....	165
GM4 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system .....	168
SAFETY REQUIREMENTS.....	168
GM1 ATS.OR.205(b) Safety assessment and assurance of changes to the functional system .....	169
PROPORTIONALITY OF SAFETY ASSESSMENT.....	169
GM2 ATS.OR.205(b) Safety assessment and assurance of changes to the functional system .....	169
SAFETY ASSESSMENT METHODS.....	169
AMC1 ATS.OR.205(b)(1) Safety assessment and assurance of changes to the functional system.....	169
COMPLETENESS OF HAZARD IDENTIFICATION.....	169
AMC2 ATS.OR.205(b)(1) Safety assessment and assurance of changes to the functional system.....	169
HAZARDS TO BE IDENTIFIED.....	169
GM1 ATS.OR.205(b)(1) Safety assessment and assurance of changes to the functional system.....	169
HAZARD IDENTIFICATION .....	169
AMC1 ATS.OR.205(b)(2) Safety assessment and assurance of changes to the functional system.....	171
DETERMINATION OF THE SAFETY CRITERIA FOR THE CHANGE .....	171
AMC1 ATS.OR.205(b)(3) Safety assessment and assurance of changes to the functional system.....	171
COMPLETENESS OF RISK ANALYSIS .....	171
AMC2 ATS.OR.205(b)(3) Safety assessment and assurance of changes to the functional system.....	172
SEVERITY CLASSIFICATION OF ACCIDENTS LEADING TO HARMFUL EFFECTS .....	172
AMC1 ATS.OR.205(b)(4) Safety assessment and assurance of changes to the functional system.....	172
RISK EVALUATION.....	172
AMC2 ATS.OR.205(b)(4) Safety assessment and assurance of changes to the functional system.....	172





RISK MITIGATION .....	172
GM1 ATS.OR.205(b)(4) Safety assessment and assurance of changes to the functional system.....	173
RISK ANALYSIS IN TERMS OF SAFETY RISK.....	173
GM2 ATS.OR.205(b)(4) Safety assessment and assurance of changes to the functional system.....	174
SAFETY ANALYSIS IN TERMS OF PROXIES.....	174
AMC1 ATS.OR.205(b)(5) Safety assessment and assurance of changes to the functional system.....	180
VERIFICATION.....	180
GM1 ATS.OR.205(b)(5) Safety assessment and assurance of changes to the functional system.....	180
OUTCOME OF RISK EVALUATION .....	180
GM2 ATS.OR.205(b)(5) Safety assessment and assurance of changes to the functional system.....	181
RISK EVALUATION — UNCERTAINTY .....	181
GM3 ATS.OR.205(b)(5) Safety assessment and assurance of changes to the functional system.....	181
RISK EVALUATION — FORMS OF RISK EVALUATION.....	181
GM4 ATS.OR.205(b)(5) Safety assessment and assurance of changes to the functional system.....	181
TYPE OF RISK MITIGATION .....	181
GM1 ATS.OR.205(b)(5)(ii) Safety assessment and assurance of changes to the functional system .....	181
VERIFICATION OF SAFETY CRITERIA .....	181
AMC1 ATS.OR.205(b)(6) Safety assessment and assurance of changes to the functional system.....	182
MONITORING OF INTRODUCED CHANGE .....	182
GM1 ATS.OR.205(b)(6) Safety assessment and assurance of changes to the functional system.....	182
MONITORING OF INTRODUCED CHANGE .....	182
AMC1 ATS.OR.210(a) Safety criteria .....	182
OTHER MEASURES RELATED TO SAFETY RISKS .....	182
AMC2 ATS.OR.210(a) Safety criteria .....	182
PROXIES.....	182
GM1 ATS.OR.210(a) Safety assessment and assurance of changes to the functional system .....	183
SAFETY CRITERIA IN TERMS OF PROXIES FOR SAFETY RISKS.....	183
GM1 ATS.OR.210(b)(2) Safety criteria .....	183
SAFETY OF THE CHANGE .....	183



**ACCEPTABLE MEANS OF COMPLIANCE AND GUIDANCE MATERIAL  
TO COMMISSION REGULATION (EU) No XXX/XXXX****GM1 to Article 5 Service Providers and Article 6(2) Oversight capabilities****MANAGEMENT, ASSESSMENT, ASSURANCE AND OVERSIGHT OF CHANGES TO FUNCTIONAL SYSTEMS****Overview**

- (a) This Guidance Material (GM) contains a description of various parts of Commission Regulation (EU) XXXX/XXX, Acceptable Means of Compliance (AMC) and GM associated with the management, assessment and assurance of changes to the functional systems of service providers and the oversight thereof. These parts are distributed throughout Annexes II, III and IV. In order to maintain their coherence, their relationships are explained here and within the GM to the Annexes.
- (b) The Implementing Rules (IRs) associated with the management, assessment, assurance and oversight of changes to functional systems included in this Regulation, as well as the related AMC and GM, were conceived and written as a coherent whole. The relationship of these regulatory elements with the rest of the elements of this Regulation and the structure of this Regulation itself has meant that they are now distributed throughout the provisions of this Regulation. Due to the extensive nature and the wide-ranging scope of this GM, it is split into two parts. One of them, that which helps to illustrate the meaning of a particular requirement or specification and is used to support the interpretation of them, is integrated within the normal structure of the AMC/GM to Annexes II, III, and IV to this Regulation. The other part is included in this GM and its Appendix.
- (c) ‘Elements of changes to functional systems in the provisions contained in the Annexes to the Implementing Rule’ below, provides an explanation of the provisions in Annexes II, III, and IV related to changes to the functional systems of service providers and the relationship between these provisions.
- (d) Appendix I to this GM gathers general guidance material related to changes to functional systems. Said guidance material has a broader scope and contains more extensively the underlying principles of the provisions that govern the management, assessment, assurance and oversight of changes to functional systems.
- (e) Appendix I to this GM containing general guidance material related to changes to functional systems has the following structure:
  - (1) Definitions of terms and concepts that are used in the AMC/GM to Commission Regulation (EU) XXXX/XXX but are not detailed in the Regulation itself.
  - (2) Models that underpin the Regulation and provide the rationale behind it.
  - (3) A process perspective on the rules, usually where more than one party is involved.
  - (4) More expansive guidance on specific topics.



**Elements of changes to functional systems in the provisions contained in the Annexes to the Implementing Rule**

- (a) Changing the functional system of a service provider is modelled as a process that is activated by the Management System/Safety Management System (MS/SMS) of the service provider. An overview of this process annotated with activities and the reference to the requirement where these activities may be found in the Regulation is provided in Figure 1.
- (b) Activation is caused by a process that assesses the desire for change or the need to change. The need to change is driven by three monitoring activities:
  - (1) Monitoring the performance of the service delivered by the functional system in order to detect when it is underperforming (ATM/ANS.OR.B.005(d)).
  - (2) Monitoring the context in which the service is provided, both internally within the organisation, e.g. the business' desire to improve efficiency/effectiveness, and externally in the operational context, for proposed changes in this context that might cause changes in the behaviour of the service delivered by the functional system (ATM/ANS.OR.B.005(a)(4)).
  - (3) Monitoring the wider environment to establish if there are changes in technology and economics that render safety improvement a practical proposition (ATS.OR.200)(a)(2)(iii)).



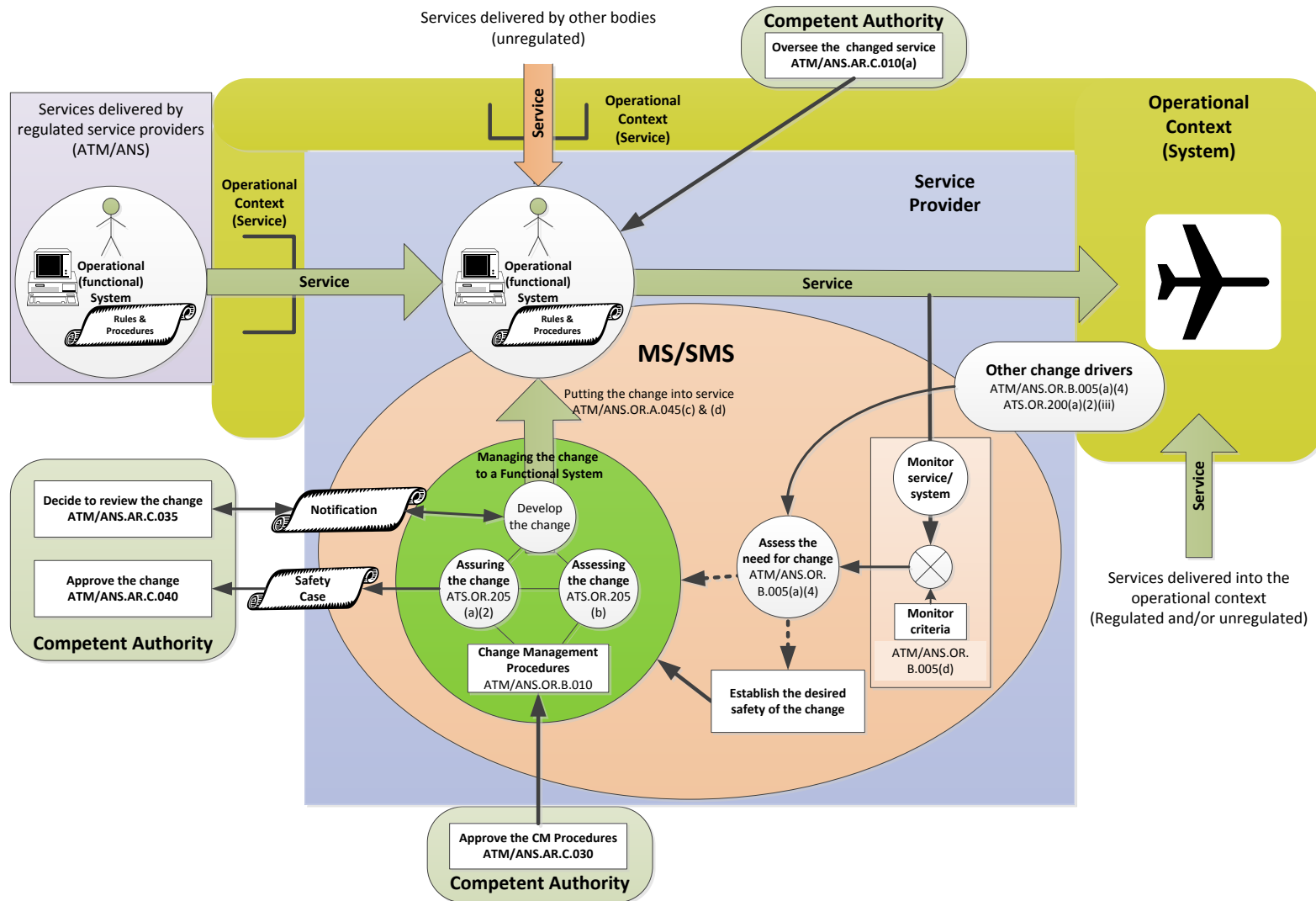


Figure 1: Functional System Change Activities



- (c) Having decided to make a change, the MS/SMS then needs to set the objective for the safety of the change, which the fulfilment of safety criteria will necessitate (ATS.OR.210(b)(2)). This can take one of the following three forms:
- (1) The change will leave the functional system as safe as it was before the change; or
  - (2) While not leaving the system as safe as before, the change has some societal benefit that compensates for the reduction in safety and this is agreed by the Competent Authority (CA); or
  - (3) While not leaving the system as safe as before, the change will be followed by one or more changes that will leave the system safe enough. The additional risk potentially introduced by the change and the time over which it will exist must be acceptable to the CA.

Note that the objective for safety may change as the change itself is developed, hence it should be seen more as a goal (objective) than a requirement.

In general, changes initiated by a service provider other than an air traffic services (ATS) provider will be multi-actor changes; consequently, a responsive change may need to be triggered by each air traffic services provider that is affected by the change. In this case, an objective for the safety of the change is established individually by each air traffic services provider who has to make a responsive change. It is, of course, possible that the original change does not alter the service provided at all. In such case, no objectives for safety need be established and all that is needed is a safety support assurance case.

- (d) The service provider needs to notify its CA of the proposed change and in the case of a multi-actor change, it also needs to inform other service providers and aviation undertakings that might be affected by the change (ATM/ANS.OR.A.045(a)). Where the proposed change is novel, complicated or large, the CA may need more information than that provided in the notification, in order to decide whether or not to review the assurance case related to the change. The CA will seek this information from the service provider (ATM/ANS.AR.C.035(a), ATM/ANS.OR.A.045(a)).
- (e) The CA decides whether to review the assurance case based on the risk posed by the change and informs the service provider of their decision (ATM/ANS.AR.C.035).
- (f) During the change, the service provider assesses:
- (1) the safety of the change, in the case of an air traffic services provider (ATS.OR.205(b)), or
  - (2) the trustworthiness of the change, in the case of another service provider (ATM/ANS.OR.C.005(b)).

The safety or trustworthiness of the change must be assured to the satisfaction of the service provider (ATM/ANS.OR.C.005(a)(2), ATS.OR.205(a)(2)) and if it is to be reviewed, then also to the satisfaction of the CA (ATM/ANS.AR.C.040)

An optimum change is one where the assurance case is developed at the same time as the change so that it may influence the structure and detail of the change. In such a change, the cost of developing the assurance case and the cost of developing the change are minimised.

In a multi-actor change, there is a need for coordination in order to establish the behavioural dependencies of each service associated with the change. This is so that assumptions related to more than one service provider may be identified and shared risk mitigations implemented accordingly



(ATM/ANS.OR.A.045(e)). Such coordination will result in the change being treated as though it were a single change.

- (g) Once a valid assurance case exists and has been approved, where applicable, the change may be implemented and the service modified (ATM/ANS.OR.A.045(c) & (d)).
- (h) The CA will continue to oversee the change after it has been implemented as part of its general oversight of the service provider (AMC1 ATM/ANS.AR.C.010(a) provides details of this oversight). This oversight, which is based on checking that the monitoring criteria, predicted as part of the assurance argument, remain satisfied, demonstrates that the assurance case remains valid (ATM/ANS.OR.C.005(b)(2), ATS.OR.205(b)(6)).
- (i) The procedures used to manage changes to the functional system have to be approved by the CA prior to their use (ATM/ANS.OR.B.010(b)). Flexibility is provided by allowing a service provider to deviate from the approved rules for a particular change, although the deviation itself must be justified by the service provider and approved by the CA in advance, i.e. before the decision is made (ATM/ANS.OR.B.010(c)).
- (j) The activities performed in making changes to a functional system and in overseeing these changes are described above. The table below summarises these activities and shows where the rules governing them may be found:

Activities	CA	Service provider	
		ATS	Other
Developing Change Management procedures	N/A	Implied by ATM/ANS.OR.B010(a), (b)(1) & (c)(1)	
Approving Change Management procedures	ATM/ANS.AR.C.030	ATM/ANS.OR.B010(b)(1) & (c)(2)	
Using Change Management procedures	N/A	ATM/ANS.OR.B.010(b)(2) & (c)(3)	
Multi-actor changes	ATM/ANS.AR.A.005(c); ATM/ANS.AR.C.040(a)(2)	ATM/ANS.OR.A.045(e), (f) & (a)(3)	
Assessing the need for change	N/A	ATM/ANS.OR.B.005(a)(4) & (d)	
		ATS.OR.200(a)(2)(iii)	
Establishing the desired safety of the change	N/A	ATS.OR.210(b)(2)	



Notifying planned changes	ATM/ANS.AR.C.035(a)	ATM/ANS.OR.A.045(a) & (b)	
Deciding to review the notified change	ATM/ANS.AR.c.035(b), (c) & (d)	N/A	N/A
Assessing the change	N/A	ATM/ANS.OR.C.005(a)(1) & (b)	ATS.OR.205(a)(1) & (b)
Assuring the change	N/A	ATM/ANS.OR.C.005(a)(2)	ATM/ANS.OR.205(a)(2)
Approving the notified change	ATM/ANS.AR.C.040	N/A	N/A
Putting the notified change into service	Where applicable, ATM/ANS.AR.C.040(b)(1)	ATM/ANS.OR.A.045(c) & (d)	
Overseeing the changed services	ATM/ANS.AR.C.010(a)	ATM/ANS.OR.C.005(b)(2) ATM/ANS.OR.B.005(d)	ATS.OR.205(b)(6) ATM/ANS.OR.B.005(d)



**APPENDIX I: GENERAL GUIDANCE MATERIAL RELATED TO CHANGES TO FUNCTIONAL SYSTEMS**

This Appendix contains general guidance material related to changes to functional systems. Said guidance material has a broader scope than the GM to Annexes II, III, and IV to this Regulation and contains more extensively the underlying principles of the provisions that govern the management, assessment, assurance and oversight of changes to functional systems, rather than an illustration of the meaning of a particular requirement or specification. The reader is suggested to read this guidance material whenever there is a reference in the AMC/GM to the Annexes to this Regulation and the reader wishes to obtain broader understanding of the topics covered here in relation to the changes to functional systems.

The Appendix has the following structure:

- (1) Definitions of terms and concepts that are used in the AMC/GM to Commission Regulation (EU) XXXX/XXX but are not detailed in the Regulation itself — e.g. ‘safety risk’, ‘component parts of functional systems and equipment’ and ‘assurance case structure’.
- (2) Models that underpin the Regulation and provide the rationale behind it — e.g. what is a ‘functional system’, what is meant by the ‘view of safety’ and what impact this has on the Regulation, and what form service providers’ organisations can take.
- (3) A process perspective on the rules, usually where more than one party is involved — e.g. interactions involved during approval of the change management procedure or the approval of a change, multi-actor changes, the way that a service provider decides to make a change to the functional system (and necessary interactions with other service providers).
- (4) More expansive guidance on specific topics, e.g. Safety Assessment and Safety support assessment, Risk analysis and evaluation, risk-based selection and review of assurance cases. This part of the Appendix contains material that is of a broader and deeper nature than that for the Annexes and consequently would obscure the succinct nature of the GM provided for each Annex.





**1. DEFINITIONS****1.1. SAFETY SUPPORT ASSURANCE AND SAFETY ASSURANCE**

The key concepts used in safety assurance and safety support assurance and the terms used to describe them are given in the table below. Please note that where reference is made to either a safety case or a safety support case (depending on the circumstance), it will be referred to as an assurance case.

Safety Support		Safety	
<b>Safety support assurance</b>	Argues that the service behaves and will behave only as specified <sup>1</sup> in the specified context. <sup>2</sup>	<b>Safety assurance</b>	Argues that the proposed change to the functional system is and will be acceptably safe for a given application in a given operating context.
<b>Safety support case</b>	A structured documented argument, supported by a body of evidence, that provides a compelling, comprehensible and valid justification that the system behaves and will behave only as specified in the specified context.	<b>Safety case</b>	A structured documented argument, supported by a body of evidence that provides a compelling, comprehensible and valid justification that a change to the functional system is and will be acceptably safe for a given application in a given operating context.
<b>Safety support case report</b>	The safety support case report for a change will identify the arguments (claims, inferences and evidence) of the safety support case (although not necessarily all of them), but will probably not include the bulk of the supporting evidence due to the practicalities of providing it in the report. The service provider is obliged to facilitate access to any of this additional information that the CA requires for the evaluation.	<b>Safety case report</b>	The safety case report for a change will identify the arguments (claims, inferences and evidence) of the safety case (although not necessarily all of them), but will probably not include the bulk of the supporting evidence due to the practicalities of providing it in the report. The air traffic services provider is obliged to facilitate access to any of this additional information that the CA requires for the evaluation.
<b>Safety support assessment</b>	All the activities required to produce a safety support case, i.e. all the activities defined in	<b>Safety Assessment</b>	All the activities required to produce a safety case, i.e. all the activities defined in

<sup>1</sup> The safety support assurance, which is documented in the safety support case, must argue that the specification as stated is complete and correct, i.e. the service behaves only as specified.

<sup>2</sup> This is not necessarily the complete statement of the way it behaves; it is limited to the ways that the user can access, i.e. that which is constrained by the context of use.



	ATM/ANS.OR.C.005.		ATS.OR.205.
<b>Assurance case</b>	The collective noun used for either safety cases or safety support cases.		
<b>Assurance case report</b>	The collective noun used for either safety case reports or safety support case reports.		
<b>Requirement:</b>	A thing that is needed or wanted (it will be or will do); a necessary condition.		
<b>Specification:</b>	A precise and detailed definition of what a thing is claimed to be and to do.		

## 1.2. SPECIFICATION OF THE CHANGED SERVICE

- (a) The specification of the change in the service defines how the service will behave after the change and does not restate how the unchanged service behaves, i.e. the change specification is an alteration of the full specification of the service.
- (b) The specification defines how the service behaves at the interface with its user, and NOT the detailed design level of the systems internal workings, i.e. a black box specification NOT a white box specification. It includes the form of the interface and any constraints on the context of use.
- (c) Typically, specifications for services describe the functionality and performance of the service in terms of e.g. accuracy, reliability, availability, continuity and timeliness.
- (d) The service provider, other than an air traffic services provider, of the service to be changed should explain where the changes in the specification have come from, e.g. International Civil Aviation Organization (ICAO), European Commission (EC), internal business, Standards, user organisation, in order to aid understanding of the change.
- (e) There are specifications for: every phase of the service, each transition of the change and the final commissioning of the change.
- (f) The specification for a specified context means that there are two kinds of specifications:
  - (1) The specification of the functionality and performance of the service, i.e. how it behaves; and
  - (2) The specification of the context in which the specification of the way it behaves is valid.

## 1.3. ARCHITECTURE OF FUNCTIONAL SYSTEMS

Notes on selected terms used to describe the architecture of functional systems

- (a) A functional system can be divided into functional subsystems, although system and subsystem may be used synonymously.
- (b) In addition, for brevity and in agreement with normal systems nomenclature, 'system' and 'subsystem' are used as synonyms for 'functional system' and 'functional subsystem'.
- (c) An element can comprise only sub-elements of the same type, i.e. equipment, procedure, human resource.
- (d) An element can be a set or assembly of elements of the same type, e.g. a group of people, a set of procedures or a collection of equipment.



- (e) Elements and sub-elements may be used synonymously.
- (f) A system or subsystem can comprise elements of different types.
- (g) A subsystem that comprises only either equipment elements, procedural elements or human resource elements is also an element.
- (h) There is no unique way of decomposing systems into subsystems or elements.
- (i) A subsystem is viewed/described as a component when, for the current analysis, there is no interest in its composition, i.e. the subsystems (parts) it consists of.
  - (1) For example, a control tower may be considered to be a component, where the analytical view is that of the parts of an airport even though the tower actually consists of many elements of different types, e.g. the control tower consists of people, procedures and equipment.
  - (2) The definition of what is viewed as a component is not absolute but depends on the analysis being carried out, i.e. in the hierarchy of the subsystems of a functional system, a subsystem may be viewed as a component for one analysis and may be considered to be part of a component for a different analysis.

#### 1.4. CONCEPT OF SAFETY RISK

- (a) 'hazard' means any condition, event or circumstance which could induce a harmful effect, as per Annex I.

'risk' means the combination of the overall probability or frequency of occurrence of a harmful effect induced by a hazard and the severity of that effect, as per Annex I.

'harm' (as per Oxford dictionary) means (*noun*):

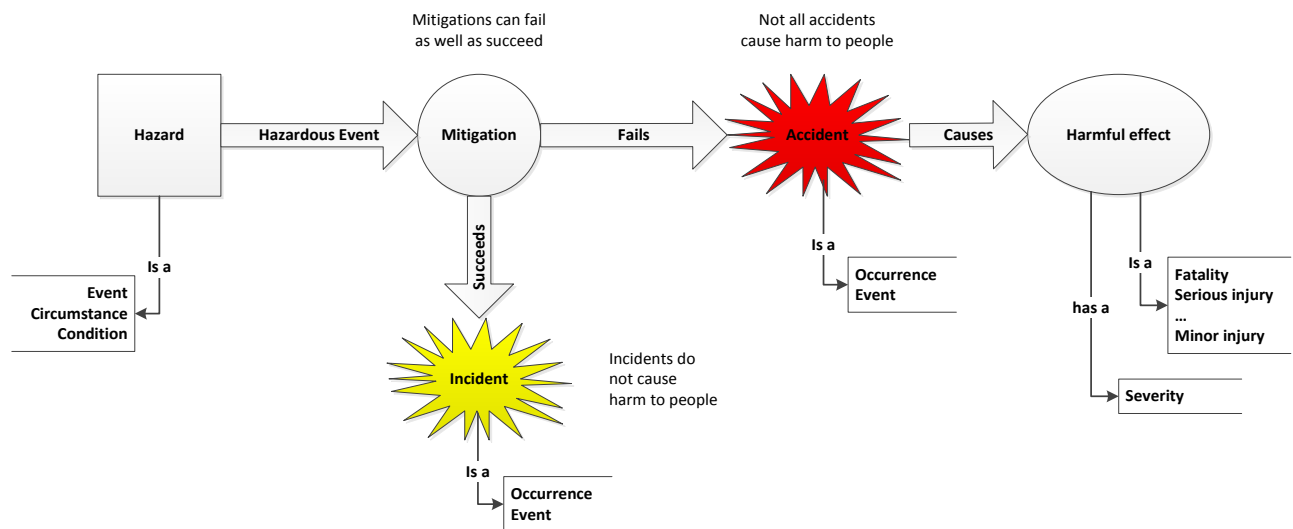
- physical injury, especially that which is deliberately inflicted, e.g. *I didn't mean to cause him any harm.*
- material damage, e.g. *It's unlikely to do much harm to the engine.*
- actual or potential ill effects or danger, e.g. *There's no harm in asking her.*

'safety' (as per Oxford dictionary) means (*noun*):

- the condition of being protected from or unlikely to cause danger, risk, or injury, e.g. *They should leave for their own safety.*

- (b) Consequently, a safety risk is a combination of the overall probability or frequency of occurrence of a harmful (injurious) effect on people and the severity of that effect. The term 'risk' is used throughout the IR, AMC and GM related to changes to the functional systems as a synonym for safety risk. This is for simplicity and is justified because the Regulation deals primarily with the safety of a change.





**Figure 2: Taxonomy of Safety**

While hazards can be a circumstance, a condition or an event, for the purposes of the taxonomy and subsequent guidance, only hazardous events are considered. While circumstantial or conditional hazards, e.g. presence of dense fog, may contribute to a hazardous event, e.g. taking a wrong taxi exit, it is the event that is primarily of interest in accident (harmful effect) analysis.

## 2. UNDERLYING MODELS OF CHANGE MANAGEMENT

### 2.1. FUNCTIONAL SYSTEM

#### 2.1.1. Functional system model

- The purpose of this guidance material is to provide a reference model that describes the structure of the functional system, the relationships between it and the context in which it is used, and the way the effects of a change are propagated throughout the wider system.
- Where reference is made to the functional system, the model described here may be used as the basis for understanding how the provisions of this Regulation should be applied.
- An Air Traffic Management/Air Navigation Services (ATM/ANS) functional system comprises its components (people, procedures and equipment (hardware (HW) and software (SW)) and the way they are organised (the architecture — the form and function of the connections between the components). The functionality and performance<sup>3</sup> of the functional system depends on the transfer functions of the components and the relationships between the components.
- Hardware and software are not explicitly treated in the Regulation because the Regulation is written in terms of the behaviour of the equipment and not of the attributes of its constituent parts. However, a rule that sets criteria for the behaviour of equipment applies to that part, or those parts of the equipment involved in producing the behaviour, e.g. a criterion that is applicable to a service delivered by a piece of equipment would, if provided by a computer, apply equally to the operation of the software within the computational environment. Consequently,

<sup>3</sup> Usually the performance comprises the constraints on the functionality, e.g. accuracy, timeliness, reliability, which are imposed on the functional system by the choice of components and the context in which they operate.

the requirements for the assurance of safety and safety support, when relevant to the behaviour of a computer, are requirements for the assurance of the software within the computational environment because that software together with the computational environment determines how the service delivered by the computer behaves.

- (e) An ATM/ANS service will normally be used in another system; for example, the service delivered by an air traffic services provider is used in the air transport system by the aircraft. The way the part of the air transport system shown in Figure 3 (referred to as the 'System') behaves<sup>4</sup> depends upon the interactions of the outputs delivered by the functional systems<sup>5</sup> (the services, i.e. their functionality and performance) and the physical environment in which they are delivered.
- (f) The context in which the System operates can be thought of as consisting of two parts:
  - (1) the environment in which the functional system operates (functional system context (FS context)), e.g. the 'people' environment in the control tower and the local equipment environment; and
  - (2) the context in which services operate (operational context), e.g. the topology enclosed by the serviced airspace, the volume of serviced traffic, other traffic, the dimensions and structure of the airspace and weather, and the context provided by all the services being delivered in the same airspace.
- (g) In addition, the service provider may use services, provided by another service provider or some other unregulated service provider, in generating the service provided by its functional system. For example, the service delivered by a communication service provider will normally be used by an air traffic service in its functional system as part of an air traffic service<sup>6</sup>. Some of these other service providers are within the scope of Regulation (EC) No 216/2008, e.g. an aerodrome, while others are not, e.g. an electrical power supplier. A complete representation<sup>7</sup> of the system in which services are provided and in which they may be created is shown in Figure 3.

<sup>4</sup> The way a system behaves is an emergent property of that system. It is not a property of any particular component, but of the system as a whole. Similarly, safety is an emergent property of a system and cannot be said to be a property belonging to any individual component.

<sup>5</sup> Which depend upon the inputs provided to the functional system from the environment or from services delivered to the functional system.

<sup>6</sup> While the information may be provided by the communication service provider directly to an aircraft, the service is usually provided as part of air traffic service, which is the responsibility of an air traffic services provider, and so in this model the communications service provider is said to be providing a service to the air traffic services provider — for more information on the reasons for this interpretation see Section 2.3 of this Appendix.

<sup>7</sup> The diagram provides a graphical representation but it is not actually the most complex one, as for any particular functional system, there may be one or many services provided to it by one or many other organisations or unregulated bodies.



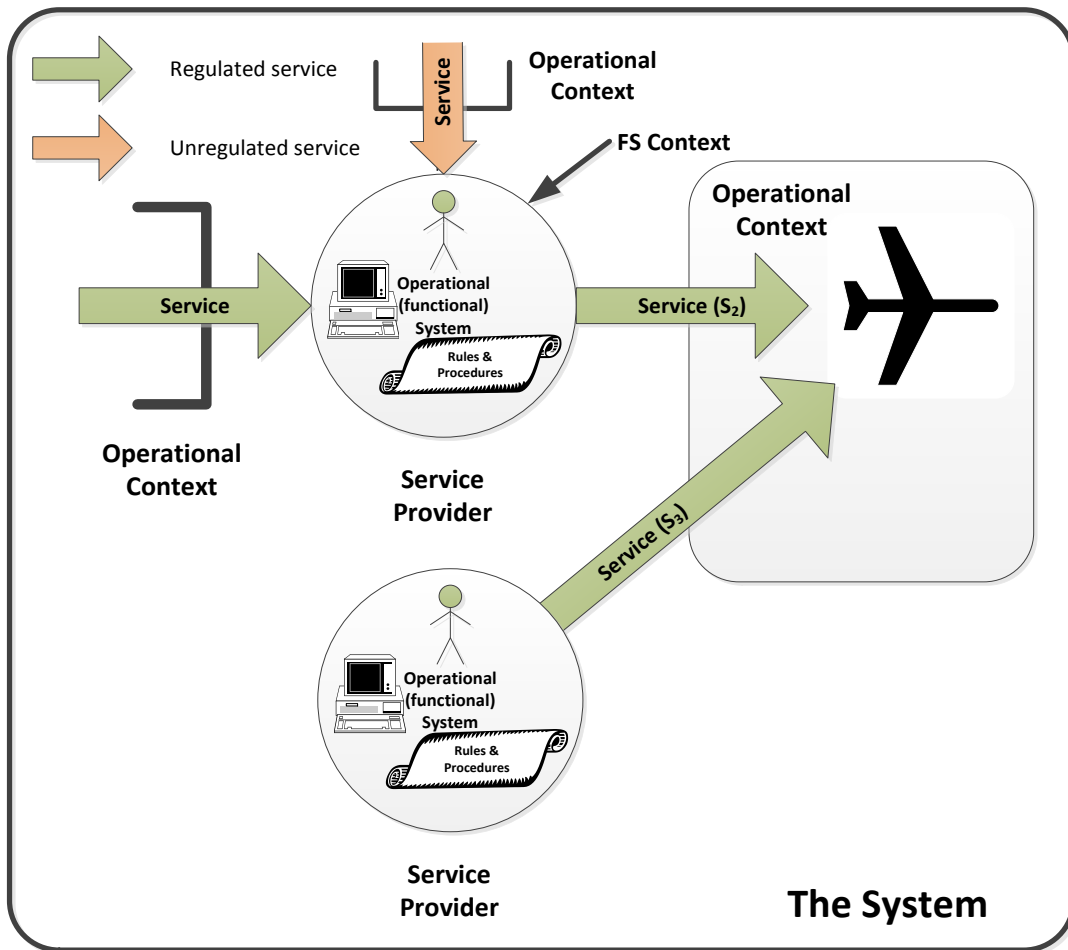
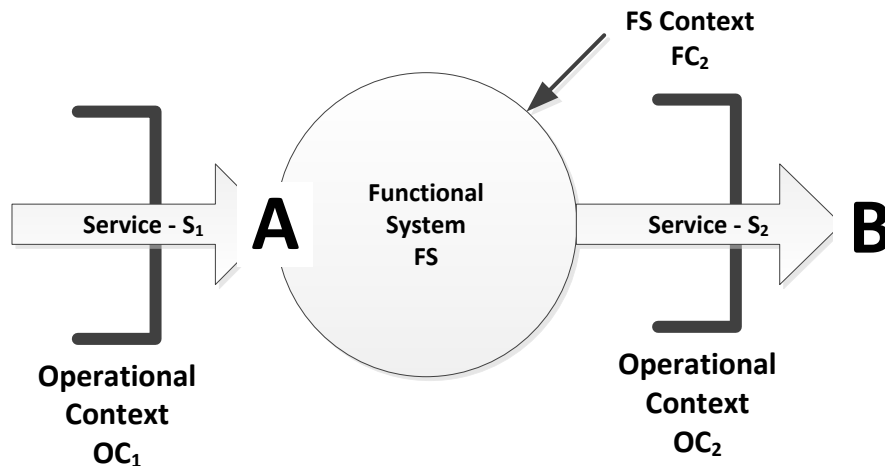


Figure 3: The functional system model in ‘The System’

- (h) In order to examine how the effects of change<sup>8</sup> are propagated, i.e. how change in any part of the system<sup>9</sup> can affect the way the system behaves, a modification to Figure 3 that will simplify the analysis, is shown in Figure 4 below.

<sup>8</sup> Note that in this Regulation, the word ‘change’ is used to describe changes to the functional system or to the context in which it operates (operational context) of an ATM/ANS provider.

<sup>9</sup> When ‘system’ is used in this guidance, it refers to the functional systems of the service providers (A and B), the services delivered to A by any unregulated bodies and the context in which the whole operates (FC<sub>1</sub>, OC<sub>1</sub>, FC<sub>2</sub>, OC<sub>2</sub>). This model is intended to be valid for any system, no matter how large or small.



**Figure 4: Simplified functional system model**

- (i) The way the service delivered to the functional system (FS) at point A behaves is a function of the properties of the service<sup>10,11</sup> delivered (S1) and the operational context (OC1) in which it is delivered. Similarly, the way the system behaves at point B is a function of the service (S2) delivered by the functional system (FS) and its operational context (OC2).
- (j) In Figure 1, two services are shown being delivered directly to a single aircraft. The way the system behaves in these circumstances is, therefore, the conjunction of the two services within a single physical operational context. If the way one of the services behaves needs to be analysed, e.g. when a change is proposed, then the simplification of Figure 2 may still be used, but with the additional constraint that the operational context (OC2) must now include the contextual impact of the other service. Consequently, in this case, the operational context (OC2) is a function of the physical environment (the topology enclosed by the serviced airspace, the volume of serviced traffic, other traffic, the dimensions and structure of the airspace, and weather) and the effects on the physical operational context due to the output of the other functional system, the service (S3).
- (k) The output of the functional system, the service (S2), depends upon the set of laws<sup>12</sup> governing the relationships between the inputs to the functional system and its outputs, the value of the inputs and the environment in which the functional system operates (FS Context: FC2). These laws are dependent on the components of the functional system and its architecture, i.e. they are a function of the people, procedures, equipment and architecture of the functional system. Similarly, since at least some of the inputs come from the service delivered to the functional system (S1), then the output of the functional system (S2) is also dependent on the way (S1) behaves at point A.
- (l) Consequently, should:
- (1) the service delivered to the provider (S1) change;
  - (2) the operational context (OC1) in which the service (S1) is delivered change;

<sup>10</sup> If this service was produced by another service provider, then it was produced by another functional system.

<sup>11</sup> This could be one or many services.

<sup>12</sup> The term 'laws' is used here in its normal mathematical sense, and does not imply anything of a legal nature.

- (3) any part of the functional system change;
  - (4) the environment in which the functional system operates (FC2) change; or
  - (5) the environment in which the system operates (OC2) change<sup>13</sup>,  
then the way the system behaves is likely to change.
- (m) In some cases, the change will be initiated by someone other than the service provider<sup>14</sup> and may also be undesired, e.g. a change to the operational context initiated by some other body. In this case, other parts of the functional system may be changed<sup>15</sup> in order to compensate for the different way the system would behave as a result. For example, if the operational context changes and we wish to keep the system behaving as it did before (the current performance), then one or more components of the functional system or its architecture needs (need) to be changed.
- (n) Even if a change, initiated by someone other than the service provider, does alter the way the system behaves, the change may still be acceptable to the user. Consequently, there is a need to distinguish between a change that has an acceptable impact on the way the system behaves and one that does not.
- (o) Equally, a change may be made to a service (S1) used by the service provider that does not impact on the service it delivers at all. This will be true when there is no relationship between the service used by the provider (S1)<sup>16</sup> and the service delivered by the provider (S2), e.g. altering the range or type of data in a message field that is not used by the functional system<sup>17</sup>.

### 2.1.2. Organisation model of service providers

The purpose of this guidance material is to show, using the functional system model described in Section 2.1.1 of Appendix I to GM1 to Article 5 & Article 6(c), and the legal basis for the definition of a service provider, how service providers may be organised.

- (a) For the purposes of safety management of changes, services<sup>18</sup> are produced by a functional system<sup>19</sup>. The description of that functional system and the way the effects of a change are propagated through a network of functional systems is described in Section 2.1.1 of Appendix I to GM1 to Article 5 & Article 6(c).
- (b) For an aircraft to travel safely, effectively and efficiently from its point of departure to its destination, many ATM/ANS services are needed.

<sup>13</sup> Including a change to S<sub>3</sub>.

<sup>14</sup> Or be a change to the operational context initiated by the ATM/ANS provider, e.g. a desire to increase traffic throughput.

<sup>15</sup> This is a responsive change, i.e. the functional system is changed in order to respond to (back off) a change by someone else. The change could also be part of a cooperative multi-actor change, where the ATM/ANS provider changes the functional system not only because the context of operation has changed, but also because the provider is seeking to change the context of operation.

<sup>16</sup> This is not the only possibility. For example, it would also be true if the functional system delivering a service to the ATM/ANS provider is changed, but neither the service (S<sub>1</sub>) nor its operational context (OC<sub>1</sub>) is changed.

<sup>17</sup> This may be an oversimplification. The way the system behaves under faulty conditions might be altered because of the range change. Also, any data checking performed by the provider using the changed service, may be affected by the range change.

<sup>18</sup> In Regulation (EC) No 549/2004, both services and functions are mentioned. However, this GM uses the notion that a function performs a service if the results of the function are delivered to another body. Consequently, only the term 'service' is used here.

<sup>19</sup> This can be thought of as the operational system as opposed to the management system.





- (c) A service provider delivers ATM/ANS services using its functional system. In providing such services, it may use the services of other service providers, the services provided by other parts of itself or the services of an unregulated body.
- (d) A representation<sup>20</sup> of a functional system is shown below:

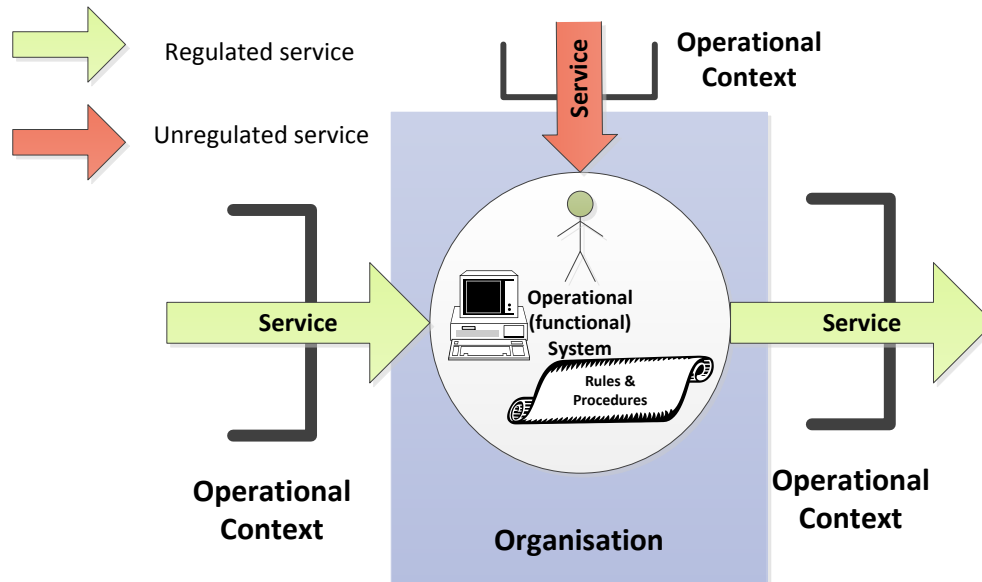


Figure 5: Functional system model

- (e) An individual organisation may provide one or more ATM/ANS services, e.g. an air traffic services provider may use its own surveillance and communications services as well as performing local Air Traffic Flow Management (ATFM) in addition to providing separation. It is also the case that the air traffic services provider, while providing surveillance services supporting the provision of separation, may also provide a surveillance service to other service providers.
- (f) A few examples<sup>21</sup> of possible internal structures of and connections between service providers and other bodies are shown below:
- (1) A service provider delivering the same type of service<sup>22</sup> to other service providers.

<sup>20</sup> The diagram is not actually complete as for any particular functional system there may be one or many services provided to it.

<sup>21</sup> These are just a few examples that illustrate the connection rules. The actual range of possible structures is probably endless.

<sup>22</sup> Although the type may be the same (e.g. surveillance service), the services to both users may be different, hence they have different specifications (e.g. the data format, the information data or the technology used to gather information may be different).

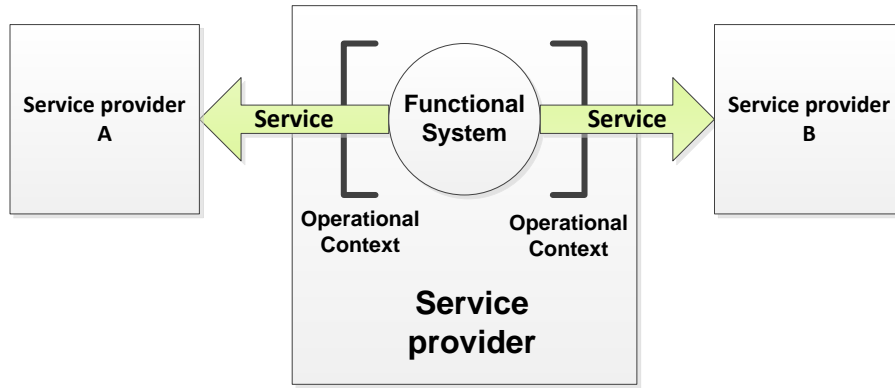


Figure 6: Functional system delivering services to different service providers

- (2) A service provider delivering<sup>23</sup> different types of services to other service providers.

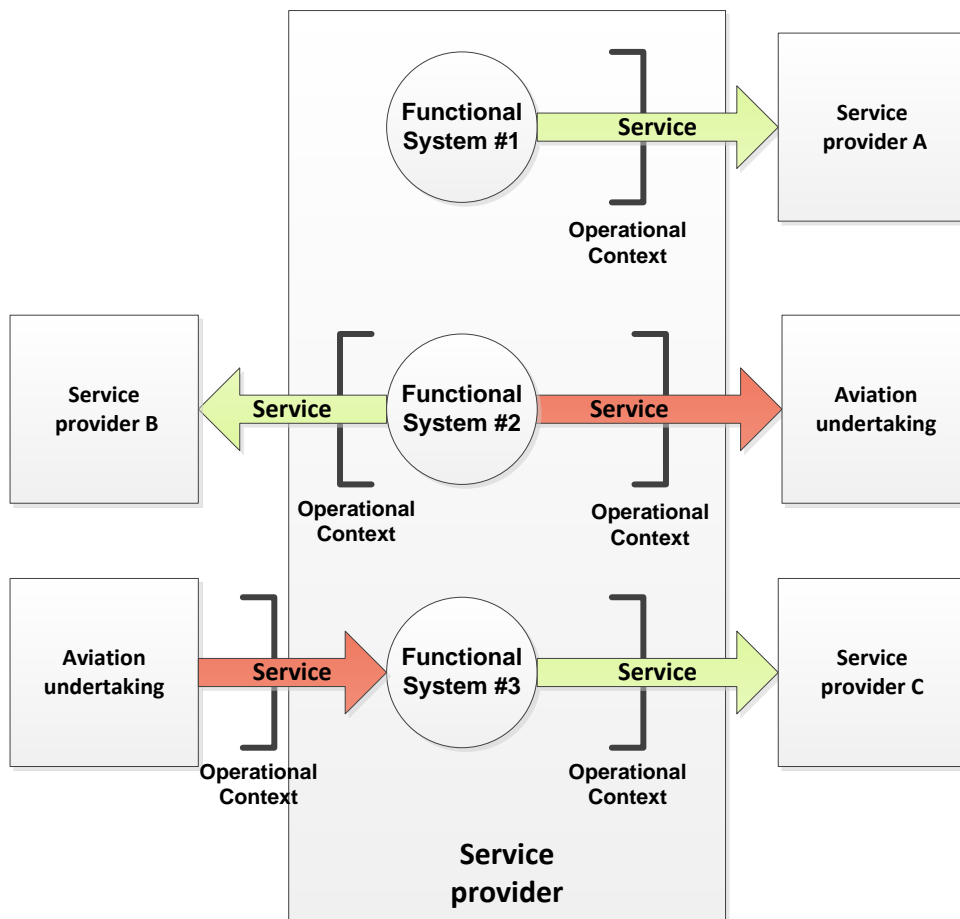
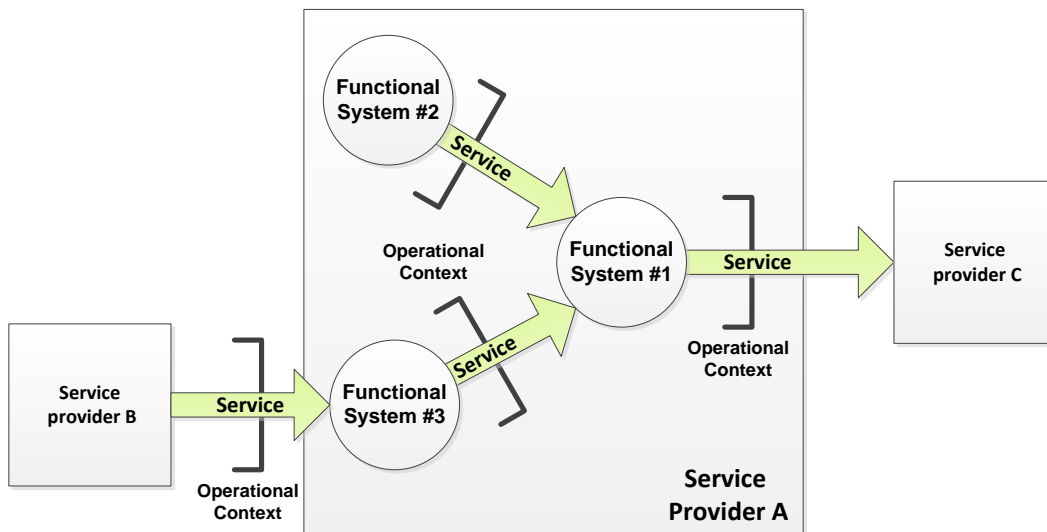


Figure 7: Service provider with multiple functional systems delivering services to other service providers and receiving services from aviation undertakings

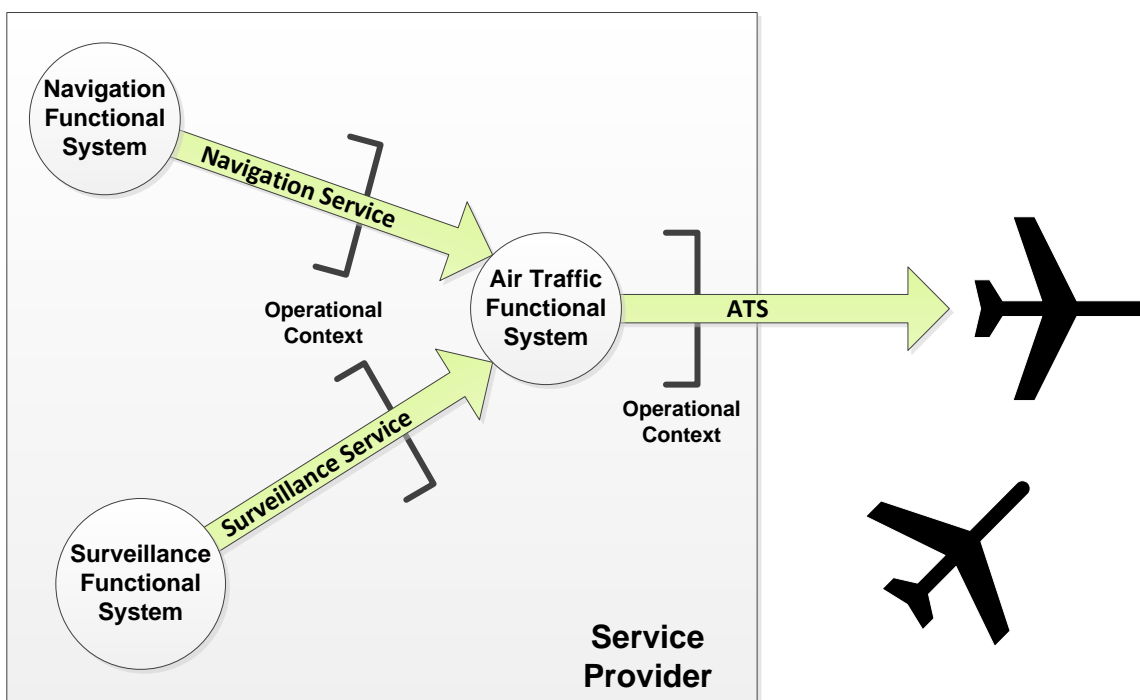
<sup>23</sup> It also receives a service from an aviation undertaking and delivers a service to an aviation undertaking.

- (3) A service provider provides different types of services<sup>24</sup>, then combines them into another type of service and delivers it to another service provider.



**Figure 8: Service provider with multiple (internal) functional systems delivering a service to a service provider and receiving a service from a service provider**

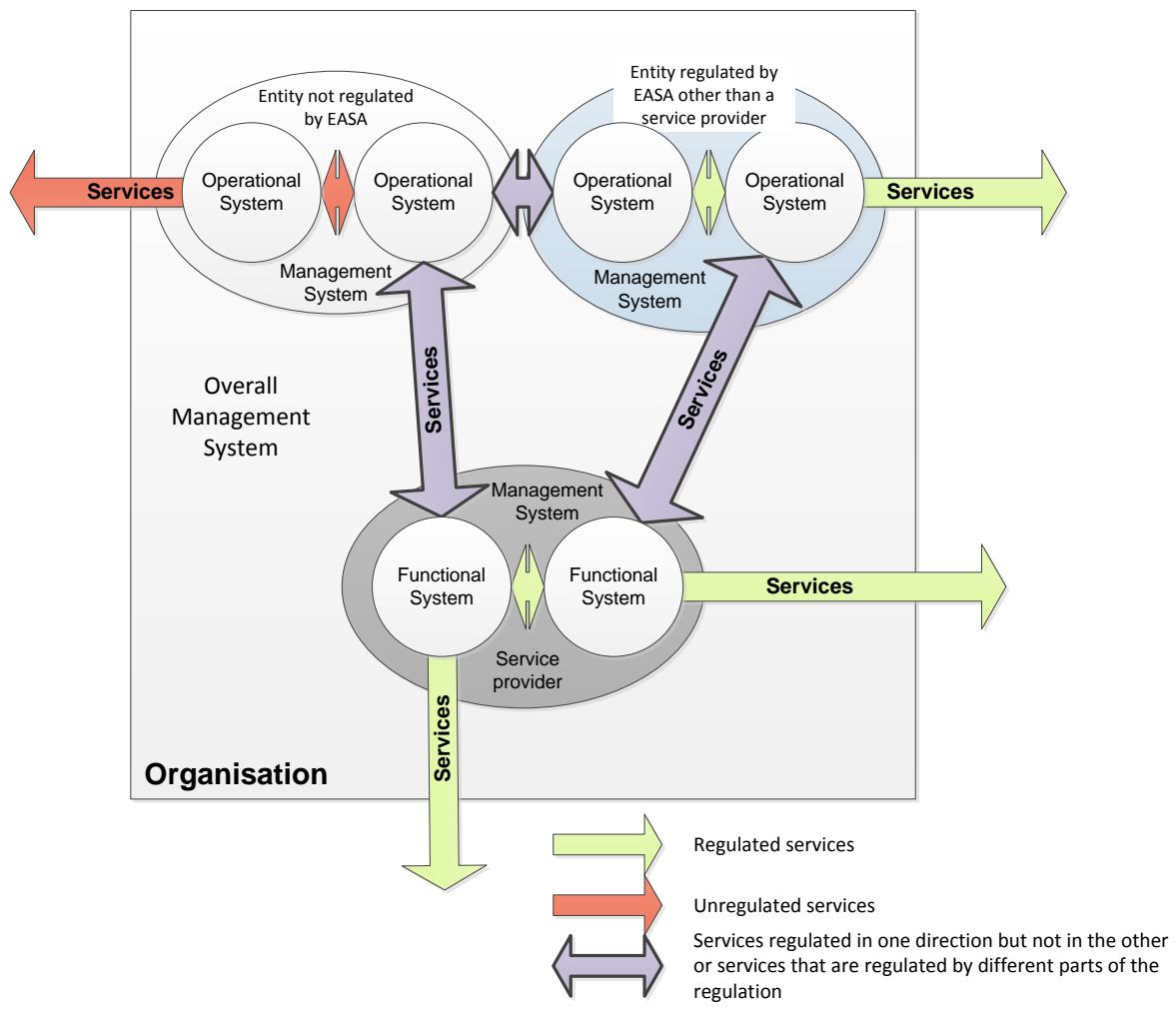
- (4) A service provider combines internal services and delivers air traffic service to aircraft.



**Figure 9: Service provider with multiple functional systems delivering a service**

<sup>24</sup> One of the services (that from FS#3) uses the services of an external organisation (Provider B) in order to create its own service.

- (g) The service provider is free to choose its management structure, provided it can show, during certification, that its management system complies with this Regulation. It is only the management system and the ATM/ANS services it delivers that are certified. Consequently, a certificate should indicate, amongst other things, the ATM/ANS services provided by the organisation or person and the scope of those services, as the service provider may only provide partial services.
- (h) An organisation may deliver services other than ATM/ANS services. In these cases, the internal structure does matter. Certification against Annex Vb(2) to Regulation (EC) No 216/2008 can only relate to those parts of the organisation that deliver ATM/ANS services, of which there may be more than one in an organisation and these may function independently of each other. Consequently, these parts should be identified by the organisation and separated in such a way that they can be managed independently of the other non-ATM/ANS parts of the organisation. A general structure for such organisations is shown below:



**Figure 10: Management system of an organisation with unregulated and regulated services, where only part of the regulated services are covered by this regulation.**

- (i) It should be noted that if the organisation chooses to have several management systems, they need to be coordinated by the overall management system. The relationship between this overall management system and the management systems of the service providers should be such that it

can be shown that the service providers' management systems comply with Regulation (EC) No 216/2008 and its Implementing Regulations.

- (j) In an organisation that also delivers other services apart from ATM/ANS services, there still may be some services that are delivered by non-ATM/ANS parts of the organisation to service providers and vice versa. In these cases, the services delivered by the non-service providers to the ATM/ANS parts of the organisation are out of the scope of Annex Vb(2) to Regulation (EC) No 216/2008, whereas the services delivered by the service provider to non-ATM/ANS parts of the organisation do fall within the scope of Annex Vb(2) to Regulation No (EC) 216/2008. Clearly, services interchanged by service providers and other non-ATM/ANS parts of the organisation that fall within the scope of Regulation (EC) No 216/2008 (shown on the diagram as an 'entity other than a service provider regulated by EASA') have to comply with that Regulation.

## 2.2. CHANGES TO FUNCTIONAL SYSTEMS

### 2.2.1. Change to functional system and its assessment

- (a) The purpose of this guidance material is to describe the circumstances that may result following a need to change the functional system and to describe the relationship between the nature of the change and its cause. Furthermore, this guidance gives a general description of the assessment of changes.
- (b) The nature of change. Changes proposed within the ATM/ANS context come in two forms:
- (1) A service provider, e.g. service provider B<sup>25</sup>, wishes to:
- (i) change its functional system; or
  - (ii) propose a change to the context in which its own services are delivered, e.g. airspace structure change, increase in traffic.
- (2) Somebody else wishes to modify something that may or may not require a responsive change to service provider B's functional system, i.e.:
- (i) Another service provider, e.g. service provider A, proposes a change to a service<sup>26</sup> delivered to and used by service provider B, e.g. a communication service provider that delivers communication services to an air traffic services provider.
  - (ii) An organisation that is not regulated by Regulation (EC) No 216/2008 but which delivers services to service provider B, proposes a change to one or more of these services, e.g. an electrical power supplier that provides electricity to a surveillance provider.
  - (iii) An external entity not regulated by the European Aviation Safety Agency (hereinafter referred to as the 'Agency') and not a service provider, e.g. a government agency, proposes a change to the context in which the services delivered by the service provider B's functional system operate<sup>27</sup>, e.g. the State decides to change the airspace structure.

<sup>25</sup> Here 'service provider B' means the provider delivering Service B.

<sup>26</sup> Or a change to the context shared with A.

<sup>27</sup> Changes in the operational environment, whether instigated by the service provider or not, may potentially impact on the way services delivered by the service provider behave. If they do, the functional system will need to be changed in response to the



(c) These changes may be due to foreseeable trends and technological or economic developments. This includes changes such as installation of new equipment, modification of software, introduction of new services, reduction of separation minima, airspace reclassification or redesign, introduction of new flight procedures, redesign of sectors, reorganisation of the ATS route structure, design of new runway configurations, physical changes to the layout of the runways and taxiways and changes to operational procedures.

(d) Planned changes

ATM/ANS.OR.A.045(a) states that planned changes to a service provider's functional system need to be notified to their CA. They are called 'planned changes' because at the point they are 'notified' they have not been implemented. Indeed, ATM/ANS.OR.A.045(c) does not allow the transition from a proposal to an implementation until an assessment has been conducted and an assurance case<sup>28</sup> exists that shows that the proposed change will be acceptable<sup>29</sup>. Where the CA decides to review the safety case, the proposed change cannot be implemented until the assurance case has been approved<sup>30</sup>. Thus, at the time they are approved, changes to functional systems are planned changes rather than implemented changes.

ATM/ANS.OR.A.045(a)(3) requires that a service provider, whose ATM/ANS services are used by another service provider, e.g. a communication provider providing services to an air traffic services provider, informs the user<sup>31</sup> if it proposes to make a change to its functional system. This acts as a driver for the user of its service to assess the impact of the change on the services the user provides. As a result, the user may need to change its own functional system.

(e) Drivers for changes

The following are some examples of reasons that may result in a need for the service provider to make changes to the functional system:

(1) Business-driven change — Improvements in:

- (i) working conditions/working environment;
- (ii) 'profitability';
- (iii) effectiveness; and
- (iv) efficiency.

(2) Context-driven change:

- (i) market share/growth;
- (ii) change in airspace use;
- (iii) introduction of environmental features, e.g. wind farms; and

---

'externally induced alteration' in order to 'back off' any risk introduced by the way the altered environment will behave after the change. Such changes are called context-driven changes.

<sup>28</sup> 'Assurance case' is used here to describe either a safety case or a safety support case. For a full definition of them, see Section 1.1 of this Appendix.

<sup>29</sup> Some notified changes may be withdrawn by the service provider. Clearly, in such cases, the assessment will not be completed and the assurance case will not be needed. It is unlikely that the CA will wish to review any incomplete data or arguments in such cases.

<sup>30</sup> Approval of a safety case may involve CA review of one or more safety support cases.

<sup>31</sup> 'User' here refers to another service provider or an aviation undertaking.



(iv) regulatory-driven changes.

(3) Management System (MS)-driven change:

(i) reverse a deficiency that affects safety/trustworthiness<sup>32</sup>;

(ii) reverse a degradation in safety/trustworthiness; and

(iii) improve safety, i.e. reduce the safety risk as low as is reasonably practicable.

Any resulting changes to the functional system require a safety (support) assessment.

(f) Examples of changes that may or may not need assessment

Table 1 contains some examples of changes that may require safety assessment and Table 2 contains examples of changes that may require safety support assessment. They show which parts of the functional system may be changed. Table 3 contains some examples of changes that may not require safety (support) assessment.

(g) Tactical changes

In the case of tactical changes, an assessment does not need to be carried out provided that they are inside the normal operational envelope and foreseen within the operating procedures and included in the operations manual. These tactical changes include circumstances associated with day-to-day operations that result in alternatives<sup>33</sup>, e.g. combining and splitting sectors, a change in runway configuration, the use of a different procedure to accommodate changing weather conditions or traffic patterns, activation of restricted airspace area, closures of an area due to search and rescue activities, procedures due to the presence of intruders, temporary closure of an aerodrome, procedures to handle special flights, and change of summer/winter hour.

(h) Maintenance activities

In the case of maintenance activities, where components are changed on a like-for-like basis, e.g. the replacement of a piece of hardware by another one with an identical part number (sometimes called a Line Replacement Unit (LRU)), an assessment does not need to be carried out provided that the maintenance activity has been foreseen and is covered by a maintenance procedure. A safety (support) assessment might need to be carried out if the maintenance activity leads to a discontinuity of the service.

(i) Changes described in (g) and (h) need to be covered in an assurance case, i.e. there needs to be an assurance case for the development of the operational procedures covering the tactical changes and maintenance activities. If these tactical changes or maintenance activities are new and arise because of the planned change, then they will need to be assured as part of the assurance case developed for the planned change. However, if they were in existence prior to the planned change, then they may have been assured in earlier assurance cases. It is possible that they have been in existence for a considerable time and as a result may have been accepted by the CA via another form of oversight. In this case, no assurance case will exist.

(j) Unplanned/unforeseen changes due to unforeseen urgent circumstances

<sup>32</sup> Safety impact applies to air traffic services providers. The impact on trustworthiness, which is a measure of the confidence one has in the correctness and completeness of the specification of the service, applies to all other service providers.

<sup>33</sup> While these alternatives can include large variations in operation that may last for long periods of time, they are only considered to be changes if they have not been previously approved.



There may be a need for unplanned changes to the functional system due to unforeseen circumstances, e.g. a system malfunction outside the contingency plan, volcanic ash or any other natural disasters affecting aviation in an unforeseen manner. In order to manage the risk introduced by these unforeseen circumstances, changes will need to be made to one or more functional systems. Such changes will be managed, by a Member State, through the application of Article 14(1) of Regulation (EC) No 216/2008 and will be dealt with outside the scope of this provision.





**Table 1 — Examples of changes that may require safety assessment<sup>34</sup>**

Examples of changes for air traffic services providers that may require safety assessment (and perhaps oversight), i.e. those within the scope of ATS.OR.205				
Change description	Possible reason for change	Potential changes to...		Remarks
Increase in traffic in airspace (Environmentally-triggered change)	Business-driven: e.g. management’s desire to increase market share by seeking an increase in the level of traffic handled	People	Training for new procedures and equipment Increase in personnel Working hours/shift patterns (fatigue and the associated increased risk of human errors)	The change is a deliberate attempt by the air traffic services provider to increase throughput. Daily fluctuations in traffic are not considered to be a change, neither is an increase in traffic that is already covered in the organisation’s certification or a previous change safety case. The change is actually a change in the environment of operation that would require a change in the functional system in order to make the operation acceptably safe. If changes are required to the surveillance or
		Procedures	New or changed procedures to handle new services and increased traffic Changes to the ATM/ANS organisation for delivering services	

<sup>34</sup> The table is written from the perspective of an air traffic services provider. However, in many places changes in equipment could refer to another service provider’s equipment, which could be linked with the air traffic services providers functional system via a service, e.g. surveillance and communications equipment could be replaced by surveillance and communications services respectively. In such cases, safety support assessments would have to be produced for these services and the change is a Multi-Actor Change.



Examples of changes for air traffic services providers that may require safety assessment (and perhaps oversight), i.e. those within the scope of ATS.OR.205				
Change description	Possible reason for change	Potential changes to...		Remarks
		Equipment	Possibly improved surveillance, communication and/or other systems, e.g. Air Traffic Controller (ATCO) decision support tools  Changes to the display of operational data to controllers at the point of service delivery  Changes to communications systems (architecture, etc.) used for the delivery of air traffic services	communications systems already present, the changes may involve the operational use of new or modified information that is already within the current system. Such use could involve an architectural change to make the information available to the changed components.
		Architecture <sup>35</sup>	Possibly, if the surveillance and communication systems change, it may require changes in the interfaces with equipment already present.	
		Environment	Increase in traffic  Airspace change	

<sup>35</sup> This refers to an organisational change to the operational system, i.e. a change to the architecture of the functional system — the way the system interacts. It does not refer to the ‘organisation’, i.e. the management of the company, which is not relevant for this provision and so is not considered.



Examples of changes for air traffic services providers that may require safety assessment (and perhaps oversight), i.e. those within the scope of ATS.OR.205				
Change description	Possible reason for change	Potential changes to...		Remarks
Changed communication system (gr/ac, gr/gr) (Functional system change)	Business-driven: e.g. obsolescence (efficiency), desire to increase market share SMS-driven: e.g. 'alarp', operational deficiencies	People	Possibly training for new equipment interface Training for technical personnel	This is not intended to include the like-for-like replacement of a piece of equipment. However, it does include the replacement of a component with a similar but not identical one, i.e. a component having similar functionality but whose design is different (including different software) as demonstrated by having a different part number. It could also include the introduction of new technology to improve the information exchange between aircraft and air traffic services, e.g. ADIRS. This may be for safety reasons or because the business wishes to introduce new services. However, the example given here deals with a simple replacement and is not intended to imply that the current operational service is altered.
		Procedures	Change to maintenance procedures	
		Equipment	New equipment	
		Architecture	A change in the equipment, e.g. the use of new interfaces, or a change in services. For example, introduction of gr/ac communications would alter the architecture.	
		Environment	Possibly the re-siting of aerials	
Introduction of new surveillance facility (Functional system)	Business-driven: e.g. desire to increase market share	People	Training on new procedures and equipment New or changed technical personnel	This example is the introduction of a new form of surveillance rather than a change to pre-existing surveillance equipment.



Examples of changes for air traffic services providers that may require safety assessment (and perhaps oversight), i.e. those within the scope of ATS.OR.205				
Change description	Possible reason for change	Potential changes to...		Remarks
change)	SMS-driven: e.g. 'alarp', operational deficiencies	Procedures	Procedures changed to include the use of new forms of surveillance Change to maintenance procedures	This may be a 'leading change', i.e. a change in the surveillance system as a prelude to making a change in the services offered in order to increase throughput.  It could also be a change to improve the quality of surveillance material in order to make the system safer or to correct recently identified operational deficiencies.
		Equipment	New equipment and possibly new or changed sensors	
		Architecture	Integration of the new surveillance with rest of the system	
		Environment	Possibly siting of new sensors or re-siting of current sensors in the external environment	
Changed surveillance facility (Functional system change)	Business driven: e.g. obsolescence (efficiency), desire to increase market share  SMS driven: e.g. 'alarp', operational deficiencies	People	Possibly training for new equipment interface Training for technical personnel	This is not intended to include the like-for-like replacement of a piece of equipment. However, it does include the replacement of a component with a similar, but not identical one, i.e. a component having similar functionality but whose design is different (including different software) as demonstrated by having a different part number.
		Procedures	Change to maintenance procedures	
		Equipment	New equipment	
		Architecture	Unlikely	



Examples of changes for air traffic services providers that may require safety assessment (and perhaps oversight), i.e. those within the scope of ATS.OR.205				
Change description	Possible reason for change	Potential changes to...		Remarks
		Environment	Possibly the re-siting of aerials/sensors	It could also include the introduction of new technology to improve the information exchange between aircraft and air traffic services, e.g. SSR. This may be for safety reasons or because the business wishes to introduce new services. However, the example given here deals with a simple replacement and is not intended to imply that the current operational service is altered.
Airspace re-organisation (Class E – A, Mil – Civil, Shape of sectors)  (Environmentally-triggered or Functional system change)	Environmentally-driven: strategic state initiative	People	Possibly additional operational personnel Training on new procedures and equipment Possibly additional technical personnel Training for technical personnel	This change is driven by the State and is probably due to a strategic review of national airspace use.  The air traffic services provider cannot ignore it and, therefore, it is an environmental change that may require a responsive change to the functional system.  If the change of airspace type makes the airspace more restrictive, e.g. airspace classes C to A, then there will be a considerable change to the operational procedures and the skills required of operational personnel. It may also
		Procedures	Change to or the creation of procedures (operational & maintenance)	
		Equipment	Possibly to improve surveillance/communications if change of airspace classification.	



Examples of changes for air traffic services providers that may require safety assessment (and perhaps oversight), i.e. those within the scope of ATS.OR.205				
Change description	Possible reason for change	Potential changes to...		Remarks
		Architecture	Likely if procedures call for the use of new/changed information.	be necessary to improve the surveillance and communication facilities in order to meet the demands of the new classification, in which case technical personnel and maintenance procedures will also change.  Such a change will, in all likelihood, alter the way that information is used and distributed in the system, thus, necessitating a change in organisation.  Both a change in airspace classification and a change in sector shape will have to be promulgated in the AIP.
		Environment	Possible change to sector shape	
Airspace re-organisation (Class E – A, Mil – Civil, Shape of sectors)  (Environmentally-triggered or Functional system change)	Business-driven: e.g. desire to increase market share, desire to increase efficiency  SMS-driven: e.g. ‘alarp’, operational deficiencies	People	Possibly additional operational personnel  Training on new procedures and equipment  Possibly additional technical personnel.  Training for technical personnel	In this case, the change is driven by the desire to improve the business. It is, therefore, likely that the drive will be for more traffic or improvements in effectiveness or efficiency. Consequently, there may be a considerable change to the operational procedures and the skills required of operational personnel. It is also likely that the business will wish to improve the surveillance and communication facilities in
		Procedures	Change to or the creation of procedures (operational & maintenance)	



Examples of changes for air traffic services providers that may require safety assessment (and perhaps oversight), i.e. those within the scope of ATS.OR.205				
Change description	Possible reason for change	Potential changes to...		Remarks
		Equipment	Likely in order to improve surveillance/communications	order to facilitate the changes it desires in its operations, in which case technical personnel and maintenance procedures will also change.  Such a change will, in all likelihood, alter the way that information is used and distributed in the system, thus necessitating a change in organisation.  The desire for efficiency may lead to a reorganisation of the airspace, e.g. changed shape or temporal/circumstantial manipulation of several sectors.  Both a change in airspace classification and a change in sector shape/organisation will have to be promulgated in the AIP.
		Architecture	Likely if procedures call for the use of new/changed information	
		Environment	Possible change to sector shape/organisation	
VFR pilots obliged to carry transponders below TMA (outside ANSP controlled airspace)	Environmentally-driven: strategic State initiative, European initiative	People	Training to recognise VFR aircraft moving towards infringement with controlled airspace	This change has a safety objective and is driven by regulation. The objective is to make VFR aircraft more easily seen and, thus, avoid conflict with controlled traffic caused by their invisibility, primarily to providers of air traffic
		Procedures	Possibly, due to different way of recognising and reacting to VFR aircraft	



Examples of changes for air traffic services providers that may require safety assessment (and perhaps oversight), i.e. those within the scope of ATS.OR.205				
Change description	Possible reason for change	Potential changes to...		Remarks
(Environmentally-triggered change)		Equipment	Possibly if the responses from Visual Flight Rules (VFR) saturate the air traffic services provider's Secondary Surveillance Radar (SSR).	services. The air traffic services providers cannot ignore it and, therefore, it is an environmental change that may require a responsive change to the functional system. This may necessitate retraining operational personnel and changing their procedures in order to accommodate the new form of surveillance for VFR aircraft. It may also necessitate changes to the SSR to accommodate the increase in responses due to VFR aircraft close by.
		Architecture	Unlikely	
		Environment	Increase in SSR traffic due to VFR aircraft	
Wind farm (Environmentally-triggered change)	Environmentally-driven: local/State initiative  Business-driven, e.g. desire to improve efficiency by generating their own electricity	People	Unlikely unless procedures change dramatically	Wind farms change the electromagnetic environment, the visible environment and the physical environment (by generating turbulence). Depending on their relationship to the controlled airspace and operation personnel, changes may vary from simply installing filters in surveillance and/or communications equipment to re-siting runways (so aircraft avoid turbulent areas), re-siting
		Procedures	Change to accommodate loss of surveillance information and likely change in flight paths	
		Equipment	To mask the interference effects of the wind farm	





Examples of changes for air traffic services providers that may require safety assessment (and perhaps oversight), i.e. those within the scope of ATS.OR.205				
Change description	Possible reason for change	Potential changes to...		Remarks
		Architecture	Unlikely	operational personnel (so their line of sight is not affected and they are not affected by flicker) and re-siting communication aerials/sensors (so as to avoid or minimise the interference effects).  Whilst wind farms are a particular example, any object that, while not placed on the aerodrome or whose placement is not a result of a decision by a provider of ATM/ANS, could still potentially affect the operation of the provider of ATM/ANS, needs to be assessed for its impact on safety and if necessary trigger a change to the functional system.
		Environment	Re-siting of aerials, changes to lines of sight for ATCOs, reconfiguration of runways	
New missed approach procedure (Functional system change)	Business-driven: e.g. desire to increase efficiency, desire to increase effectiveness  SMS-driven: e.g. 'alarp', operational deficiencies	People	Training on new procedure	
		Procedures	New procedure	
		Equipment	Unlikely	
		Architecture	Unlikely	
		Environment	Unlikely	



Examples of changes for air traffic services providers that may require safety assessment (and perhaps oversight), i.e. those within the scope of ATS.OR.205				
Change description	Possible reason for change	Potential changes to...		Remarks
Removal of assistant position (tasks go to ATCO and/or automation) (Functional system change)	Business-driven: e.g. desire to increase efficiency	People	Reduction in operational personnel Training for new role, possibly different personnel. Possibly additional technical personnel Training for technical personnel	In order for the ATCO to take over the role of the assistant, then it is likely that the information used by the assistant will have to be presented to the ATCO. Moreover, in order to avoid overload, the information used by the assistant and the information used by the ATCO will have to be presented in a different, more user-friendly, form. It may also be necessary to provide additional automation to perform some assistant’s tasks or additional safety nets to accommodate the loss of the ‘second pair of eyes’. This certainly implies changes to the equipment at the ATCO’s working position and very probably implies changes to the functions providing information to those working positions.
		Procedures	Change to operational and maintenance procedures	
		Equipment	Change to operator interface likely to change the functions for the manipulation and visibility of surveillance and communications information/management Possibly the addition of safety nets	



Examples of changes for air traffic services providers that may require safety assessment (and perhaps oversight), i.e. those within the scope of ATS.OR.205				
Change description	Possible reason for change	Potential changes to...		Remarks
		Architecture	Removal of assistant position and likely changes to the way information is managed and distributed within the system.  Redistribution of function/responsibility between human-automation	
		Environment	Possible change to sector shape/organisation to limit ATCO workload	
Integration of automatic meteorological information, e.g. METAR, SIGMET (Environmentally-	The provider of MET services wishes to improve its efficiency or seeks a larger share of the market	People	Possibly training if operational personnel were used to transform MET data for operational use  Possibly training if MET data will now be displayed in a different form  Training for technical personnel	Depending on the form and content of the data supplied by the provider of MET services currently, the air traffic services provider may simply have to change the way the equipment manipulates and displays the data. However, it may also be able to reduce the need for human intervention in transforming the data



Examples of changes for air traffic services providers that may require safety assessment (and perhaps oversight), i.e. those within the scope of ATS.OR.205				
Change description	Possible reason for change	Potential changes to...		Remarks
triggered or Functional system change)		Procedures	Possibly change of procedures if MET data cannot be transformed automatically and displayed in the current form  Change to maintenance procedures	so that it can be used directly by the ATCO (or transmitted to the aircraft). If it chooses to do the latter, then procedures will have to be changed and, consequently, operational staff re-trained.
		Equipment	Possibly new or changed equipment to receive the data in its new form and modify/distribute it to operational personnel	
		Architecture	Changed interface with the provider of MET services	
		Environment	Unlikely	
Integration of automatic meteorological information, e.g. METAR, SIGMET	Business-driven: e.g. desire to increase efficiency  SMS-driven: e.g. 'alarp', operational	People	Reduction in personnel used to transform MET data for operational use  Likely training to accommodate changes in operational use/display of MET data  Training for technical personnel.	The desire to improve efficiency would, in all probability, lead to an increase in automation, i.e. the automatic transformation and display of MET data in a form more easily used by the ATCO or aircraft.



Examples of changes for air traffic services providers that may require safety assessment (and perhaps oversight), i.e. those within the scope of ATS.OR.205				
Change description	Possible reason for change	Potential changes to...		Remarks
(Environmentally-triggered or Functional system change)	deficiencies	Procedures	Likely change of procedures to accommodate automatic transformation and display of MET data  Change to maintenance procedures	The business driver would be a reduction in the number of staff used to transform and communicate MET data.  This may also be an appropriate solution to an operational deficiency if it is related to the manual transformation or communication of MET data.
		Equipment	Likely new or changed equipment to receive the data in its new form and modify/distribute it to operational personnel	
		Architecture	Changed interface with the provider of MET services	
		Environment	Unlikely	
Change to crosswind limits (Environmentally-triggered or Functional system change)	Environmentally-driven: discovery that the aircraft type manual is wrong  SMS-driven: e.g. safety is worsening	People	Unlikely	A reclassification of the aircraft type for crosswind manoeuvres probably does not necessitate retraining of operational personnel. Notification and awareness may be sufficient.  However, a change to the crosswind classification of many aircraft, which may be
		Procedures	Re-categorisation of aircraft type for crosswind manoeuvres	
		Equipment	Unlikely	
		Architecture	Unlikely	



Examples of changes for air traffic services providers that may require safety assessment (and perhaps oversight), i.e. those within the scope of ATS.OR.205				
Change description	Possible reason for change	Potential changes to...		Remarks
		Environment	Different distribution of aircraft in crosswinds	due to the observation that safety is worsening, may result in the need for more extensive changes to the procedures and, consequently, the retraining of operational personnel.
Change to crosswind limits (Environmentally-triggered or Functional system change)	Business-driven: e.g. desire to increase market share	People	Possibly additional operational personnel Training on new procedures and equipment Possibly additional technical personnel Training for technical personnel	Larger aircraft can usually manoeuvre safely in higher crosswinds than lighter aircraft. Therefore, this business-driven change is to allow the aerodrome operator to handle larger aircraft, presumably because the organisation wishes to increase passenger throughput.  Consequently, the change to the functional system is related to the change in aircraft types and the number of them handled by the aerodrome operator, and is, therefore, much more extensive than the change described above.
		Procedures	Change to or the creation of procedures (operational & maintenance)	
		Equipment	Likely in order to improve surveillance/communications due to increase in traffic	
		Architecture	Likely if procedures call for the use of new/changed information	



Examples of changes for air traffic services providers that may require safety assessment (and perhaps oversight), i.e. those within the scope of ATS.OR.205				
Change description	Possible reason for change	Potential changes to...		Remarks
		Environment	Heavier and possibly many more aircraft in the environment	

Table 2 — Examples of changes that may require safety support assessment<sup>363738</sup>

Examples of changes for service providers other than air traffic services providers that may require safety support assessment (and perhaps oversight), i.e. those within the scope of ATM/ANS.OR.C.005				
Change description	Possible reason for change	Potential changes to...		Remarks <sup>39</sup>
Introduction of a new tool for issuing	Business-driven: e.g. desire to increase	People	Training for new procedures and equipment	If the service does not change, then there is no need for the users of the service to make any

<sup>36</sup> The table is written from the perspective of a service provider other than an air traffic services provider. However, in many places these changes services with be dealt with as a multi-actor change.

<sup>37</sup> Safety assessments are only necessary if the air traffic services provider is using the changed service.

<sup>38</sup> ‘Safety assessment’ is used here within the context of the ATM/ANS IR. It is not intended to mean a general form of safety assessment such as would be performed by others, e.g. pilots prior to flight.

<sup>39</sup> A safety support assessment is needed in all cases except where noted.



Examples of changes for service providers other than air traffic services providers that may require safety support assessment (and perhaps oversight), i.e. those within the scope of ATM/ANS.OR.C.005				
Change description	Possible reason for change	Potential changes to...		Remarks <sup>39</sup>
Notice To Airmen (NOTAM)	efficiency	Procedures	New or changed procedures to handle the new tool  Changes to the AIS organisation for delivering services	assessment of that change. If the service changes, e.g. the content and format of the NOTAM change, then the NOTAM users may need to make an assessment of the impact of these changes on them. The change then becomes a multi-actor change.
		Equipment	Likely changes in software and also in hardware	
Changes on the Transmissometer providing runway visual range information	Business-driven: e.g. desire to reduce maintenance costs by changing the units by others with longer MTBFs	People	Training for new procedures and equipment, where needed	The proposed change may not change anything in the information contained in the METARs and will not, therefore, affect the air traffic services provider or the airspace users. However, if there would be any impact in the information provided in the METARs or in the way and time they are distributed, the change may affect the air traffic services provider and/or the airspace user and needs to be treated as a multi-actor change
		Procedures	New or changed procedures to maintain the new units	
		Equipment	Changes of units	
Introduction into service (or modification) of an ILS CATIII on a controlled	Business-driven: e.g. desire to improve availability of services.	People	Training for new procedures and equipment, where needed	The safety support assessment may need to address the quality and the way that the ILS signal behaves, installation and maintenance of the ILS, definition of the critical areas, etc.
		Procedures	New or changed procedures to maintain the new units	





Examples of changes for service providers other than air traffic services providers that may require safety support assessment (and perhaps oversight), i.e. those within the scope of ATM/ANS.OR.C.005				
Change description	Possible reason for change	Potential changes to...		Remarks <sup>39</sup>
aerodrome		Equipment	Changes of units	A safety assessment may be needed to address the impact on the air traffic services provider, the definition of LVP in the OPS manual, the training of the ATCOs.
Introduction into service (or modification) of a (VHF Omnidirectional Range) VOR on an uncontrolled aerodrome (used only for instrument approach)	Business-driven: e.g. desire to improve availability of services.	People	Training for new procedures and equipment, where needed	
		Procedures	New or changed procedures to maintain the new units	
		Equipment	Changes of units	
New software release for mitigating the ionospheric perturbation on the EGNOS Safety of Life service	SMS-driven (Multi-Actor change): e.g. 'alarp', operational deficiencies	People	Training for maintenance of new equipment, where needed	A safety assessment may be needed to address the impact on the air traffic services (and in particular when the quality of the Safety of Life service is degraded)
		Procedures	New or changed procedures to maintain the new units	
		Equipment	Changes of units	



Examples of changes for service providers other than air traffic services providers that may require safety support assessment (and perhaps oversight), i.e. those within the scope of ATM/ANS.OR.C.005				
Change description	Possible reason for change	Potential changes to...		Remarks <sup>39</sup>
Replacement of a satellite for the broadcast of the EGNOS Safety of Life service (in order to have a more robust Signal In Space)	SMS-driven (Multi-Actor change): e.g. 'alarp', operational deficiencies  Business-driven: e.g. desire to reduce maintenance costs by changing the units by others with longer MTBFs	People	Training for maintenance of new equipment, where needed	A safety assessment may be needed to address the impact on the air traffic services (and in particular when the quality of the Safety of Life service is degraded)
		Procedures	New or changed procedures to maintain the new units	
		Equipment	Changes of units	
Increase/decrease of the span of the EGNOS Safety of Life service area	Business-driven: e.g. desire to improve availability of services.  SMS-driven (Multi-Actor change): e.g. 'alarp', operational improvement	People	Training for new procedures and equipment, where needed	A safety assessment will be needed to address the impact on the air traffic services
		Procedures	New or changed procedures to maintain the new units	
		Equipment	Changes of units	
New radio and/or telephone system for	Business-driven: e.g. desire to improve	People	Training for new procedures and equipment, where needed	A safety assessment will be needed to address the impact on the air traffic services



Examples of changes for service providers other than air traffic services providers that may require safety support assessment (and perhaps oversight), i.e. those within the scope of ATM/ANS.OR.C.005				
Change description	Possible reason for change	Potential changes to...		Remarks <sup>39</sup>
any entity providing air traffic control services	availability of services.	Procedures	New or changed procedures to maintain the new units	
		Equipment	Changes of units	
Introduction of datalink services	Business-driven: e.g. desire to improve availability of services.	People	Training for new procedures and equipment, where needed	A safety assessment will be needed to address the impact on the air traffic services
		Procedures	New or changed procedures to maintain the new units	
		Equipment	Changes of units	
Modification of the type of emission/reception aerals/equipment with no change in the frequencies used by the air traffic services provider and no degradation of the coverage	Business-driven: e.g. desire to reduce maintenance costs by changing the units by others with longer Mean Time Between Failures (MTBFs)	People	Training for maintenance of new equipment, where needed	A safety assessment should not be needed as there should be no impact on the air traffic services
		Procedures	New or changed procedures to maintain the new units	
		Equipment	Changes of units	



Examples of changes for service providers other than air traffic services providers that may require safety support assessment (and perhaps oversight), i.e. those within the scope of ATM/ANS.OR.C.005				
Change description	Possible reason for change	Potential changes to...		Remarks <sup>39</sup>
Evolution of a Mode A/C radar into a Mode S radar	Business-driven: e.g. desire to improve availability of services.	People	Training for new procedures and equipment, where needed	A safety assessment will be needed to address the impact on the air traffic services
		Procedures	New or changed procedures to maintain the new units	
		Equipment	Changes of units	
Replacement of the radar tracking and monitoring software system	Business-driven: e.g. desire to improve availability of services.	People	Training for new procedures and equipment, where needed	A safety assessment will be needed to address the impact on the air traffic services except where the ATCO Human-Machine Interface (HMI) and the way that the tracking system behaves are not impacted.
		Procedures	New or changed procedures to maintain the new units	
		Equipment	Changes of units	
Setup of ADS-B in a non-radar area	Business-driven: e.g. desire to improve availability of services.	People	Training for new procedures and equipment, where needed	A safety assessment will be needed to address the impact on the air traffic services.
		Procedures	New or changed procedures to maintain the new units	
		Equipment	Changes of units	



Examples of changes for service providers other than air traffic services providers that may require safety support assessment (and perhaps oversight), i.e. those within the scope of ATM/ANS.OR.C.005				
Change description	Possible reason for change	Potential changes to...		Remarks <sup>39</sup>
Replacement of visibility metres by new ones of a different brand but that behave in the same way	Business-driven: e.g. desire to reduce maintenance costs by changing the units by others with longer MTBFs	People	Training for maintenance of new equipment, where needed	A safety assessment should not be needed as there should be no impact on the air traffic services.
		Procedures	New or changed procedures to maintain the new units	
		Equipment	Changes of units	
Modification of the tool used to produce and broadcast 'significant weather charts'	Business-driven: e.g. desire to improve availability of services.	People	Training for new procedures and equipment, where needed	A safety assessment should not be needed as there should be no impact on the air traffic services.
		Procedures	New or changed procedures to maintain the new units	
		Equipment	Changes of units	
Setup of cloud ceilometers on a controlled aerodrome	Business-driven: e.g. desire to improve availability of services.	People	Training for new procedures and equipment, where needed	A safety assessment will be needed if the cloud base height information was not available to the ATCOs before.
		Procedures	New or changed procedures to maintain the new units	
		Equipment	Changes of units	



Examples of changes for service providers other than air traffic services providers that may require safety support assessment (and perhaps oversight), i.e. those within the scope of ATM/ANS.OR.C.005				
Change description	Possible reason for change	Potential changes to...		Remarks <sup>39</sup>
Modification of the NOTAM production and publication tool	Business-driven: e.g. desire to improve availability of services.	People	Training for new procedures and equipment, where needed	A safety assessment should not be needed as there should be no impact on the air traffic services.
		Procedures	New or changed procedures to maintain the new units	
		Equipment	Changes of units	
Set-up of a new WGS84 server for Aeronautical Data Quality ADQ Implementing Rule (ADQ-IR) compliance	Business-driven: e.g. desire to improve availability of services.	People	Training for new procedures and equipment, where needed	A safety assessment should not be needed as there should be no impact on the air traffic services.
		Procedures	New or changed procedures to maintain the new units	
		Equipment	Changes of units	
Any change to the tools used to produce the Aeronautical Information Publication (AIP) —	Business-driven: e.g. desire to reduce maintenance costs or improve availability of	People	Training for new procedures and equipment, where needed	A safety assessment should not be needed as there should be no impact on the air traffic services
		Procedures	New or changed procedures to maintain the new units	



Examples of changes for service providers other than air traffic services providers that may require safety support assessment (and perhaps oversight), i.e. those within the scope of ATM/ANS.OR.C.005				
Change description	Possible reason for change	Potential changes to...		Remarks <sup>39</sup>
Aeronautical Information Circular (AIC), IAC, AIP Sup, etc. — with no change to the format and content itself	services	Equipment	Changes of units	
New version of the Collaborative Interface for Flow Management Positions (CIFLO) used by the Flight Management Position (FMP) position of an ACC and provided by the network manager	Business-driven: e.g. desire to improve availability of services.	People	Training for new procedures and equipment, where needed	A safety assessment will be needed for the use of the new version.
		Procedures	New or changed procedures to maintain the new units	
		Equipment	Changes of units	



**Table 3 — Examples of changes that may not require safety or safety support assessment**

<b>Examples of changes for service providers that may not require safety or safety support assessment, i.e. those not in the scope of ATM/ANS ATS.OR.205</b>		
<b>Change description</b>	<b>Type of change</b>	<b>Possible reason for change</b>
Organisational change	Change to organisation, not to the functional system.	Political reasons/desire to increase efficiency
Maintenance change, covered by a procedure <sup>40</sup> , where components are changed on a like-for-like basis	Planned/Regular	Preventive actions on technical components
Day-to-day operations, e.g. a change in runway direction, described in operational manuals <sup>41</sup>	Operational tactical change	Change in environment of operations, e.g. wind direction, weather, regular change associated with noise abatement
Use of alternative procedures <sup>42</sup> in response to the failure of a system/component	Operational tactical change	Failure of an operational system

<sup>40</sup> 'Covered by a procedure' includes the concept that a safety assessment has been performed on the procedure, and the maintenance action is shown to be acceptably safe. So here we are dealing with maintenance action against a pre-approved procedure.

<sup>41</sup> It is assumed that a safety or safety support assessment has already been performed on the operations manual and the change is simply dealing with the use of the procedure, not its introduction or removal.

<sup>42</sup> These are pre-approved operational and maintenance procedures that have been specifically created for use in the circumstances of the failed system/component, e.g. for a large system failure, the operational procedure will be one for reducing and limiting traffic in the airspace until normal operation can be resumed.





### 2.3. SERVICES, INFORMATION AND THE RESPONSIBILITY FOR SAFETY

- (a) This guidance material explains the difference in responsibilities for safety between an air traffic services provider and other types of service providers. It also describes the rationale behind the differences in the type of assessment each has to make, i.e. safety assessments are required from air traffic services providers while safety support assessments are required from other service providers.
- (b) In some circumstances, services provided directly to an aircraft are provided by a service provider other than an air traffic services provider, e.g. a navigation service. It has been argued that this makes the provider responsible for safety and would necessitate the production of a safety case for the service being delivered, rather than the safety support case required by this Regulation. This general guidance material explains why this is not the case by comparing the responsibilities and capabilities of a navigational service provider with those of an air traffic services provider. It then goes on to show why this example is generally applicable to all service providers other than air traffic services providers.
- (c) Figure 11 below illustrates a common scenario: A signal is provided in a manner that cannot easily be restricted to a particular volume of airspace and so there can be many users and these users may be unknown to the signal provider. The signal provides information that can be used for navigational purposes. Clearly accurate information, which is consistently available, is necessary for safety. However, accurate navigation and avoidance of other aircraft and obstacles do not rely solely on the signal providing the navigational information. Consequently, even if the signal provider did know who was using the navigational information and could prevent unauthorised use, it would still not be able to say that all users would use the information safely. Furthermore, it certainly could not in any way assure that all aircraft using the information would be safe. As a consequence, the signal provider could not write a safety case; however, it could write a safety support case. This is because the safety support case demonstrates<sup>43</sup> that the signal in space meets its specification<sup>44</sup> and that the specification (and the context in which it is valid) is available to all users.
- (d) The provision of this signal in space, transmitting navigational information, is usually called a navigational service. To call the provision of the signal in space a service seems rational as there is a system (the functional system) involved in encoding navigational information and transmitting it. The information is transferred from one entity to another and so the information transfer falls within the broad definition of a service. Even if the definition of a service is restricted so that it also requires some contract governing both the provision and the receipt of the signal to exist, then the transfer of navigational information described could still be considered a service. This is because it can be argued that such a contract exists. The provider makes the availability of the signal known to those it believes will wish to use the service. In doing so, the provider will probably indicate the range of uses foreseen, the availability of the signal and any constraints users should bear in mind. This would normally be seen as one half of the contract. The other half

<sup>43</sup> This should not be taken to mean that producing a safety support case is in any way inferior to producing a safety case. Nor should it be taken to mean that there should necessarily be any lower degree of confidence needed in a safety support case than that needed in a safety case. Demonstrating that something behaves only in accordance with its specification can be extremely challenging, but is nonetheless required.

<sup>44</sup> And that the specification is complete i.e. it does nothing else.



involves the user, who would be deemed to have accepted the conditions under which the service is offered, simply by using it.

- (e) There is a difference between the navigation service used by aircraft in uncontrolled airspace (airspace classes F and G) and the use of this navigation service within the context of the provision of air traffic services<sup>45</sup>. In both cases, the navigation service provider has only a limited knowledge of who is the end user of the service, where they are using it, what they are using it for and what other services are being provided to the user at the same time. In both cases, the navigation service provider is neither responsible for how the service is used nor the separation of aircraft that may be using the service.
- (f) The difference is in the use of the service. The air traffic services provider may be responsible for separating aircraft, depending on the airspace class, in receipt of its services within a defined airspace and 'uses'<sup>46</sup> the navigational service within that context. Other air transport users are simply responsible for using the service in order to navigate their own aircraft. This difference is not the responsibility of the navigation service provider, even though there may be different charging schemes for different uses.
- (g) The air traffic services provider knows what any particular aircraft is using the navigation service for (because it is directing its use) and what other services are being provided to the aircraft. In airspace class A, B, C, and to a lesser extent class D and E airspaces, the air traffic services provider also knows the location and intent of other aircraft in the vicinity<sup>47</sup>. This allows the air traffic services provider to form a safe, effective and efficient navigational plan, which takes all of the circumstances of the service into account e.g. the regulatory context as well as the physical context; and to provide instructions to the aircraft<sup>48</sup> receiving its service.
- (h) Even though the pilot can take independent action and so it can be said that the air traffic services provider is not in total control of the situation, the air traffic services provider is obliged to attempt to keep all aircraft in the airspace under its control separated<sup>49</sup>. This is done by requiring one or more other aircraft to alter their trajectories. Consequently, the air traffic services provider does have a view of what it takes to make the airspace safe for all users and is coordinating the use of all the services, whether the information delivered by these services is delivered directly to the service provider, directly to the aircraft or generally available within the airspace<sup>50</sup>. Certainly, the pilot does not have such a view and neither do the other service providers. Consequently, the air traffic services provider, due to its ability to coordinate all the services and its responsibility for the separation of some aircraft, can produce a safety case even though there are circumstances, within the airspace it controls but not within its control, that could lead to an accident.

<sup>45</sup> Strictly speaking, this relates to the provision of an ATCS, however it is sometimes the case that information oriented services are treated as control services by pilots, simply because the air traffic services provider has a more complete picture of the airspace and its users. The air traffic services being provided will depend on the airspace classes. Therefore, the scenario described below is a general one without going into the details of the services being provided to IFR or VFR traffic in each airspace class.

<sup>46</sup> Strictly speaking, the air traffic services rely on the use of the navigation signal by the aircraft in order to provide its service of separation.

<sup>47</sup> In class E, F and G airspaces, the air traffic services provider may know the location of most, if not all, aircraft (depending on the effectiveness of his surveillance techniques) and may also be the one best placed to make assumptions about the intent of the aircraft. So to a lesser extent the argument also holds for service provision in these classes of airspace.

<sup>48</sup> In doing so, he may need to make assumptions about the plans of some users; however, these assumptions will be based on standard practices.

<sup>49</sup> And by doing so the airspace remains safe

<sup>50</sup> 'Information generally available within the airspace' is used here in a very broad way – it includes maps, AIP, etc.



- (i) This then begs the question of who is the user of the navigational service. In the case of the pilot who uses navigational information without receiving air traffic services, then clearly the user is the pilot. However, in the case where a pilot is using the navigation information as part of air traffic services, then it is less clear. Certainly, in both cases the pilot receives the same information. However, in the latter case it is only a part of the information he receives and, indeed, where it is the only navigational information he received, it would not allow him to participate in the air traffic services being provided<sup>51</sup>. So it is probably more useful to think of the relationship as follows: the air traffic services provider is using its knowledge of the navigational service provided to the aircraft and other information available to him, in creating and communicating its own navigational plan for the whole airspace. Consequently, it is the air traffic services provider who, while not directly receiving the service, uses it as well as the pilot and in so doing has a more complete view of the safety of the airspace, in which its service is provided, than the pilot. Another way of describing the situation is that the pilot receives the information as part of a much broader service, i.e. that of separation. Figure 11 below illustrates this difference.
- (j) The case has been argued for a navigation service provider. It is equally true for all service providers. Air traffic information/data is created or used by the ATCO in order to derive the navigational plan. Primarily this data is surveillance data (so that the ATCO knows where all aircraft are), communications data (so that the ATCO can establish the intent of the aircraft and issue instructions to them), and navigational data (so that the instructions can relate global reference points, that all are aware of, to the local position of the aircraft). This data is dynamic — it changes due to the circumstances prevailing within the airspace at the time. Other semi-static and static data is used. For instance, the design of the airspace, the rules of the air and other regulations are static data. These are rather like navigational data in that everyone is aware of them and, therefore, instructions can refer to them rather than spelling out every individual detail. The data relating to the local management of air traffic flow in the airspace is semi-static and so is the range of airspace configurations. This semi static data provides the ATCO with information about the long-term intent of aircraft entering the airspace and the options available to the ATCO for the local management of the airspace.
- (k) The safety of each aircraft depends on the plan<sup>52</sup> being safe and the given instructions being carried out correctly.
- (l) It is expected that the ATCO will ‘see’ all the aircraft and sense if they are not conforming to the plan. The ATCO is then expected to re-formulate the plan and issue corrective instructions to one or more of the aircraft receiving the control service in the airspace.
- (m) It is this ‘observe, re-plan, instruct’ cycle that ensures safety. Both the plan and the instructions are created and maintained in the mind of the ATCO and this is the primary reason why it is the air traffic services provider that is responsible for assessing and assuring the safety of the service it is providing.
- (n) Other service providers i.e. Surveillance, Communications, Navigation, MET, ATFM, AIS, DAT and ASM service providers, enable the air traffic controller’s plans to be formulated and implemented. In the airspace where air traffic services are provided, they have an impact on the safety of

<sup>51</sup> Because, in this case, he would only know where he was not, where the air traffic control service wanted him or was expecting him to go.

<sup>52</sup> Which includes assumptions made by the ATCO about uncontrolled aircraft.



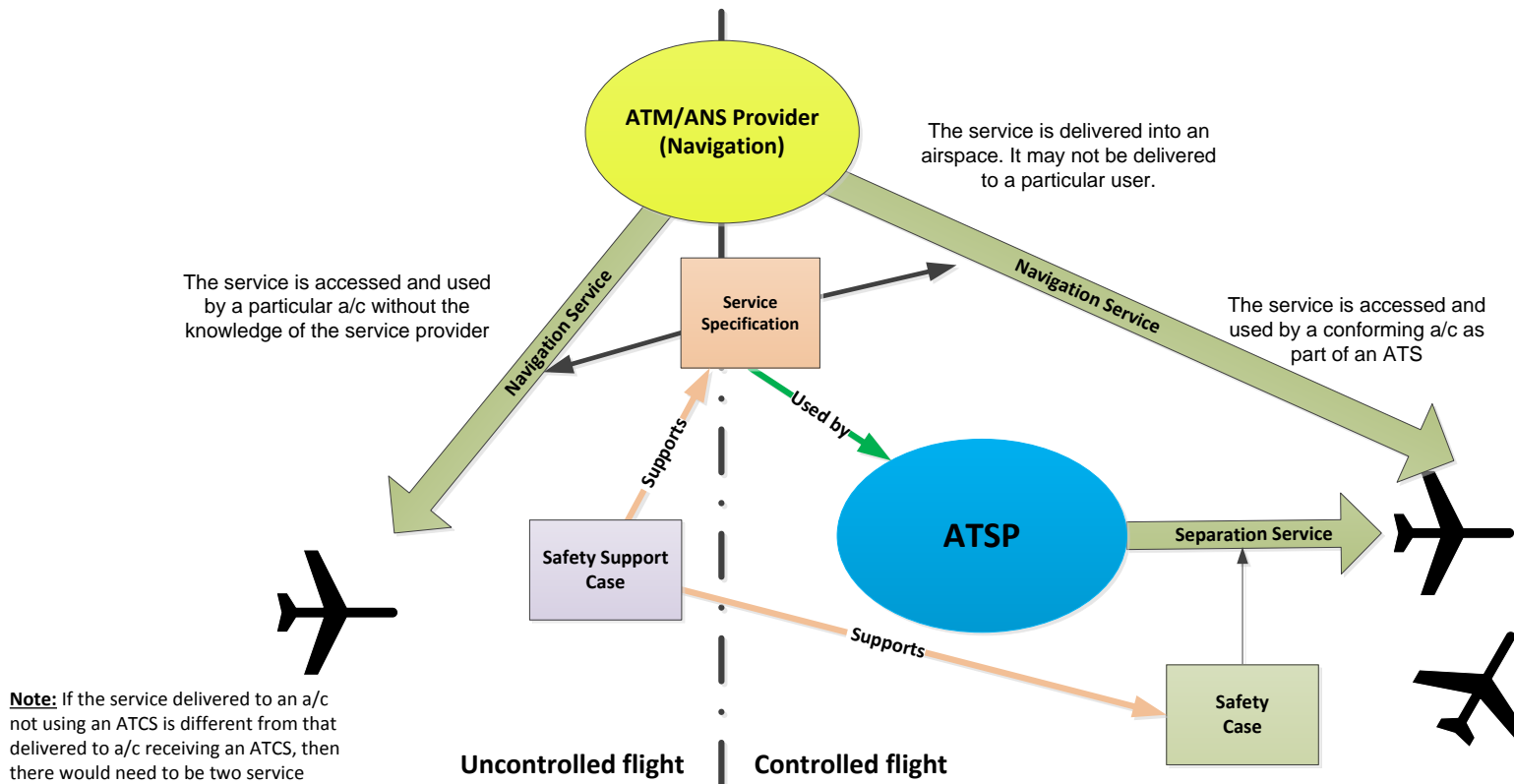
aircraft operations. If they perform in a manner anticipated by the air traffic services provider, e.g. they behave as is required by their contract<sup>53</sup> with the air traffic services provider even though that contract may be abstract, as in the case of satellite navigation services, then the navigational plan will work, as intended, and the airspace will be safe.

- (o) Some service providers are involved in the provision of air traffic services but are unregulated by the Agency e.g. telecoms companies who provide telecom services between service providers regulated by the Agency. The Agency's regulated service providers are responsible for assuring themselves that these services are fit for purpose
- (p) Consequently, these service providers are not responsible for the assessment of the safety of the air traffic services, but are responsible for the 'trustworthiness' of the services they provide to the air traffic services provider.
- (q) Summarising the above, the provider of a service may not 'control' the use of the service and, therefore, will not be placed in the best position to judge whether it will be used safely. However, while an air traffic services provider cannot be said to have absolute control over the use of any service directly supplied to an aircraft, those services are provided within the framework of a navigational plan (a plan controlling separation) for all aircraft receiving air traffic services. Within that plan, the air traffic services provider has to be aware and take care of the fact that the initial plan may not be adhered to and so will have to modify the plan in order that all aircraft remain safe. Consequently, it is only the air traffic services provider that has all information and can adequately perform a safety assessment and provide a safety case. All other service providers should only perform safety support assessments and provide safety support cases.

---

<sup>53</sup> Note that loss of information and all forms of corruption of information is expected to form part of the contracted service definition.





**Note:** If the service delivered to an a/c not using an ATCS is different from that delivered to a/c receiving an ATCS, then there would need to be two service specifications and two safety support cases, one for each service. However, there may be many common elements in each case.

Individual a/c that are not receiving an ATCS may also use the service in controlled airspace. The Nav service provider still would not be able to control who they are and may not know who they are. The service provider will not know how a particular a/c will use the service and cannot control the provision of other services to the same aircraft.

While the service provider may attempt to write a generic safety case, it is unlikely that it would have any direct relevance to the system since each a/c can be using many or few services at the same time and can be equipped to vastly different levels.

**Services, Information and Responsibility for Safety**  
 (for controlled and uncontrolled flight)

**Figure 11: Services, Information and Responsibility for Safety**



## 2.4. MULTI-ACTOR CHANGES

### 2.4.1 Multi-actor changes — General

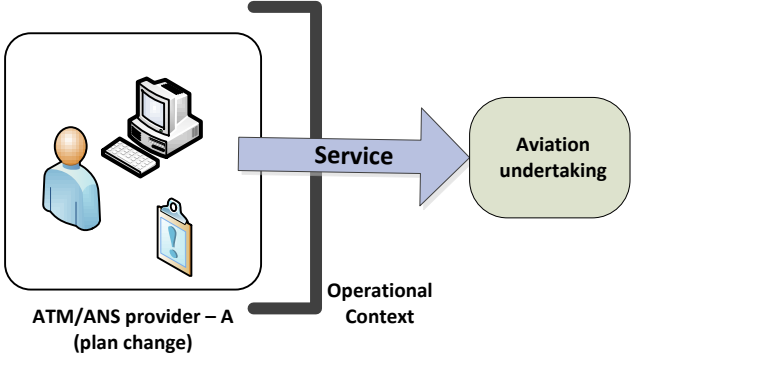
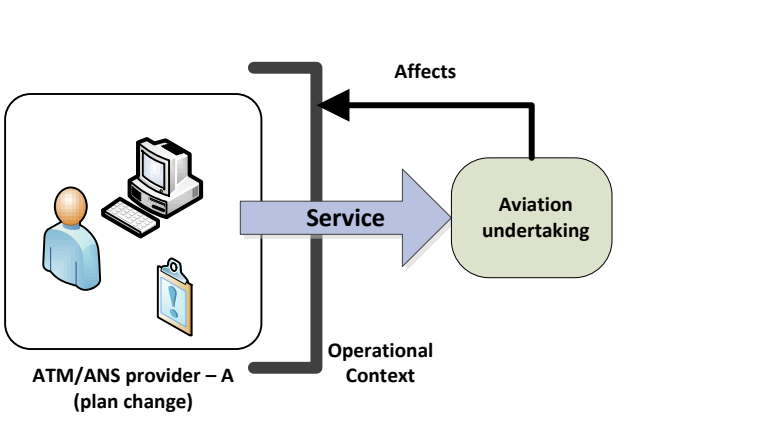
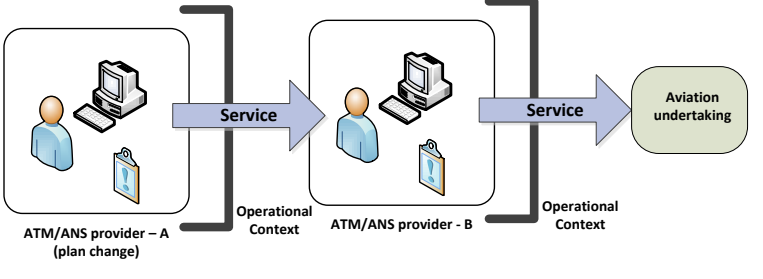
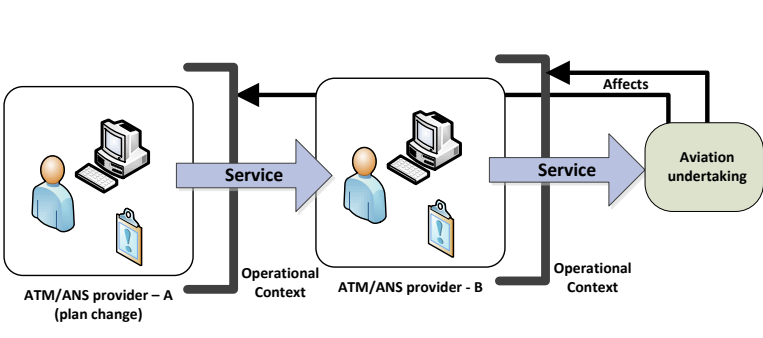
- (a) A multi-actor change is a change to a functional system proposed by a service provider that affects other service providers and/or aviation undertakings. Any change to the functional system of a service provider affects other service providers and/or aviation undertakings when:
  - (1) the proposed change may alter the service delivered to other service providers and aviation undertakings as users of that service; or
  - (2) the proposed change may alter the operational context in which the services of other service providers and aviation undertakings are delivered or in which the aviation undertakings are operating.
- (b) Multi-actor changes require coordination due to the presence of dependencies between the service provider that plans the change and other affected service providers and/or aviation undertakings.

### 2.4.2 Change affecting multiple service providers and aviation undertakings — Forms of dependencies

- (a) Dependencies can be of two forms: unidirectional dependencies and bidirectional dependencies, i.e. interdependencies.
- (b) Unidirectional dependencies always exist between a provider of a service and its users. The way the users behave depends on the properties of the service, and in that sense the behaviour of the user is dependent on the provider. There are two types of unidirectional dependencies:
  - (1) Direct: This is the dependence that exists between the provider of a service and its users when the service is delivered directly.
  - (2) Indirect: There may be indirect dependencies between a provider and the end user if there are other providers in between.
- (c) Interdependencies are bidirectional dependencies, where each stakeholder is dependent upon the other. For example, in the simplest case, where a single service provider delivers a service to a single (type) of aviation undertaking, an interdependency exists when the service provided by the service provider depends on the behaviour of the aviation undertaking. In other cases, involving several service providers and aviation undertakings, the identification of interdependencies is more complex and, therefore, it is more important to identify them in coordination as they may not be immediately obvious for the service provider proposing the change. The identification of dependencies and interdependencies is essential in determining the scope of the change and the extent of the assessment and assurance activities required.
- (d) In addition, the presence of interdependencies may suggest that the service provider proposing a change will not be able to implement it unless the affected service providers and aviation undertakings have implemented changes themselves. This may result in the need for common assumptions and risk mitigations and, therefore, the alignment of these shared assumptions and risk mitigations among those affected is paramount.



- (e) The notion of dependencies and interdependencies is depicted in Figure 12. The figures do not contain all possible situations but just the most representative ones in order to make the notion of dependencies and interdependencies clearer.

Notional Depiction	Description
	Unidirectional dependency
	Direct Interdependency (bidirectional dependency)
	Series of unidirectional dependencies <sup>54</sup>
	Indirect interdependency (example). The aviation undertaking has an indirect interdependency with service provider A. A direct interdependency between the aviation undertaking and service provider B is

<sup>54</sup> The aviation undertaking may be indirectly dependent on the service provided by service provider A.

Notional Depiction	Description
	also depicted.
<p>The diagram illustrates a notional depiction of dependencies. It features two boxes representing 'Operational Context' for 'ATM/ANS provider - A (plan change)' and 'ATM/ANS provider - B'. Each box contains icons of a person, a computer, and a clipboard. Large blue arrows labeled 'Service' point from each provider to a central icon of an aircraft. Black arrows labeled 'Affects' show a feedback loop: from the aircraft to provider A, from provider A to the aircraft, from the aircraft to provider B, and from provider B to the aircraft.</p>	<p>Indirect interdependency (example). Service provider A has an indirect interdependency with service provider B. This is because a change in service provided by A may affect the behaviour of aircraft operator (an aviation undertaking), which in turn may affect the context in which service provided by B is delivered, and, thus, may affect the context and the service of service provider A.</p>

**Figure 12: Notional depiction of examples of dependences**

- (f) When interdependencies exist, the change to the service may create new or modified interactions that affect services not apparently related to the change, e.g. a change to the form of communications, such as datalink, may increase pilot workload to the point where there is an increased number of potential conflicts for the ATCO to resolve, thus, having a negative impact on navigation. In turn, this would increase the messages between controllers and pilots, which may have an impact on the communication service. For this reason, it is important that all interactions are analysed before the change is implemented to identify those that may be altered as a result of the proposed change.
- (g) When interdependencies exist, the change to the service may cause a reaction by the CA, which in turn causes a change to the practices used in the environment, e.g. a change in the nature of an ATM/ANS service might change the regulatory context for all other air transport stakeholders, which may in turn affect the way they behave in the environment.
- (h) The apparent absence of interdependencies does not automatically imply that the change does not affect multiple actors. There may be direct and indirect unidirectional dependencies impacting on multiple service providers that require coordination. For example, a change to a functional system that affects the service used by another service provider, which in turn affects the service delivered to aircraft operators.
- (i) Trying to identify all dependencies, even in simple cases, it is more likely to be successful if carried out in a cooperative manner with all affected parties than if carried out by individual service providers. Dependencies and, above all interdependencies, can be subtle and this coordination



may help uncover them more efficiently, thus, resulting in a more successful identification of affected services and functional systems. This will result in a correct identification of the scope of the change.

### 2.4.3 Changes affecting multiple service providers and aviation undertakings — Examples

The following is a list of examples of changes affecting multiple service providers and/or undertakings, which is not necessarily complete.

- (a) Any coordinated set of changes proposed by several service providers to their functional systems, where the ultimate purpose of the change is a shared objective of all the stakeholders involved in the change. For instance, within a Functional Airspace Block (FAB) two neighbouring air traffic services providers agree to redesign completely their respective adjacent airspace to move the departure flows from two main airports (each one served by each provider) reducing interference of traffic flows, improving efficiency and increasing the throughput of both airports.
- (b) Any change to a functional system of a service provider that affects how the service behaves and has a potential impact on the service provided by a different service provider to the end user. For instance, a MET provider seeks to improve its efficiency and reduce cost by fully automating the weather observations, production of MET aeronautical reports, e.g. METARs, and its delivery to the air traffic services provider at airports. This change will have implications for the air traffic services provided at the airports because the ATCOs will have to be retrained on certain issues associated with the reports, such as implications on the accuracy of observations, interpretations of automatic observations or backup procedures to deal with sensor failures. The implication of the effects of the new report (i.e. the information, the delivery, and the new procedures) will require a safety assessment by the air traffic services provider, potentially involving the airport operator too.
- (c) Any change to a functional system of a service provider that has a potential impact on the context in which services are provided by a different service provider, even where both service providers do not share any service. For example, an air traffic services provider introduces a new approach procedure in the airspace near another air traffic services provider's airspace where initially there are no interactive procedures between the providers. This new approach procedure close to the other provider's controlled airspace may impact on the other air traffic services provider's services by, for example, increasing the number of intrusions into the other air traffic services provider's airspace. A coordinated safety assessment is required between both providers.
- (d) Any change to the functional system of an air traffic services provider that may affect exclusively the aircraft operators that use its delivered services and require coordination with aircraft operators to ensure that the service provider is able to implement the change as intended. For example, to ameliorate the noise impact of arrival approaches at a certain airport, the air traffic services provider serving the airport seeks to introduce new arrival procedures utilising continuous descent operations and, thus, avoid the conventional stair-step approaches. The envisaged continuous descent operation requires the usage of a ground automation tool that advises, via data-link, pilots and ATCOs where and when to initiate the descent in order to resolve separation conflicts while satisfying time-based metering constraints at destination. The need to evaluate the effects of the changed information on the operation of the aircraft has to be assessed by the aircraft operators. In order to implement the change, the aircraft operators need



to agree on the training of pilots and implement, if needed, changes to the on-board equipment that manage the information uplinked, so as to ensure that the change works in the way intended by the design.

- (e) Any change to the functional system of a service provider that may affect an aerodrome operator. For example, an air traffic services provider decides to balance the use of runways at a certain airport in order to balance the noise impact on the areas surrounding the airport (this may be required by local or national regulatory authorities through requirements on the air traffic services provider). The new balance may result in changing the active runway more often than the wind conditions would require. This will have an effect on the taxiing flows at the airport, and potentially an effect on runway incursions and excursions. Evaluating the effects must be coordinated with the airport operator and local airlines.

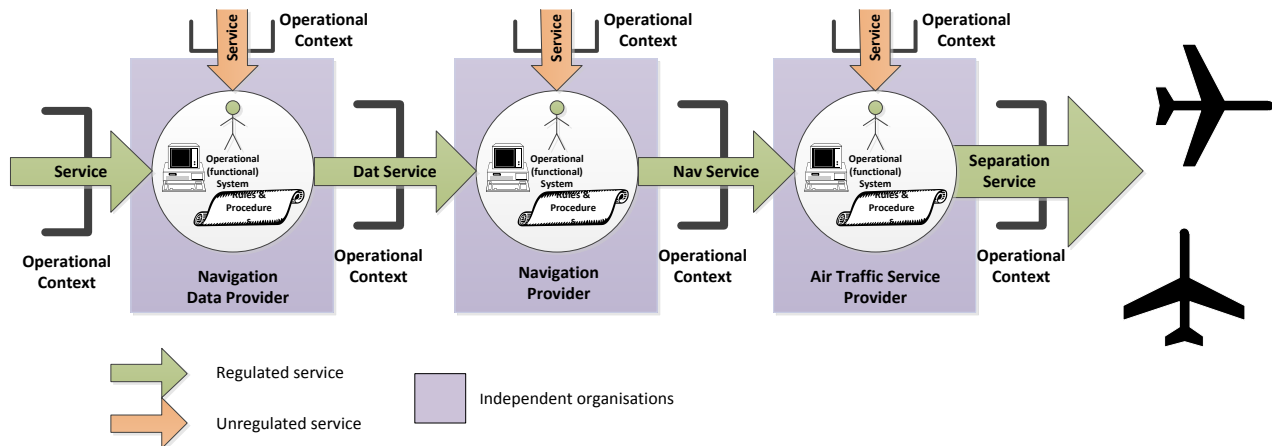
#### **2.4.4 Changes affecting multiple service providers — Multi-actor changes involving safety support assessment and assurance**

- (a) The purpose of this section is to describe multi-actor changes that involve, in addition to an air traffic services provider, at least one service provider other than an air traffic services provider changing its functional systems and, therefore, performing a safety support assessment, and the relationship between this safety support case and the associated safety case, if any, elaborated by the air traffic services provider.
- (b) Whenever a multi-actor change involves more than one service provider changing their functional system, those of them who are service providers other than air traffic services providers will produce a safety support assurance case. Service providers other than air traffic services providers, i.e. AIS, MET, CNS, ASM, ATFM and DAT, must comply with the requirements of this Regulation and make an assessment of any changes to their functional systems, but the type of assessment they are able to undertake is necessarily different from those produced by air traffic services providers. This different type of assessment has been termed a 'safety support assessment' in the rule and relates to the behaviour of services (rather than their use for flight navigation and control directly by pilots or indirectly via air traffic services providers, which is not within the responsibility of the provider making the change). This behaviour refers to such properties as function, accuracy, availability, continuity, timeliness, reliability, confidence, integrity, etc.
- (c) If a service provider, other than an air traffic services provider, provides services directly to an aircraft without involving an air traffic services provider (e.g. a navigation signal provided in uncontrolled airspace), then the provision of a safety assessment is outside the scope of this Regulation, because the safe use of the service is the responsibility of the end user, i.e. the aircraft operator or the pilot. However, a safety support assessment is required in that case to describe the behaviour of the service in the specified context.
- (d) Service providers producing a safety support assessment need to assess what impact the changes to their functional systems will have on the functionality and performance of the services they provide. This impact is defined in the specification of the changed service. The context in which this specification is valid is defined in the context specification. The result of a safety support assessment is evidence supporting the argument about the trustworthiness of the specification in



the context of use. The specification of the changed service and the context specification should be made available to any service provider or other body or person that uses the changed service.

- (e) If a service provider uses a function or service provided by another service provider, the user must assess whether any changes made to the service that it uses affects the way the ATM/ANS service it delivers behaves. This assessment<sup>55</sup> must take into account the specifications of the changed service, which are supported by the results of any associated safety support assessments.
- (f) A safety assessment or a safety support assessment can be supported by one or more safety support assessments, e.g. a chain of services (Figure 13) or a tree of services (Figure 14).

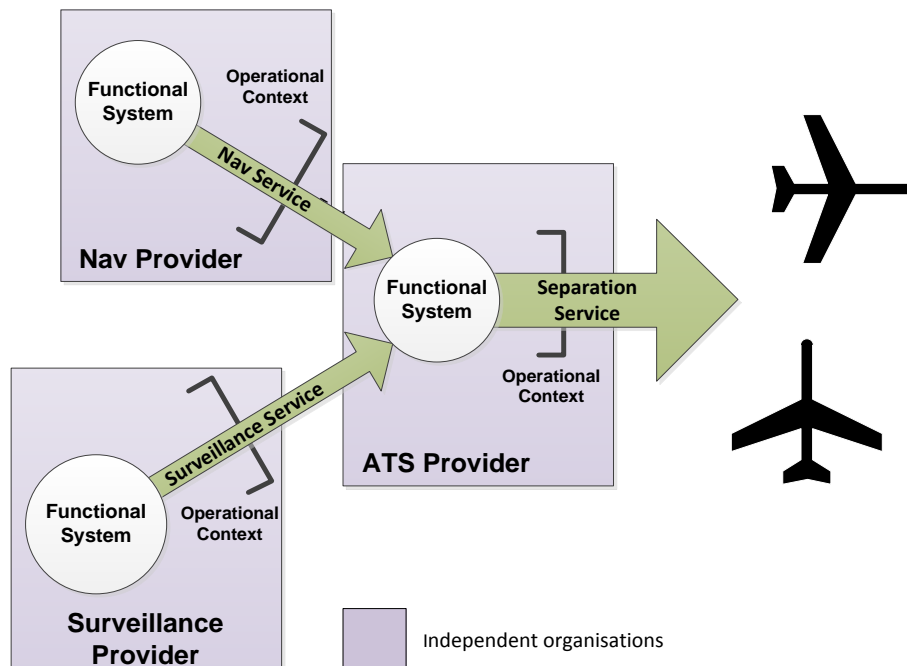


**Figure 13: Example of a chain of services**

- (g) In Figure 13 above, when the Navigation Data Provider proposes a change, it will perform a safety support assessment and develop a safety support case, which it will submit to the CA for review and approval, if required to do so. If the safety support case shows that the service provided is unchanged, then no further action is required by the service provider and the CA may review and approve the safety support case in isolation. However, if the service provided is changed, then the Navigation Data provider will supply the specifications of the changed service to the Navigation Provider as well, and the Navigation Provider must also perform a safety support assessment and submit the assurance case to its CA. If the Navigation provider's safety support case report confirms that its service is unchanged, i.e. the service specification remains valid, then no further action is required by the air traffic services provider. This is the only case where a safety support case will be produced without there being an associated safety case. However, if the service provided is changed, then the air traffic services provider uses the specifications delivered by the Navigation Provider to identify the effects of the change on its air traffic services. If there is none, then no further action is necessary. If, however there is an effect, then the air traffic services provider needs to notify the CA of the change and then decide whether a responsive change is needed to its functional system. In either case, the air traffic services provider needs to produce an assurance case. The air traffic services provider must then submit the assurance case to its CA, if required to do so. In this case, the CA will review and approve this safety case, if it finds it

<sup>55</sup> The assessment may either be a safety assessment or safety support assessment, depending on whether the service provider that uses the service is an air traffic services provider or not, respectively.

acceptable, and when necessary, it will also review and approve the other safety support cases associated with it.



**Figure 14: Example of tree of services**

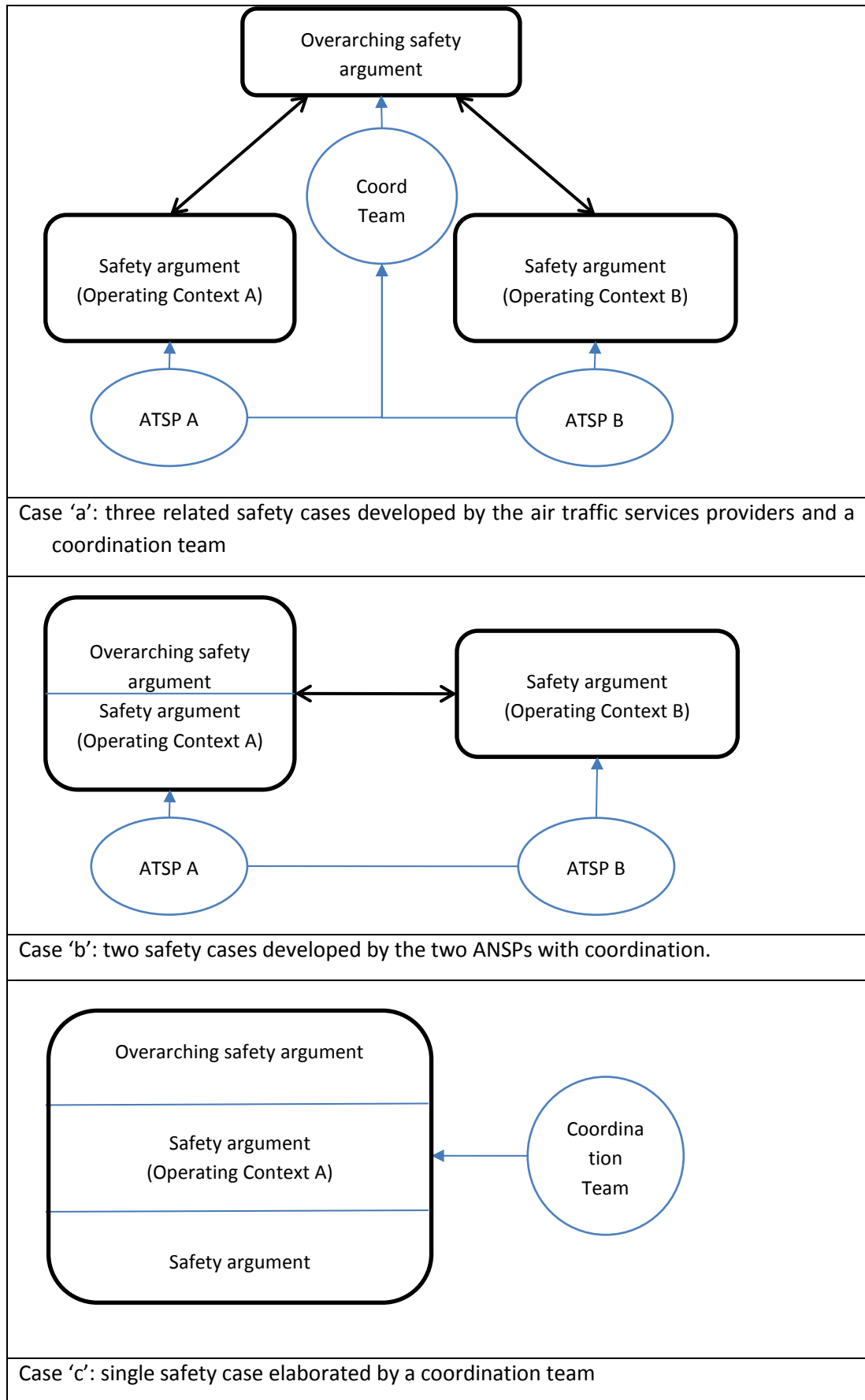
- (h) In Figure 14 above, the Surveillance provider and the Navigation provider will supply a safety support case to the CA, if required to do so. They will provide the service specifications and the context specifications to the air traffic services provider, who will take them into account in developing a change to its functional system, if necessary, and creating the safety case for the air traffic service it provides. When several safety support cases are used in a safety assessment (or another safety support assessment), the interdependencies between the different services must have been assessed.
- (i) If a safety support assessment and a safety assessment are performed in the same organisation, the safety support assessment could either be done separately or together as part of the safety assessment. In this case, the scope of the safety assessment must cover the whole change.

#### 2.4.5 Changes affecting multiple air traffic services providers — Example of overarching safety argument

- (a) The purpose of this section is to describe multi-actor changes that involve more than one air traffic services provider changing their functional systems and, therefore, performing safety assessments for their respective changes and developing an overarching safety argument.
- (b) The overarching argument, stating that a complete change (i.e. a change that comprises changes to functional systems of several air traffic services providers) is acceptably safe, can be provided in various forms. For illustrative purposes, an example of a particular approach, which is by no means unique, is presented. Other forms of organising the safety arguments and the coordination between air traffic services providers may be also valid, provided the complete change is covered.

- (c) Two air traffic services providers are providing services in two different but neighbouring airspaces. Air traffic services provider A decides to make a change to its functional system that has an impact on the environment in which the service is provided, which in turn impacts the operating context in which air traffic services provider B provides its services (because their operating contexts interact). As a consequence, it is identified that air traffic services provider B has to change its own functional system in order to achieve an acceptably safe service in its context of operation. Air traffic services provider A can only argue about the safety of the service it provides in the part of its operating context (A) where there is no interaction with the operating context of air traffic services provider B. Similarly, air traffic services provider B can only argue about the safety of the service it provides in the part of its operating context (B) where there is no interaction with the operating context of air traffic services provider A. In the interface (and surroundings) where both contexts overlap and there are interdependencies between the air traffic services providers, the safety argument can only be produced when there is full cooperation between the providers. A coordination team may be set up, but it is not required. Consequently, this cooperation generates a common overarching safety argument. The way the arguments are built and in which safety cases they are included is irrelevant, as far as the coordination is performed. The following is a non-exhaustive list of ways in which this overarching argument can be presented:
- (1) In an overall safety case that uses two separate safety cases from air traffic services provider A and air traffic services provider B (see Case 'a' in Figure 15);
  - (2) As part of the safety case of air traffic services provider A, as initiator of the change (see Case 'b' in Figure 15);
  - (3) As part of a single safety case that argues about the combined changes of both air traffic services providers (see Case 'c' in Figure 15)





**Figure 15: Notional depiction of examples of overarching safety arguments**

### 3. PROCESS VIEWS

#### 3.1. SERVICE PROVIDER CENTRIC VIEW

##### 3.1.1. Change to functional system and its assessment

This guidance contains a description of the internal processes and actions of a service provider during change. It covers: the detection of a possible or actual change, the assessment of its impact on the behaviour of the service provided, the decision to change the functional system and finally the assessment of the effects of the planned change on the service provided.

(a) Assessing the need for a change to a functional system.

- (1) Identifying whether a change, proposed by the service provider itself or by someone other than the service provider, requires a responsive change to the service provider's functional system, relies on a process for deciding whether the proposed change will, in the case of an air traffic services provider, have: no effect; an acceptable effect or an unacceptable effect on the safety of the service delivered by the service provider. In the case of a service provider other than an air traffic services provider, the process needs to decide whether the proposed change will have: no effect; an acceptable effect or an unacceptable effect on the behaviour of the service as currently specified. The process uses many of the techniques and criteria associated with safety assessment and safety support assessment (and assurance). Moreover, the nature of the change will determine how easy it is to satisfy those criteria.
- (2) The process described below, together with the examples of changes that show different paths through the process and different levels of difficulty, is for guidance purposes only. It is not intended to be a representation of any particular process. It is only complete insofar as it explains the differences in assessing whether a responsive change is necessary and the assessment needed if the service provider decides to make a change to its functional system. It does not describe interactions with other service providers who may have instigated the change or who may receive the changed service<sup>56</sup>. The process is illustrated in Figure 15. The process is very similar for an air traffic services provider and a service provider other than an air traffic services provider, except that questions and actions associated with safety risk are replaced by questions and actions associated with the specification of the service and the specification of the context over which the specification is valid.

<sup>56</sup> For a description of the interactions between service providers during a change see Section 3.3 in this Appendix.



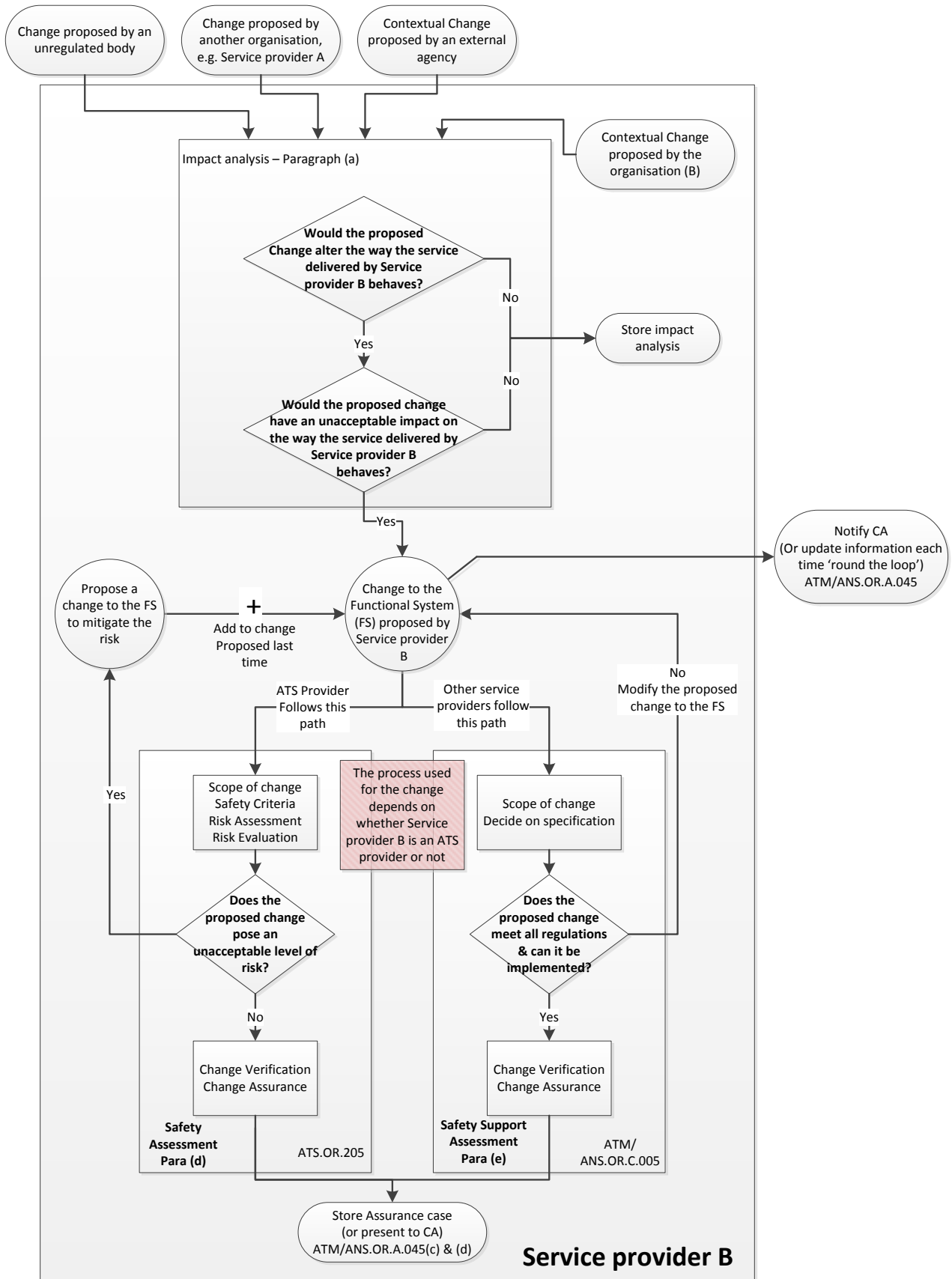


Figure 16: The assessment of change





- (3) The first thing that needs to be done is to establish whether the way Service B (provided by service provider B) behaves is in any way dependent on the proposed change. This can be as simple as reading the change description and immediately coming to the conclusion that there is no impact on safety or the specification of the service. Alternatively, it can be as complicated as having to do a full scope analysis on a sizeable part of service providers B's functional system. The need to do an interdependency analysis is stated in ATM/ANS.OR.A.045(e)(1).
- (4) At this stage, a scope analysis is needed, i.e. service provider B needs to identify all the parts of its functional system that may be affected by the change<sup>57</sup>.
- (5) If the scope analysis determines that there are no interactions between the proposed change and the functional system, then the answer to the question: 'Would the proposed change alter the way the service delivered by service provider B behaves?' is 'no', and the service provider simply stores the impact analysis<sup>58</sup>. Clearly, the impact analysis needs to be fit for purpose<sup>59</sup> (of acceptable quality and with a valid argument). Consequently, depending on the difficulty of identifying dependencies, the analysis can be from a few lines to many pages.
- (6) However, if the analysis determines that there is some interaction between the proposed change and the functional system or its context of operation and, consequently, there may be some impact on service provider B's service, then the level of impact needs to be established<sup>60</sup>. In order to do this, there is a need to establish:
- (i) what 'hazards' are affected (or whether new ones will be introduced);
  - (ii) what level of 'risk' these changes to the hazards represent; and
  - (iii) whether this level of 'risk' is acceptable without changing the functional system.

For an air traffic services provider, 'hazards' and 'risks' are safety hazards and safety risks. For a service provider other than an air traffic services provider, 'hazards' and 'risks' are not safety hazards or safety risks. Instead, they will be hazards that might cause the service to behave differently from that which is currently specified and the risks of so doing.

---

<sup>57</sup> Such a scope analysis needs to identify:

- (1) interfaces and interactions between the elements being changed and the functional system; and
  - (2) interfaces and interactions between the elements being changed and the environment in which it is intended to operate.
- This analysis uses similar techniques to those responding to ATS.OR.205(a)(1) or ATM/ANS.OR.C.005(a)(1).

<sup>58</sup> If the impact analysis does not lead to a responsive change, then the CA may wish to review the results of the impact analysis during periodic oversight.

<sup>59</sup> The purpose here is that of communicating the findings to someone else, e.g. a CA, so that their adequacy may be assessed.

<sup>60</sup> Such determination uses similar techniques to those responding to ATS.OR.205(b)(1) or ATM/ANS.OR.C.005(b)(1), e.g. for an air traffic services provider:

- (1) identification of hazards;
- (3) determination of the safety criteria applicable to the change;
- (4) risk analysis in relation to the harmful effects or improvements in safety related to the change; and
- (5) risk evaluation.



- (7) If the level of impact is determined as being acceptable, then the answer to the question: ‘Would the proposed change<sup>61</sup> have an unacceptable impact on the way the service delivered by service provider B behaves?’ is ‘no’, and the analysis stops here. The analysis is stored<sup>62</sup>. Again, it can be quick and simple or long and difficult; it all depends on the nature of the change. The analysis must be of acceptable quality and the argument valid. The stored analysis is effectively an assurance case.
- (b) Changing the functional system
- (1) If the answer to the question: ‘Would the proposed change<sup>63</sup> have an unacceptable impact on the way the service delivered by service provider B behaves?’ is ‘yes’, then in these circumstances, service provider B must propose a change<sup>64</sup>. The minimum change is simply to do the minimum necessary to mitigate the risk — the service provider should do more to improve safety, if it is feasible<sup>65</sup>.
- (2) As there is now an identified need to change the service provider’s functional system, the change must be planned and the CA must be notified. The planned change is assessed<sup>66</sup> and an assurance case produced<sup>67 68</sup>.
- (3) There may be no externally instigated change. The service provider may simply wish to change its functional system. When it decides to do so, it plans the change and notifies the CA. The planned change is assessed and an assurance case produced.
- (4) It may be found that the change to the ATM/ANS functional system has an acceptable level of impact on the first pass through the assessment process, i.e. no mitigation is needed. It would, therefore, appear that the safety assurance case could be produced after the question: ‘Would the proposed change pose an unacceptable level of risk?’ is answered negatively or the safety support assurance case could be produced after the question ‘Does the proposed change meet all regulations and can it be implemented?’ is answered positively. It could be argued that to perform verification of the change is an unnecessary and consequently inefficient use of resources because adequate safety or specification of service has already been demonstrated by design. Such a view appears to be a proportionate response to the findings of the assessment. However, this view is unjustified because while the intent may be to perform a change that ‘does what it is supposed to do’ and the design supports this intent, the implementation may not match the design and so a change which has no designed safety or other performance consequences may have some

<sup>61</sup> Note that here we are still dealing not with a proposed change to the functional system, but with some other proposed change. This other proposed change may or may not require notification to the CA.

<sup>62</sup> There is a subtlety here: If the way the service behaves still meets the specification promulgated by service provider B, then there is no change. However, if service provider B still believes it behaves acceptably but it does not meet the specification, then service provider B will have to notify the CA of the change.

<sup>63</sup> Note that here we are still dealing not with a proposed change to the functional system, but with some other proposed change. This other proposed change may or may not require notification to the CA.

<sup>64</sup> It could also attempt to prevent service provider A or any other change proposers making the change they propose.

<sup>65</sup> Complying with ATS.OR.210(b) & ATS.OR.200(a)(2)(iii)

<sup>66</sup> Complying with ATS.OR.205(b) or ATM/ANS.OR.C.005(b) as appropriate.

<sup>67</sup> Complying with ATS.OR.205(d) or ATM/ANS.OR.C.005(d) as appropriate.

<sup>68</sup> For a full explanation of the interactions between the service provider and the CA during change, see Section 3.2 of this Appendix I.



when it is implemented. The verification, therefore, guards against the failure to implement the design as intended<sup>69</sup>.

(c) Setting the objective for safety

(1) Having decided to make a change, the air traffic services provider needs to set an overall objective for the safety of the change, which will be used in setting the criteria for acceptability of the change<sup>70</sup>. This can take one of three forms:

- (i) The change will leave the functional system at least as safe as it was before the change; or
- (ii) While not leaving the system as safe as before, the change has some societal benefit that compensates for the reduction in safety and this is agreed by the CA; or
- (iii) While not leaving the system as safe as before, the change will leave the system safe enough and may be followed by one or more changes that will compensate for the loss of safety. The additional risk potentially introduced by the change, the time over which it will exist, and the way it will be compensated for in the future must be acceptable to the CA.

(2) The safety criteria are developed from this overall objective for safety as the architecture of the change evolves and the desirable properties of the change can be established. The fulfilment of all these safety criteria will be necessary in order to satisfy the objective for safety (ATS.OR.210(b)(2)).

(3) The objective for safety may change as the change itself is developed. The change may prove more difficult than envisaged at first and so, while the original aim was to satisfy (1)(i) above, it may only be possible to satisfy (1)(iii) above. Consequently, it should be seen more as a goal (objective) than a requirement.

(4) In general, changes initiated by a service provider other than an air traffic services provider will be multi-actor changes; consequently, a responsive change may need to be triggered by each air traffic services provider who is affected by the change. In this case, an objective for the safety of the change is established individually by each air traffic services provider who has to make a responsive change. It is, of course, possible that the original change does not alter the service provided by the service provider other than an air traffic services provider at all. In which case no objectives for safety need be established and all that is needed is a safety support assurance case.

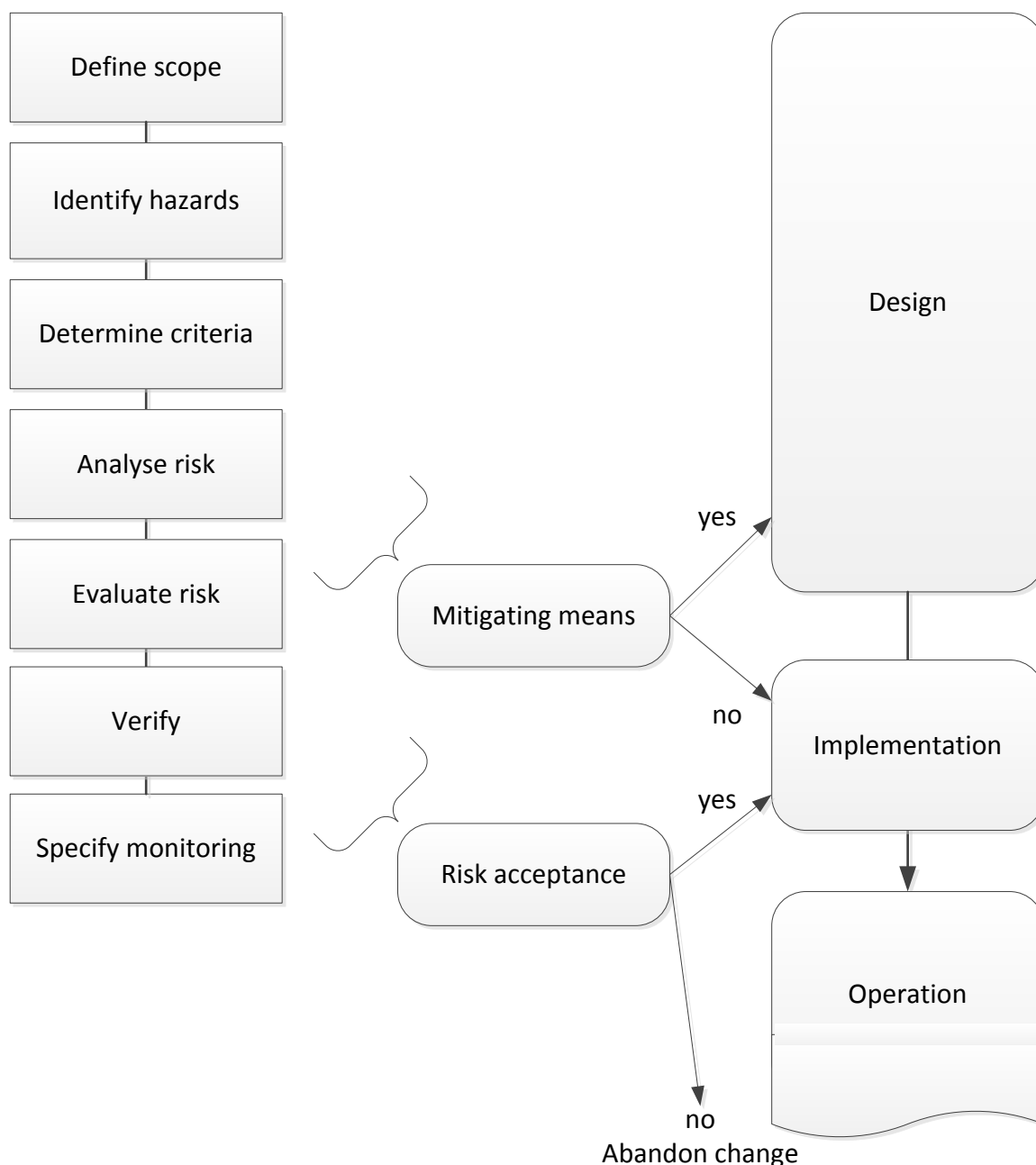
(d) Performing a safety assessment

Figure 17 below shows a schematic representation of the safety assessment process.

<sup>69</sup> This argument applies to the verification of changes to all ATM/ANS functional systems and not just to ATS functional systems.

<sup>70</sup> Complying with ATS.OR.210(b).





**Figure 17: Schematic representation of the safety assessment process**

- (1) The rectangular boxes in Figure 17 correspond to the steps in the execution of a safety assessment. The lines between these boxes are not intended to indicate that these steps must be executed sequentially; they simply indicate a top-down order that is a comprehensible sequence and a common practice. However, it might be beneficial to go from one step to another in a different sequence or in a number of steps.
- (2) The box ‘Mitigating means’ corresponds to the decision by the air traffic services provider to adapt the design by incorporating mitigating means (‘yes’) or to accept the design from the perspective of risk evaluation (‘no’). The box ‘Risk acceptance’ corresponds to the

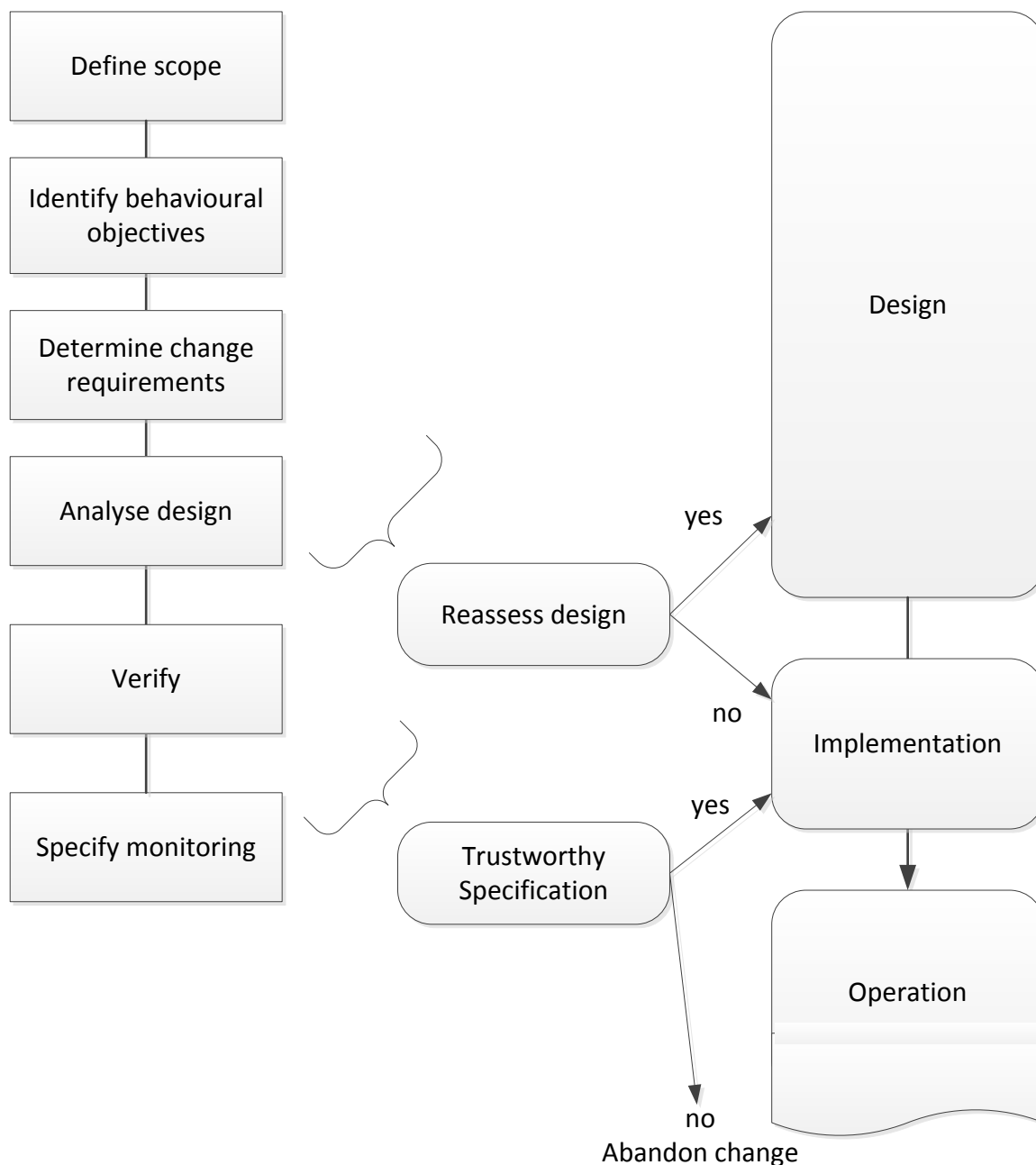
decision by the air traffic services provider and, whenever the change is reviewed by the CA, the approval by the CA, to let the change enter operation ('yes') or not ('no').

- (3) It is possible that, initially, the proposed change does not adequately mitigate the risks, i.e. the answer to the question in Figure 16: 'Does the proposed change pose an unacceptable level of risk?' is 'yes'. In this case, a proposal to mitigate the additional risk is made, i.e. an additional mitigation is proposed and is added to the previous change proposal. The CA is informed of any changes to the material it has already received as part of the process used to determine whether it wishes to review the change or not and the safety assessment process starts again from the beginning<sup>71</sup>. Whether it can deal simply with the differences or it means a considerable re-work of the material developed so far, depends upon why the first change did not mitigate the risk — as it was intended to do.
  - (4) The rounded boxes at the right of the figure correspond to the main steps in the processes for the development of the change. The rounded boxes in the middle correspond to the main decisions that govern the outcome in the development of the change made during the safety assessment. Several processes and decisions are not explicitly indicated. These include decisions and actions by the CA, preparatory activities and documentation.
  - (5) The decisions can occur at different points in the safety assessment process:
    - (i) It is possible to adopt mitigating means (indicated by 'yes' at the right of the box 'mitigating means') before the risk evaluation is finished. The decision to implement the change (indicated by 'no') should, however, be based on the results of the risk evaluation.
    - (ii) It is possible to decide not to implement the change (indicated by 'no', below the box 'risk acceptance') before all steps of the safety assessment process are finished. The decision to put the change into service (indicated by 'yes') should only be taken when a valid safety case for the change exists, which is based on the overall results of the safety assessment.
  - (6) The process of executing the risk analysis and the risk evaluation may depend on the maturity of the change and on the selected safety assessment method.
    - (i) It is, for example, possible to compare the estimated risk directly to the safety criteria, after which decisions on implementation, adaptations of the design and risk mitigation can be made. This is more likely to be of benefit later on in the process when the risk evaluation is relatively mature.
    - (ii) It is also possible to derive safety objectives and safety requirements from the safety criteria. These are allocated to the different elements/parts of the functional system affected by the change. The planned change is adapted during its development to make sure that the safety objectives and safety requirements can be met.
- (e) Performing a safety support assessment

Figure 18 below shows a schematic representation of the safety support assessment process.

<sup>71</sup> Guidance on the safety assessment process may be found in GM4 ATS.OR.205(b) Safety Assessment and Assurance.





**Figure 18: Schematic representation of the safety support assessment process**

- (1) The rectangular boxes in Figure 18 correspond to the steps in the execution of a safety support assessment. The lines between these boxes are not intended to indicate that these steps must be executed sequentially; they simply indicate a top-down order that is a comprehensible sequence and a common practice. However, it might be beneficial to go from one step to another in a different sequence or in a number of steps.
- (2) The box 'Reassess design' corresponds to the decision by the service provider to alter the design because it will not satisfy the behavioural objectives ('yes') or to accept the design from the perspective of design analysis ('no'). The box 'Trustworthy specification'

corresponds to the decision by the service provider and, whenever the change is reviewed by the CA, the approval by the CA to let the change enter operation ('yes') or not ('no').

- (3) It is possible that, for a service provider other than an air traffic services provider, the proposed change will behave as intended, i.e. the answer to the question in Figure 16: 'Does the proposed change meet all regulations and can it be implemented?' is 'no'. Mitigation would take the form of either modifying the proposed change to the functional system so that it better matches service provider B's intent or changing the specification to match the functionality and performance of the changed service. The CA is informed of any changes to the material it has already received as part of the process used to determine whether it wishes to review the change or not and the safety support assessment process starts again from the beginning<sup>72</sup>. Whether it can deal simply with the differences or it means a considerable re-work of the material developed so far, depends upon why the first change would not behave as it was intended to do.
- (4) The rounded boxes at the right of Figure 18 correspond to the main steps in the processes for the development of the change. The rounded boxes in the middle correspond to the main decisions that govern the outcome in the development of the change made during the safety support assessment. Several processes and decisions are not explicitly indicated. These include decisions and actions by the CA, preparatory activities and documentation.
- (5) The decisions can occur at different points in the safety support assessment process:
  - (i) It is possible to alter the design (indicated by 'yes' at the right of the box 'Reassess design') before the analysis of the design is finished. The decision to implement the change (indicated by 'no') should, however, be based on the results of the analysis of the design.
  - (ii) It is possible to decide not to implement the change (indicated by 'no', below the box 'Trustworthy specification') before all steps of the safety support assessment process are finished. The decision to put the change into service (indicated by 'yes') should only be taken when a valid safety assurance case for the change exists, which is based on the overall results of the safety support assessment.

## 3.2. SERVICE PROVIDER — COMPETENT AUTHORITY INTERACTION VIEW

### 3.2.1. Interactions between service providers and competent authorities during the change process

The purpose of this guidance is to describe the interactions that take place between the service provider making a change to its functional system and the CA in deciding whether to review the change or not, and in reviewing the change. It also explains the use of some of the technical terms provided in the Regulation<sup>73</sup>.

<sup>72</sup> Guidance on the safety support assessment process may be found in GM1 ATM/ANS. OR.C.005 Safety support assessment and assurance of changes to the functional system.

<sup>73</sup> Many different process models and technical terms are used by ATM/ANS providers and CAs to describe aspects of change. These models and the technical terms used are not standardised throughout Europe and the scope of changes varies considerably. It is, therefore, impossible to define a generic process model that includes all variability in terms used, the stages/phases used and the milestones. Consequently, the approach taken in this General GM is to explain the terminology, phases and milestones used in the



This GM uses the model described in Section 2.1.1 of this Appendix as the basis for understanding what is meant by a change, i.e. it is some physical alteration to one or more of the components (people, procedures or equipment (HW or SW)) of the functional system or to the architecture (connections between components or the set of laws governing the relationships between the inputs to the functional system and its outputs) of one or more service providers that would potentially alter the way the service they deliver behaves. The change may be a necessary response to a (proposed) change in the operational context of one or more of these services. As the word 'change' has many meanings, it is not possible to give an adequate and appropriate definition of a 'change'; some guidance has been provided to explain the different cases of changes needing safety and safety support assessments as per ATM/ANS.OR.C.005 and ATS.OR.205 and some examples have been provided.

(a) Overview of the change process (See Figure 19)

- (1) Most changes start by identifying the need for a change and establishing sufficient information about the change, that it can be put to the organisation's management board for their agreement. From the perspective of change regulation, this (planning) phase is not included in this GM and is not shown on Figure 19.
- (2) When a service provider has a real intent to implement a change, it should notify the CA of its intent to change the functional system as early as possible bearing in mind that:
  - (i) it has to give the CA sufficient time to decide whether to review the assurance case or not; and
  - (ii) if the CA decides not to review the change, the service provider may make the change in accordance with the approved procedures. An important element of the procedures is that the service provider will produce a valid assurance case before making any change to the functional system that could affect the operation.

Note that, as part of general oversight, the CA may select such a change to determine if the procedures are applied properly and the change is safe. Apart from general oversight, the CA will not be involved in the change.
  - (iii) If the CA decides to review the change, the CA may wish to be involved in the change process. As a consequence of the CA's decision, the implementation of the change is dependent on the approval of the CA.
- (3) The details of the interaction process will be described in both the CA and service provider's procedures. For optimum effectiveness and efficiency, the parts of these procedures dealing with the interaction between the CA and the service provider are best developed cooperatively.
- (4) The general concept that rules such procedures will be that the service provider will inform the CA about the planning and important steps in respect of safety in the development of the change. If the CA decides not to review a change, the exchange of information will be minimal.

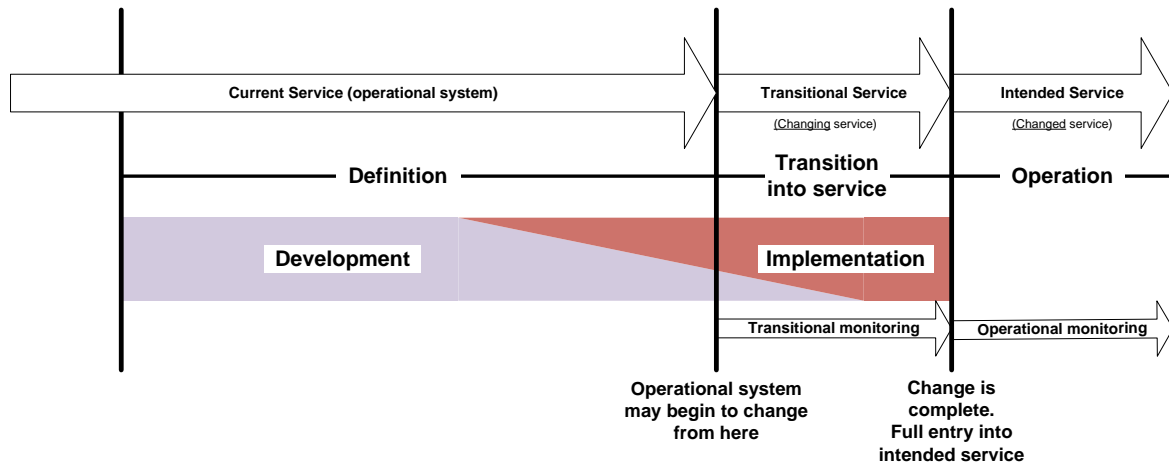
---

legislation in enough detail and with enough clarity that both ATM/ANS providers and CAs can see how the legislation maps to their particular model of the change process.





- (5) All work related to the development of the change can continue until any part of the change, if implemented, would affect the operational service. At this point, the change needs to be accepted by the service provider and where the change is to be reviewed, approved by the CA.



**Figure 19: An overview of the change process**

- (6) Figure 19 shows that the change process consists of two different processes: development and implementation. No timescales are implied in Figure 19 because the definition and transition into service phases may take many years in some cases, e.g. moving an ATC unit to a different location, and a few days in others, e.g. simple change to a procedure is made and communicated to the operators by means of a briefing paper.
- (7) The difference between developing and implementing a change is that development deals with design<sup>74</sup>, whereas implementation deals with concrete artefacts, i.e. those built or manufactured component parts that were identified in the design, and also with integrating them into the functional system to become a whole. Since, at any stage, some artefacts are being developed, while others are being implemented, e.g. Commercial Off The Shelf (COTS) components may be purchased before some other components have been designed, and simple changes to software may predate the changes to the hardware on which it operates, the diagram shows considerable overlap between development and implementation.
- (8) Note that any part of the implementation that has the potential to affect the operational service<sup>75</sup> cannot be started until a valid assurance case for the part of the change being

<sup>74</sup> There is also an interaction between development and implementation. Concrete (implemented) artefacts may be used in a manner that assists the development (design) of other dependant artefacts.

<sup>75</sup> That is, one that potentially changes the way the operational service behaves, e.g. the installation of Mode S, even though the information is not used immediately after installation. Note that building and testing the Mode S radar can be done before it is installed into the functional system. So implementation of the radar comprises two parts: building and testing it in isolation from the functional system and implementing (installing) it within the functional system.

implemented exists or, where the CA has decided to review the assurance case, it or part thereof has been approved<sup>7677</sup>.

- (9) The service provider may decide to implement the change in phases. This is described in (d) below, which introduces the notion of a ‘transitional service’ where the change may be introduced gradually. Figure 20 shows such a situation. The first implementation activities begin before the change has any influence on the operation. Overall development continues during the transitional service and is finalised well before the change reaches the point where the change is completed. Each transition may enter operational service provided a valid assurance case for it exists.
- (10) The development of the change may continue during the transition of the change into service. However, the assurance case needs to contain a valid safety argument that is in line with such an approach.
- (11) The ‘operation’ phase begins when the change has been completed<sup>78</sup> and the operation is as intended. As part of the safety/safety support assessment<sup>79</sup>, it may have been decided that, during operation, monitoring activities are required to be established. The CA may wish to review this monitoring process or may wish to be informed about its results as part of its general oversight. This will lead to the necessary interactions.
- (12) Assurance of the safety of the change may lead to two types of monitoring requirements:
- (i) Temporary monitoring requirements; and
  - (ii) Permanent monitoring requirements.

Temporary monitoring may be used, during transitions, to build confidence in the assurance case. It may be accompanied by temporary measures such as mitigations that reduce the risk of the operation. These measures can be removed once the necessary level of confidence has been established.

Transition finishes (and ‘Operation’<sup>80</sup> begins) when all the confidence building measures (Temporary monitoring and mitigations) have been removed. Consequently, if the transition phase is long, the implementation phase is correspondingly long. The monitoring that remains is then the permanent monitoring that is required to show that the change remains safe and behaves as predicted in the assurance case.

- (13) In cases where the change does not meet the expectations, i.e. does not satisfy the temporary monitoring requirements, then a ‘back out’ or recovery plan is needed. This plan

<sup>76</sup> This is shown on the diagram as a vertical line separating the current and transitional services.

<sup>77</sup> This may be more difficult than would appear to be the case at first sight. It is difficult to prevent the knowledge gained in training or the skills learnt in the simulation of a new procedure being adapted to modify the current procedures. Consequently, it may be necessary to include such training and simulation exercises as part of the transitional service rather than part of development.

<sup>78</sup> Shown on the diagram as a vertical line, with the caption ‘Change is complete. Full entry into intended service’, separating the transitional service from the intended service.

<sup>79</sup> See monitoring requirement in safety assessments and safety support assessments as part of ATS.OR.205(b)(6) and ATM/ANS.OR.C.005(b)(2) respectively.

<sup>80</sup> This is the Operation phase shown in Figure 19. During transitions, operations are affected. However, these operations are part of the phase called ‘transition in to service’ in Figure 19, in order to differentiate them from those operations that will be in place once the change is complete.



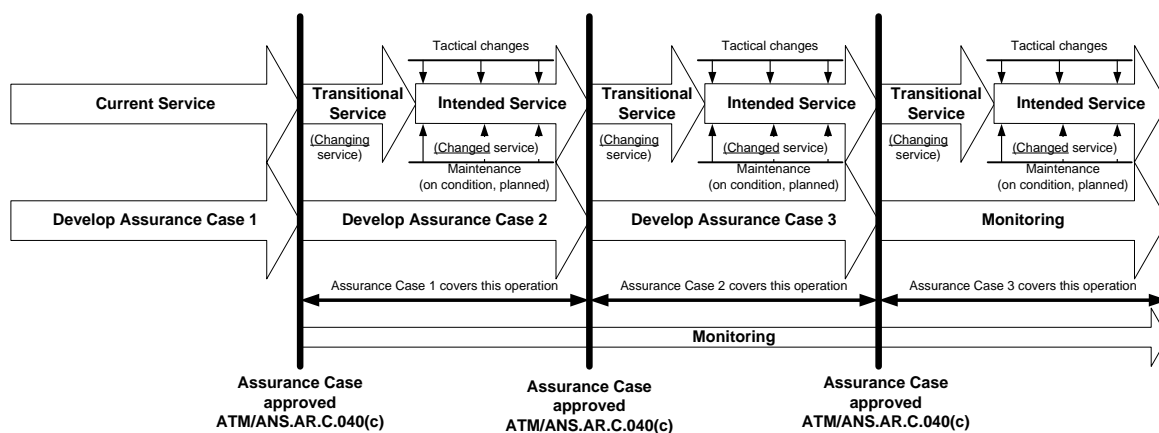
may depend on the risk involved and also may be conditional on the probability of an unexpected outcome after implementation of the change.

(b) Different types of transitions in services

- (1) Changes, e.g. novel, large or multi-actor changes, may involve several transitional steps when going from the current operational service to the intended service. The service provided during these steps varies as a result of phased changes to the functional system. These steps are included in the 'Transitional Service' shown in Figure 20.
- (2) The service provider's decision to implement the change in steps may have various reasons, such as planning, training of personnel, gaining experience with specific elements of the change before progressing. Independently of the reason for the decision, it is important to inform the CA of the approach that is chosen and the consequences for the change process, as it allows the CA to prepare, if necessary, for a series of related changes rather than approaching it as a single change.

In general, there are two ways of making transitional changes:

- (i) Each transition is treated as a separate change. In this case, each change is notified separately to the CA and will have its own assurance case (as illustrated in Figure 20 below<sup>81</sup>).
- (ii) All the transitions are included within a single change and governed by a single assurance case that must cover all transitions (as illustrated in Figure 21).



**Figure 20: Concatenated changes**

- (3) In cases where separate changes are concatenated, as shown in Figure 20, the CA will decide for each change whether it will be reviewed or not. However, the provider should avoid separating the change into multiple small changes unnecessarily (the so-called 'salami slicing') as the lack of information about the relationships between the various changes may leave the intent of the final service uncertain.
- (4) If there is a relationship between the changes, it would be best to inform the CA about the relationship in order to expose the common information. For such changes, specific

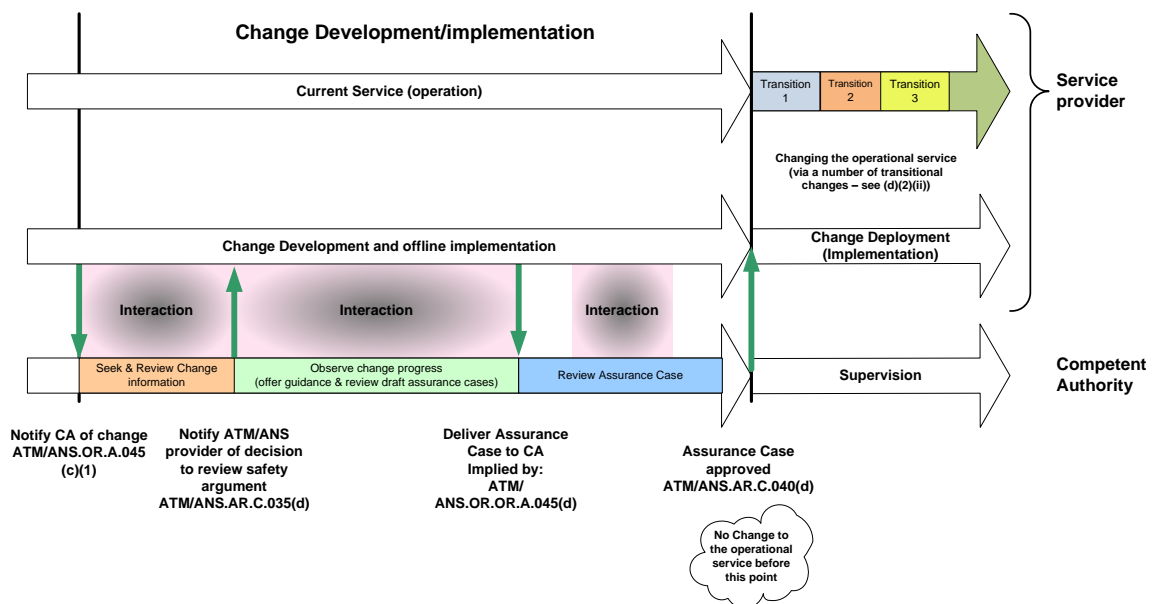
<sup>81</sup> For simplicity, this diagram and all others are illustrated as though the change were being made by an air traffic services provider. If the change only involved an ATM/ANS provider, then the diagram would use Safety Support language.

arrangements between the service provider and the CA may be supportive for proper understanding and communication. Furthermore, the CA may wish to make suitable internal arrangements in respect of its own phasing of the review of the change.

- (5) The assurance case must argue and provide evidence that shows that the final operational service is acceptable<sup>82</sup>. Following a transition, the changed system may not behave in accordance with the criteria established for that transition<sup>83</sup>. Therefore, as part of the transition planning, the service provider should establish a way of returning to an acceptable service. This part of the transitional planning may be called a ‘back out plan’ in the assurance case.
- (6) If it is foreseen that the overall change would lead to an improvement of safety, but a specific transitional step would lead to a reduction of safety, the CA needs to decide if this is acceptable and may impose specific conditions. The foreseen reduction in safety is to be brought to the CA’s attention as soon as it becomes clear. In supporting such a decision, the service provider will explain why such a reduction of safety cannot be prevented, what measures will be taken to limit the reduction of safety and what overall safety gain will be achieved.
- (7) As discussed in (d) above, in all cases, the assurance case must cover the transition service(s) and the operational service(s) of concern.

(c) Interactions — From notification to approval

A more detailed view<sup>84</sup> of the process from notification to approval is shown below:



<sup>82</sup> In the case of a change to the functional system of an air traffic services provider, it is ‘acceptably safe’. In the case of any other ATM/ANS service, ‘acceptable’ means that the service meets the declared specification for the particular transition.

<sup>83</sup> Note that this implies that the next transition should not begin until sufficient time has elapsed for there to be confidence that the temporary monitoring criteria have been satisfied.

<sup>84</sup> In the diagram, the ‘transition into service’ (see ATM/ANS.OR.C.005(a)(1)(iv) and ATS.OR.205(a)(1)(iv)) is accomplished via a series of transitional changes to the functional system which results in a number of transitional services. To aid readability, the diagram uses the term ‘transition’ instead of the more correct ‘transitional service’.

**Figure 21:** Processes prior to initial entry into service

- (1) The CAs activities in this part of the model are divided in three stages:
  - (i) Seek and review change information;
  - (ii) Observe change progress<sup>85</sup> and possibly review draft versions of the assurance case; and
  - (iii) Review assurance case.
- (2) Seek and review change information
  - (i) This stage begins when the service provider notifies the CA of the change<sup>86</sup>. Immediately after this, the CA will seek the information needed in order to decide whether to review the assurance case<sup>87</sup> or not<sup>88</sup>. This information will result from interaction between the CA and the service provider and it will help the CA in understanding the scope, size, complexity and novelty of the change. As every change is different, definitive rules for the required information cannot be given and so the process is best regarded as one that is beneficial to both parties. The CA does not need or wish to review every assurance case and the service provider will minimise the effort of interacting with the CA if it provides appropriate and sufficient information about the change<sup>89</sup>.
  - (ii) Notification is an event. Its intent is to alert the CA to the fact that a change is proposed by a service provider. However, given that some changes, those that carry very low levels of risk, will not be reviewed, the notification carries sufficient information to identify these cases without further interaction between the CA and the service provider<sup>90</sup>.
  - (iii) Having decided whether or not to review the assurance case for the change, the CA needs to inform the service provider of the decision<sup>91</sup>. The service provider should be advised of the decision whether it is positive or negative. This guarantees for each change clarity between the service provider and the CA about the involvement of the CA.
- (3) Observe change progress

<sup>85</sup> This is usually achieved by regular coordination activity during development and implementation. See (e)(3) for more detail.

<sup>86</sup> Please see ATM/ANS.OR.A.045(a).

<sup>87</sup> It may seem unusual to review the assurance case rather than review the change. However, since the change has not been implemented at this stage, then the only available course of action is for the CA to review the change via its assurance case.

<sup>88</sup> See ATM/ANS.AR.C.035(a).

<sup>89</sup> If the information provided is not appropriate or sufficient to help the CA make its review decision, the CA should request additional information from the service provider about the change as requested in ATM/ANS.AR.C.035(a).

<sup>90</sup> See AMC2 ATM/ANS.OR.A.045(a) & GM1 ATM/ANS.OR.A.045(a) for a definition of the information required in a notification.

<sup>91</sup> See ATM/ANS.AR.C.035(c).



- (i) Once the service provider has been advised that the assurance case will be reviewed, the CA could wait for the assurance case report<sup>92</sup> to be delivered by the service provider. However, in reality, since the review will normally take place where the change is either large, complex or novel<sup>93</sup>, the CA would be well advised to engage with the service provider earlier. This will allow the CA to acquire knowledge of the safety aspects and the details of the change slowly via workshops, attending the service provider's coordination activities or the phased delivery of the assurance case, rather than having to assimilate a very large amount of information in a short time. The review time is critical, as once the service provider has completed the assurance case, it is likely that it would wish to start changing the operational service quickly. These coordination activities will also allow the CA to establish that the acceptance criteria are valid<sup>94</sup> (relevant, sufficient and necessary).
  - (ii) Interaction may also be beneficial to the service provider. For instance, the CA may have experience of similar projects for which the service provider does not have (i.e. the change may be larger or more complex than they are used to or may be novel). The CA may be able to provide timely information that will assist the service provider's approach and should do so, providing it does not compromise the regulator/regulated relationship (regulatory capture).
  - (iii) In summary, in the period between advising the service provider that a change is to be reviewed and receiving the assurance case, there will be a period of interaction between the CA and the service provider where the CA learns about the change in a comfortable way and can offer guidance on the likely acceptability of the assessment and the assurance case<sup>95</sup>.
- (4) Review assurance case
- (i) The next stage begins once the assurance case has been delivered to the CA<sup>96,97</sup>. Fundamentally, the purpose of the review to determine that:<sup>98</sup>
    - (A) the change is and will remain safe in accordance with the safety criteria (for air traffic services providers) or the service after the change will behave and will continue to behave only as specified in the specified context (for service providers other than air traffic services providers);

<sup>92</sup> Assurance case report: a summary of the assurance case that enables the CA to gain full access to the assurance case — see definition in Section 1.1 of this Appendix.

<sup>93</sup> The CA may also randomly select assurance cases for review. This may be done as a means of validating the review selection criteria.

<sup>94</sup> In the case of a safety case, the acceptance criteria are safety criteria. In the case of a safety support case, the acceptance criteria are the validity of the specifications of behaviour and context.

<sup>95</sup> Including the acceptance criteria.

<sup>96</sup> Implied by ATM/ANS.OR.A.045(d).

<sup>97</sup> The assurance case delivered may not actually be an assurance case, but may be an assurance case report, which may be limited to the identification of the claims and arguments (although not necessarily all of them) and will probably not include the bulk of the evidence. That will be retained by the ATM/ANS provider simply because of its bulk.

<sup>98</sup> If any of these criteria are not satisfied, it could be a result of flaws in the approved change procedures. The realisation of this should trigger separate supervisory activity. Clearly, this activity will interact with the change review process, but is not the subject of this General GM.



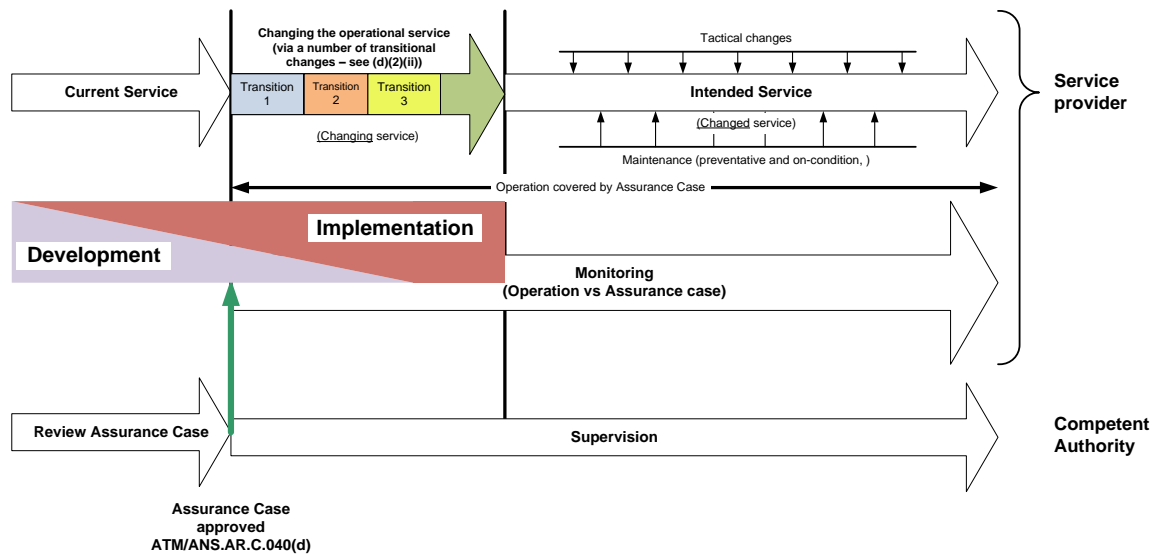
- (B) for air traffic services providers, the proposed change conforms to the scope that was subject to safety support assessment, the safety criteria are justified and establish a valid safety level that is as low as is reasonably practicable; or
  - (C) for other service providers, the proposed change conforms to the scope that was subject to safety support assessment, the service behaves only as specified in the specified context, and the way the service behaves complies with and does not contradict any applicable requirements of this Regulation placed on the services provided by the changed functional system; and
  - (D) the assurance case validly argues that the safety criteria will be satisfied when the change is implemented and will remain satisfied throughout the perceived operational use (for the air traffic services provider) and that the assurance case validly argues that the service after the change will behave and will continue to behave only as specified in the specified context (for service providers other than air traffic services providers).
- (ii) The assurance case will be discussed by the service provider and the CA. When an assurance case submitted by the provider is judged to be not sufficient, not completely correct or not comprehensible, it is not necessary, in the first instance, for the CA to reject the assurance case. It may instead involve itself in additional interaction with the provider. The additional interaction may uncover missing information, unclear arguments or misunderstandings about the validity of arguments, the sufficiency of evidence or the justification of the methods used in the assessment. This could lead to an update of the assurance case (perhaps more than once) or a disagreement that will have to be resolved by management.
  - (iii) When the proposed change and the argument are considered acceptable to the CA, the assurance case will be approved<sup>99</sup> and the change to the functional system can begin. If either are not acceptable to the CA, the assurance case will be rejected. For purposes of transparency and ultimately resolution of any legal challenge, the CA needs to justify the decision. In case of rejection, the justification will be included with the rejection notification, since it is important for the service provider to understand the considerations<sup>100</sup>.
- (d) Interactions — Making the change operational

An overview of the final part of the process is shown below.

<sup>99</sup> See ATM/ANS.AR.C.040(b).

<sup>100</sup> See ATM/ANS.AR.C.040(b)(2).





**Figure 22: Making the change operational**

- (1) The operational service may begin to be changed after the:
  - (i) receipt of the CA's approval if the assurance case has been reviewed<sup>101</sup>; or
  - (ii) completion of a valid assurance case if the change is not to be reviewed by the CA<sup>102</sup>.
- (2) In this final stage, there is a transition from the current operational system to the new intended operational system (the changed system). This transition may itself consist of several phases. These are shown as Transitions 1, 2 & 3 on the diagram and described fully in (c).
- (3) Where the change is approved by the CA, normally there will be no interaction between the service provider and the CA in this phase. However, the review will have taken into consideration that the assurance case also covers any foreseen<sup>103</sup>:
  - (i) tactical changes<sup>104</sup>, i.e. day-to-day alterations in the operation; and
  - (ii) maintenance activities, i.e. preventive and on-condition maintenance.

In all cases, the service provider will consider these elements as part of their change.
- (4) The service provider will monitor the operational system to show that it conforms to the monitoring requirements in the assurance case. Some of these monitoring requirements may be for specific and permanent monitoring and are addressed through the ongoing performance monitoring of the functional system, while others may be temporary. Later changes may make monitoring requirements identified in previous assurance cases

<sup>101</sup> See ATM/ANS.OR.A.045(d).

<sup>102</sup> See ATM/ANS.OR.A.045(c).

<sup>103</sup> Only those tactical changes and maintenance actions affected by the change need to be covered in the assurance case of interest. It is expected that others are part of the design basis for the current functional system and so will already have been covered by a previous assurance case.'

<sup>104</sup> As defined in point (g) of Section 2.2.1 of this Appendix.



obsolete. The service provider may decide to introduce this type of monitoring into the framework of the SMS.

- (5) If the change does not satisfy the monitoring requirements, then usually either the change is not as predicted or the assurance case itself is incomplete or incorrect, or both. In either case, the service provider must take action to make the service and the assurance acceptable again, which may include ‘backing out’ the change, i.e. the service reverts to a previously known safe state, or proposing a new change.
- (6) During general oversight related to changes, the CA may perform audits and/or inspections to check that<sup>105</sup>:
  - (i) changes made were made validly, i.e.:
    - (A) no un-notified changes have been made;
    - (B) all un-reviewed changes have assurance cases; and
    - (C) the properties that determine whether a change should or should not be reviewed have not altered such that a change that was not reviewed, should have been reviewed.
  - (ii) the service operation is being monitored and checked against the monitoring requirements; and
  - (iii) if, as a result of the supervision, the assurance case is found to be invalid, then the CA will require the service provider to take appropriate corrective actions, which may include an amendment to make the argument valid, the instigation of a change in order to make the service acceptable or even to revert to the situation before the change.

### 3.3. MULTI-ACTOR VIEW

- (a) Changes to the functional system of a service provider, other than an air traffic services provider, may be proposed either at the request of a customer e.g. another service provider, or by itself. The interactions involved in both cases are examined below. In the first case, where the customer has requested a change, it has to check that its requirements have been satisfied. In the second case, where the supplier wishes to make an unsolicited change, the customer has to evaluate how the proposed change would affect the services it provides and may have to make a responsive change to its own functional system in order to accommodate the change in the way that the service provided behaves.
- (b) Case 1: An air traffic services provider<sup>106</sup> requests a change to the service delivered by a service provider other than an air traffic services provider.

<sup>105</sup> The checks described in this GM fall only within the scope of the supervision of a particular change. That supervision is, as with other periodic supervision, done on a sampling basis and so these checks will not be performed each time a CA periodic supervision visit occurs. Clearly, other checks are made during periodic supervision, but these are not the subject of this GM. One related check is that, as a result of the experience of a particular change, the CA may decide to review the fitness for purpose of the change procedures themselves.

<sup>106</sup> In other cases, the customer may be a service provider other than an air traffic services provider.



If the user of a service delivered by a service provider, other than an air traffic services provider, requests a change to that service, a safety support case is produced by the service provider other than an air traffic services provider and is used to demonstrate that the user's requirements are met or have been modified to reflect what can be delivered. In **Figure 23**, an air traffic services provider has requested such a change from a service provider other than an air traffic services provider.

- (1) Step 1: The requirements for the change (Service Requirements<sup>107 108</sup>) are written by the air traffic services provider and given to the other service provider along with the specification of the context in which the service will be used (Service Operational Context). However, both the air traffic services provider and the service provider making the change must remember that any proposed change must still comply with the requirements of other regulations that may proscribe and prescribe the way the service behaves, therefore, having an impact on the change. Such requirements may come, for example, from the requirements for the services included in Annexes V to Annex XII to this Regulation, in Regulation (EC) No 552/2004<sup>109</sup> and in other more general standards published by ICAO, CEN/CENELEC/ETSI or guidance published by EUROCAE.

Having developed the changed service, the other service provider will assess the service and assure itself that the Service Requirements are satisfied over the Service Operational Context. It can then write down the arguments for assurance in the Safety Support Case.

- (2) Step 2: However, initially, the other service provider may not be able to achieve the functionality or performance required or even may wish the service to do more than is required. In this case, the safety support assessment would fail (and so would the safety assessment fail if it were to be performed at this stage). In order to achieve a successful change, either the service will have to meet the requirements of the air traffic services provider or the ATS system will have to change in order to accommodate the functionality and performance that can be achieved by the service. Consequently, the differences between the functionality and performance achieved and that required by the air traffic services provider are discussed (Differences) and agreement reached as to whether the service will change to meet the initial ATS requirements or the ATS functional system will be changed to accommodate these differences.
- (3) Step 3: If the component or service is to be modified, then the differences will disappear and the safety support case can be completed.
- (4) Step 4: If the ATS system is to be changed to accommodate the actual functionality and performance of the service, then the air traffic services provider will have to change the Service Requirements and possibly the Service Operational Context. However, since the Service Requirements will now match the functionality and performance that can be achieved by the service, then the differences will disappear and the safety support case can be completed.

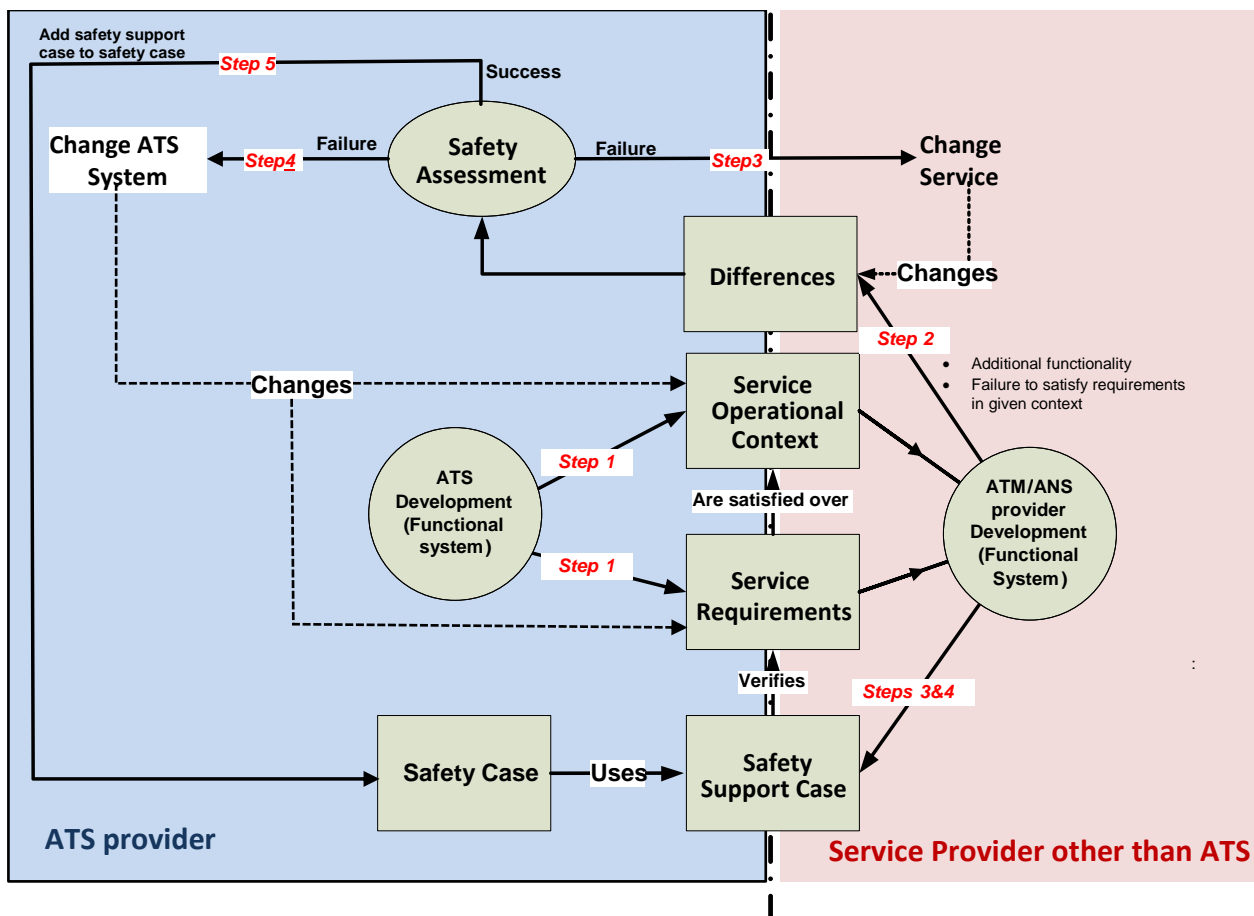
<sup>107</sup> Bracketed terms refer to items on the diagrams.

<sup>108</sup> Some of these will be safety requirements.

<sup>109</sup> Regulation (EC) No 552/2004 of the European Parliament and of the Council of 10 March 2004 on the interoperability of the European Air Traffic Management network (the interoperability Regulation) (OJ L 96, 31.3.2004, p. 26).



- (5) Step 5: Once the functionality and performance matches the ATS requirements, i.e. there are no differences then, the safety support case can be used by (added to) the safety case<sup>110</sup>.



**Figure 23: Interactions in a multi-actor change as result of an ATS’ request to change the service provided by a service provider other than an air traffic services provider**

(c) Example of case 1

- (1) For instance, when an air traffic services provider wants an additional data field to be added to the data it gets from a MET provider, the service requirements and the service operational context are used by the air traffic services provider to assure itself that its requirements are met or have been modified to reflect what can be delivered by the MET provider.
- (2) The requirements for the change to the MET data (Service Requirements) are written by the air traffic services provider and given to the MET provider along with the specification of the interface to be used to deliver the data (Service Operational Context). Having developed the additional data field, the MET provider will assess it and assure itself that the

<sup>110</sup> Note that this is a logical addition; not a physical one. The safety support case is not delivered to the air traffic services provider, rather it uses the service requirements and the service operational context, which are delivered, to argue the safety of the air traffic services when using the other service.

air traffic services provider's requirements are satisfied over the Service Operational Context. It can then write down the arguments for its assurance in the safety support case.

- (3) However, the MET provider may not be able to achieve the update frequency required, i.e. there will be differences between what can be achieved and what is required. In order to achieve a successful change in these circumstances, the ATS functional system will have to be changed in order to accommodate the lower update frequency. If the ATS system can be changed to accommodate the lower update frequency of the MET service, then the air traffic services provider will have to change the MET data requirements (Service Requirements) and possibly the interface to be used to deliver the data (Service Operational Context) to record the new design intent.
  - (4) Alternatively, if the ATS functional system cannot be changed, it may still be possible to modify the MET functional system so that it does fulfil the original requirements. However, this may incur some additional cost and delay. In this case, the differences between the performance that can be achieved by the MET functional system and what is required by the air traffic services provider will disappear.
- (d) Case 2: A service provider other than an air traffic services provider makes an unsolicited change to the service it delivers to other service providers.

Service providers, other than air traffic services providers may independently elect to make changes to their functional systems or change them as a consequence of a change to a standard or rule that is pertinent to the service they are providing. The key rules that might require such changes are identified in the requirements for the services included in Annexes V to XII to this Regulation and in Regulation (EC) No 552/2004. It is also possible that changes to other more general standards published by ICAO, CEN/CENELEC or ETSI, or guidance published by EUROCAE, which have to be complied with, may trigger the change. Where a service provider, other than an air traffic services provider, makes such an unsolicited change to its functional system, it uses the safety support case to confirm that the specification of the proposed changes to the service provided is valid, where 'valid' means that the specification correctly specifies the way the service behaves and that it complies with and does not contradict any requirements placed on the service by another part of the regulations, e.g. both rules and necessary standards.

The service provider may have proposed the change in order to sell the service to a number of current and new end users. In these circumstances, it cannot know the full context of its use. The safety support case must, therefore, clearly state the context within which the service was evaluated and ensure that the service does not behave in any other way than that which is stated in the specification. In Figure 24, a service provider other than an air traffic services provider modifies the service that is used by an air traffic services provider, without having been requested to do so.

- (1) Step 1: A safety support case will be produced showing that the specification of the changed service (Service Specification) is satisfied over some context (Evaluation Context) that the service provider other than an air traffic services providers assumes will be representative of the context of use for the service.
- (2) Step 2: In order to use the service, the air traffic services provider has to show that it can develop safety requirements that match the specification of the changed service. It also has



to show that the operational context for the service is the same as the context the other service provider used in the safety support assessment for the service (Evaluation Context). The air traffic services provider may find that it cannot produce a valid safety case because either the Safety Requirements do not match the Service Specification or the contexts are different (Evaluation Context does not match the Operational Context for the service). It could also be because the safety support assurance does not provide sufficient confidence in the performance of the component in order for it to be used in the manner foreseen by the air traffic services provider.

- (3) Step 3: In the case where the matching of specification to requirement fails or the matching of the contexts fails, the air traffic services provider may need to alter the ATS system in order to use the component or service in its changed form. In so doing, the requirements (Safety Requirements) will be changed, the context in which the service is used (Operational Context) will be changed or both will be changed. This will allow a valid safety assessment to be performed and the safety case including the safety support case to be created<sup>111</sup>.
- (4) Step 4: Where there is insufficient confidence in the service, the air traffic services provider may either change the ATS functional system such that the service can be used safely or can ask the other service provider<sup>112</sup> to increase the depth of evaluation, i.e. change the Evaluation Context, in order to improve the level of assurance as argued in the safety support case.
- (5) Step 5: In both cases, the safety support case can now be used by the safety case.

---

<sup>111</sup> Note that this is a logical addition not a physical one. The safety support case is not delivered to the air traffic services provider, rather it uses the service requirements and the service operational context, which are delivered, to argue the safety of the air traffic services when using the other service.

<sup>112</sup> Or perform a deeper evaluation itself or ask a third party to do so.



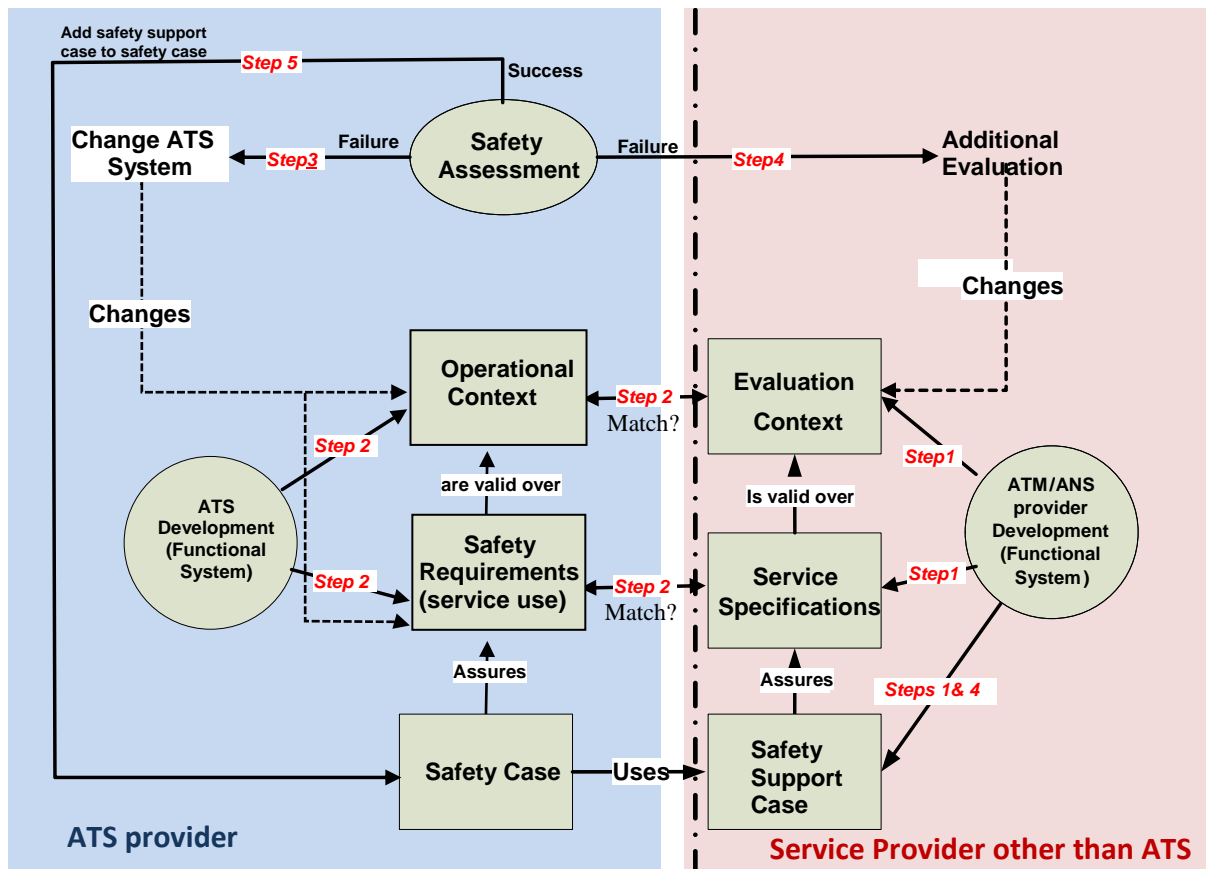


Figure 24: Interactions in a multi-actor change as result of an unsolicited change by a service provider other than traffic services provider

(e) Example of case 2:

- (1) For instance, when a Surveillance provider wants to change the format of the data fields it provides to an air traffic services provider, e.g. from UK CAA format to ASTRIX format, the safety support case is used to demonstrate to that the data will be delivered as specified (Service Specification) over the interface to be used to deliver the data (Evaluation Context). It should be noted that such changes will not be limited to adopting new publicly available standards or regulations. The service provider may elect to introduce new features, of their own design, to the service that is provided in the hope that it will provide a commercial competitive advantage or in response to demands made by other service providers.
- (2) Having developed the provision of the new data format, the Surveillance provider will assure itself that the Surveillance data is delivered as specified (Service Specification) in the new format over the interface to be used (Evaluation Context). The Surveillance Provider will then write down the arguments and provide the evidence for this assurance in the safety support case.
- (3) The air traffic services provider now needs to establish whether or not changes in the Surveillance data format (Service Specification) or the interface to be used (Evaluation Context) are compatible with their existing system, e.g. the Radar Data Processor can

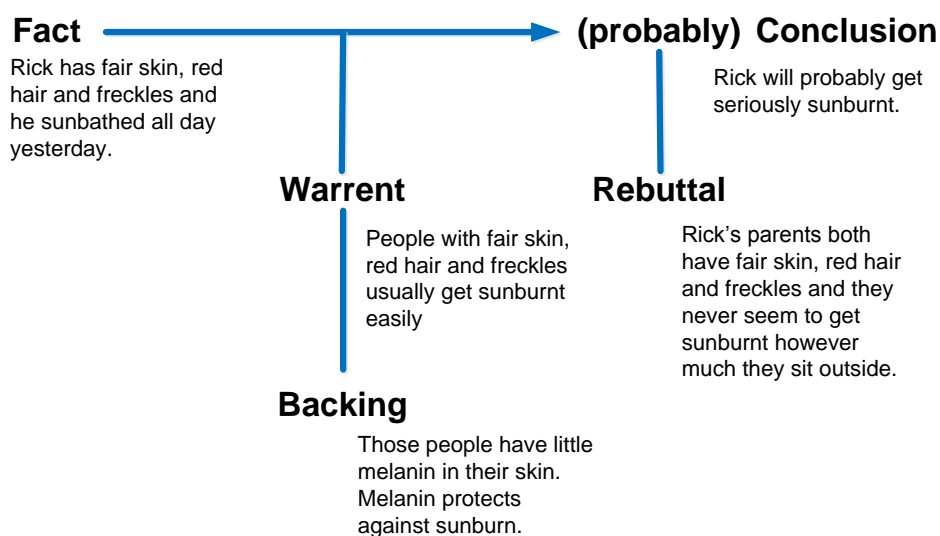
already accept either format. In this case, the new component specification matches the safety requirements and the Evaluation Context matches the Operation Context

- (4) However, the air traffic services provider may not be able to fully accommodate the change in the data format within its existing system, i.e. the Surveillance provider’s Service Specification no longer matches the air traffic services provider’s Safety Requirements or the Evaluation Context no longer matches the Operational Context. In order to achieve a successful change in these circumstances, the ATS functional system will have to be changed in order to match the new data format and interface. If the ATS system can be changed to accommodate the new Surveillance data format, then the air traffic services provider will have to change its Safety case to reflect any changes in Safety Requirements and interface (Operational Context) made as a consequence of the changed Surveillance service.

**4. SAFETY ASSESSMENT AND SAFETY SUPPORT ASSESSMENT**

**4.1. MODEL OF AN ARGUMENT**

The general shape of arguments<sup>113</sup> consists of grounds, claims, warrants, backing, qualifier and rebuttal. Claims, as the name suggests, are assertions put forward for general acceptance. The justification for the claim is based on some grounds, the ‘specific facts about a precise situation that clarify and make good the claim’. Next, the basis of the reasoning from the grounds (the facts, the evidence) to the claim is articulated. This is referred to as a ‘warrant’, which are ‘statements indicating the general ways of arguing being applied in a particular case and implicitly relied on and whose trustworthiness is well established’. The basis for the warrant may be questioned and here the notion of backing for the warrant is introduced. The confidence in the claim may also be questioned and here the notion of a qualifier is introduced, e.g. phrases such as ‘probably’, ‘possibly’ or ‘certainly’ may be used to temper or vary the confidence apparent in the claim. Finally, there may be evidence or a further argument that the warrant may not in fact be true in all circumstances. In such cases, it is said that the claim has been rebutted which is shown a ‘rebuttal’ on Figure 25.

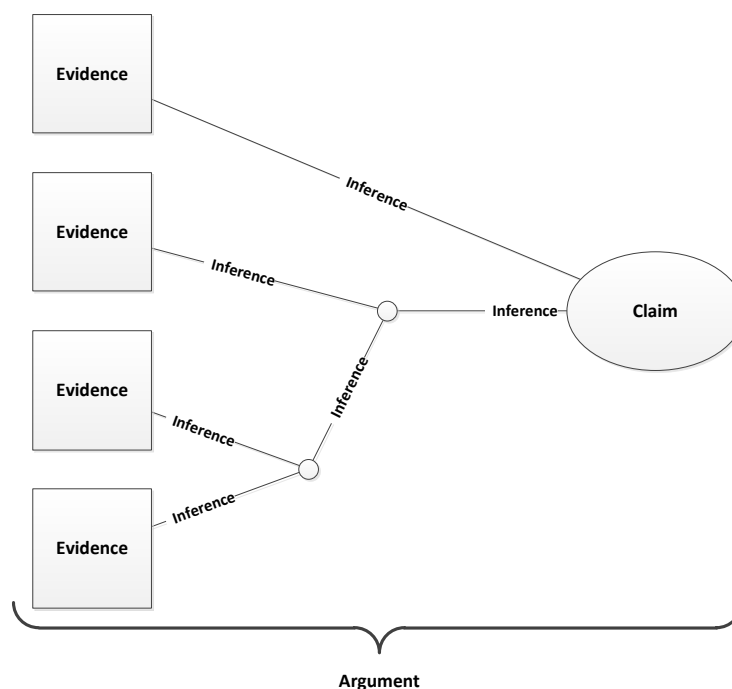


<sup>113</sup> Put forward by Toulmin in one of the first formal analyses of arguments — Toulmin's *The Uses of Argument*, 1958.



**Figure 25: The general form of an argument**

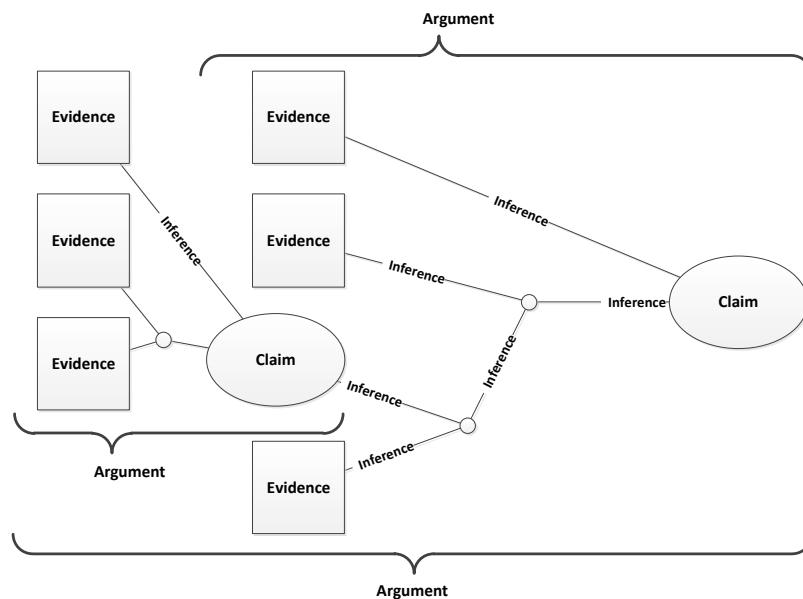
- (a) An assurance case is, in general, the argument that the provider of a service makes to demonstrate that the service meets pre-ordained criteria (the claim) with an acceptable level of confidence. It is analogous to the case that the service provider may have to make to a court following a serious challenge to the integrity or efficacy of the service.
- (b) The assurance case is an argument, its general form is illustrated below. In this diagram:
- (1) a claim is an assertion that something is true;
  - (2) evidence is the available body of facts or information indicating that the claim is true. The evidence may be directly related to the claim ('Facts' in Figure 25) or may be related to the warrant ('Backing' in Figure 25).
  - (3) An inference<sup>114</sup> is the basis of the reasoning linking the evidence ('Facts' or 'Backing' in Figure 25) to the claim. It is equivalent to the warrant in Figure 25.

**Figure 26: The general form of an assurance case**

- (c) More properly, since evidence can be replaced by a lower level argument, an assurance case is an argument that contains a hierarchy of arguments, culminating in a single claim<sup>115</sup> as illustrated below:

<sup>114</sup> Note that inference replaces warrant from the general form of an argument because the definition of inference is more suitable to the written form of argumentation used in assurance cases.





**Figure 27: The assurance case as a hierarchy of arguments**

- (d) The symbols used represent parts of the argument that are provided in the form of narrative text (claims and inferences) combined with data/facts (evidence) taken from many sources. In simple cases, all this may be contained in a single document. However, in any reasonably-sized assurance case the data will be extensive. Consequently, an assurance report is usually produced, which is a document that contains the argument structure in sufficient detail such that all the narrative and data that form a part of the assurance case may be unambiguously located. It is often the case that notations based on the diagram above are used as an index into the narrative of the assurance case and the data/facts used to support the claims made. Therefore, an assurance report can be thought of as an index for the assurance case.
- (e) Inductive and deductive arguments: An argument is deductive or inductive. An argument is deductive insofar as it is intended or claimed to be valid. A deductive argument is valid if and only if it is impossible for the conclusion to be false when its premises are true; a deductive argument is often just an instantiation of a universal principle. An example of such argument is the following one on an approach on certain airport A:
- All ILS approaches are safe;
  - The approach on runway X of airport A is an ILS approach;
  - The approach on runway X of airport A is safe.

This argument is valid, according to logic warrants, but as the first premise is not true, the argument is flawed.

<sup>115</sup> For a safety case, this is that the system is acceptably safe for a given application in a given operating context and its risk is as low as is reasonably practicable. For a safety support case, this is that the service meets its specification in a given context and does nothing else.

An argument is inductive if it is only intended to provide a reason for the claim. An inductive argument might be incorrect but should not be considered as invalid if it is intended to be a generalising inference. An example of an inductive argument is the following:

- No incidents occurred in the last 100 000 approaches on runway X of airport X;
- There were not significant changes and there will not be any significant changes of any aspects of the approaches on runway X of Nunting A;
- The approach on runway X of airport X is safe.

This argument does not claim to be valid. It intends to provide support for the claim and it can be discussed whether the support is strong enough.

- (f) The majority of arguments in assurance cases, like almost all arguments in real life, are inductive arguments. Hence, the discussion about the assurance cases is not only a discussion about its validity, but more often about the strength of the presented evidence and warrants.
- (g) It is not possible to give guidance on the complete structure of a change assurance case because it depends on the circumstances of the change and the strategies used to argue the case. This is deliberately so as it allows for the necessary flexibility in arguing in novel circumstances such as those likely to be found when introducing SESAR concepts of operation.
- (h) Since an argument contains a hierarchy of arguments, it follows that any of these arguments may be treated independently of the others and may, therefore, come from any source providing that the claim is valid in the context of its use. For example, there may be an argument about the behaviour of part of a proposed change, perhaps specifically related to a general piece of equipment or some common concept, which has already been assessed and generated by someone other than the service provider planning the change. The evidence for this argument can come from any source and may be reused in the assurance case provided it is valid and the context in which it is going to be used matches the context in which it was produced.

## 4.2 LIFECYCLE OF THE CHANGE FOR EQUIPMENT AND ASSURANCE

- (a) The life cycle of the change for equipment can be considered to consist of a number of phases:
  - (1) During the design phase, a concept is repeatedly refined until elements are described that can be built. During the refinement process, elements whose characteristics are proposed are analysed to show that, given a perfect build, the change will behave as intended. This design phase may include building models of some of the elements (particularly software in a host environment) in order to gain confidence that the design will behave as intended.
  - (2) At some point there is sufficient confidence in the design to start building the equipment, i.e. to manufacture the equipment that will be used in service. This implementation phase consists of building equipment, testing it, usually in isolation, then integrating it with other pieces of equipment and testing the integration as a whole.
  - (3) Testing software on a host that is not part of the final system implementation is considered to be part of design.
- (b) Design assurance, therefore, is argued from the evidence gathered during the development of elements or their constituent parts. The design assurance demonstrates that constructs known to be prone to error or constructs for which the behaviour cannot be predicted, are prevented from being included in the design. Design assurance also demonstrates that only the design intent will be implemented.



- (c) Implementation assurance is argued from the evidence gathered by testing the elements or their constituent parts.
- (d) Evidence about the design of an element is gathered from inspecting and analysing the design of the constituent parts of the element, e.g. computer programmes, whereas evidence about the operation of the element is gathered from testing the constituent part, e.g. software.
- (e) Typically, for design assurance and implementation assurance, following industry standards helps in the gathering of evidence.

#### 4.3 DEGRADED MODES OF OPERATION

- (a) The following guidance deals with the safety and safety support assessment associated with degraded modes of operation; it, therefore, applies to the assessment of all components of all functional systems (people, procedures, equipment (software & hardware)) and includes how training for personnel should be addressed, the degraded modes of operation of the services delivered to functional systems and the specification of the degraded modes of operation of the functional systems. The work involved, described below, is considered to be part of the assessment of the change and does not require separate safety or safety support assessments.
- (b) The scope of the change includes all planned degraded modes. Degraded modes occur for two reasons:
  - (1) The service behaves incorrectly or is incomplete because of a malfunction;
  - (2) The level of the service offered varies due to maintenance activities, i.e. when repairing the functional system as a result of a malfunction or when trying to prevent a malfunction.
- (c) Malfunctions
  - (1) The service will at some point malfunction. Malfunctions result in:
    - (i) loss of function; or
    - (ii) corruption of the information associated with a service.Corruptions, may be taken as a synonym for unwanted behaviour.
  - (2) A loss implies that some necessary service or part of a service has become unavailable. A corruption implies that the system is behaving incorrectly.
  - (3) Both forms of malfunction unless covered in the assurance case of the service, would mean that the service would be behaving in a manner that had not been assessed and so the consequences of the behaviour would be unknown and therefore unacceptable. In the case of an air traffic service, the unacceptable behaviour would be safety related and could possibly be dangerous. For other services, the unacceptable behaviour would fall outside the specified behaviour<sup>116</sup> and so the assurance cases of users of the changed service would not be valid.
- (d) Planning for degraded modes

<sup>116</sup> There are no absolute criteria for what is acceptable and what is not. Agreement with users or common sense should be the main guide. For example, it is almost certain that flooding a network with data as a result of a malfunction would be considered to be unacceptable behaviour.



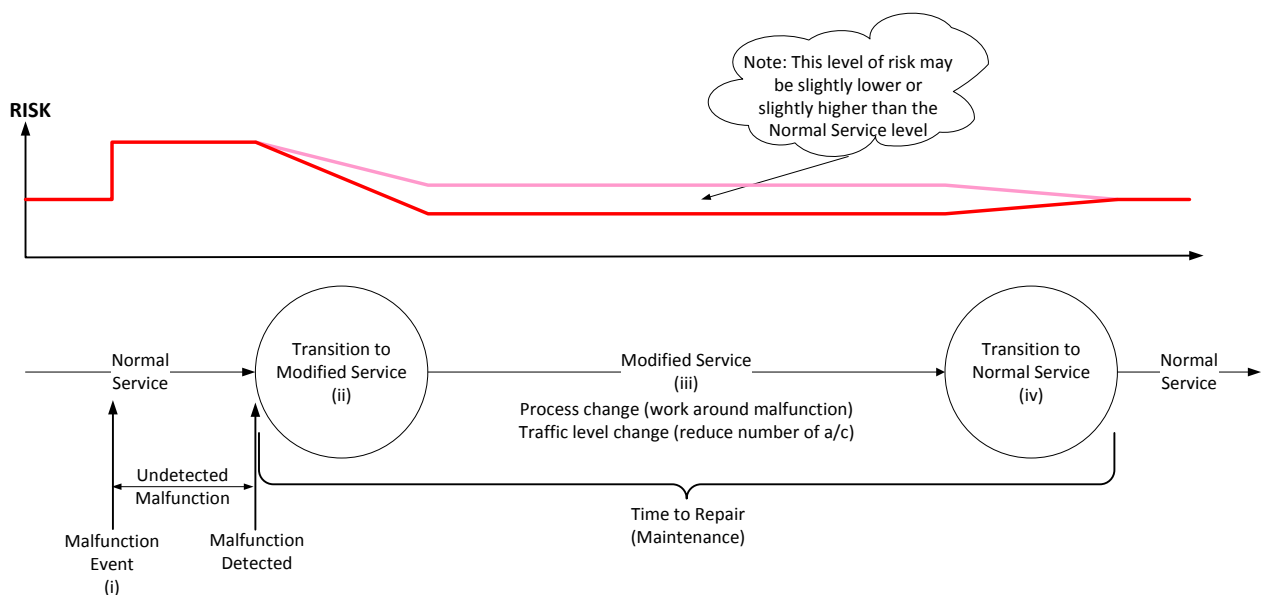
- (1) In order to be confident that the service will remain acceptable, even though malfunctions occur, all conceivable malfunctions associated with the change should be identified, their behaviour assessed and any necessary responses identified, i.e. malfunctions and their associated behaviours are foreseen and mitigated.
  - (2) Mitigation takes the form of maintenance and operational procedures that come into play either periodically or when a malfunction is identified. These procedures are considered further below. The assessments have to consider these procedures and show that while the service being delivered is not the normally intended service, it is nonetheless acceptable. Consequently, the behaviour associated with these procedures also needs to be assessed and they must be shown to correctly mitigate unacceptable variations in the way the service behaves as a result of the malfunction, i.e. they need to be proposed, designed, validated, assessed for their impact on the way the service behaves and their implementation verified.
  - (3) Note that not all the behaviour induced by a malfunction can be accurately or completely described. Consequently, in mitigating the unacceptable behaviour associated with a malfunction, the time between the onset of the malfunction and the point at which the maintenance activity mitigates this behaviour, i.e. it becomes acceptable, may be significant. In such cases, the means of automatically detecting some malfunctions may need to be designed into the service in order to decrease this time to a point where the risk associated with the undescribed behaviour is acceptable.
  - (4) Planned degraded modes can, therefore, be considered to be those modes of operation where maintenance activities are occurring due to the presence or potential presence of malfunctions and where the behaviour associated with the degraded mode of operation is considered to be unacceptable in the long term, i.e. there is a need to return to the normal (intended) service.
- (e) Maintenance is of three forms:
- (1) On condition maintenance — an element within the functional system has failed or will fail imminently and needs to be replaced with an identical element. Notice that replacing an element with a different element is a change, it is not maintenance and so it requires a new assessment.
  - (2) Preventive maintenance — the operational performance will degrade sometime in the future if maintenance is not performed. This may also be called periodic maintenance, since in order to preserve the future performance of the system, it is performed periodically, usually at regular intervals.
  - (3) Maintenance of configuration — operational performance is not assured if an element of the functional system or its architecture deviates from that which was evaluated during the assessment and justified in the assurance case.
- ‘Maintenance’ is not meant to be restricted to ‘technical systems’. It applies to all the constituents of the functional system: procedures, people and equipment (hardware & software). In that sense, preventive maintenance applied to people should be understood as refreshment training.



## (f) On condition maintenance

- (1) Maintenance activity results from the detection of the malfunction. In general, the loss of a function of the service is usually detected when it happens, whereas corruption may not be detected for some time and then only as a result of an incident occurring.
- (2) Prior to the malfunction, the user receiving the services is supported by the full range and capability of the services offered. After the malfunction is detected and the faulty part isolated and removed from service, the range or level of services offered may necessarily need to be reduced as the functional system, now available, is incomplete.

The diagram below shows how risk<sup>117</sup> might vary during a malfunction and the processes through which the malfunction is managed.



**Figure 28: Level of risk during malfunction**

- (3) It can be seen that the processes following a malfunction encompass the following phases:
  - (i) The malfunction occurs, but may initially be undetected.
  - (ii) The malfunction is detected and the service is modified to account for the malfunction<sup>118</sup>.
  - (iii) A modified service is performed while the cause of the malfunction is investigated and put right.
  - (iv) Once the malfunction has been put right, the functional system is restored to its normal state and the normal service is resumed.

<sup>117</sup> The diagram and the explanation below is written from the perspective of an air traffic service. However, it is equally relevant to other services, i.e. the rationale is the same and so should be the approach adopted, except that the malfunction affects the service delivered directly and safety indirectly. If a service other than an air traffic service has a malfunction then, since that service will be used, in some form, by an air traffic service, it will affect the safety of one or more air traffic services.

<sup>118</sup> Note that in some circumstances the detection of a malfunction may result in an automatic isolation of the faulty part and indication to the operators that degraded mode operational procedures should be put in place. The physical removal and repair of the faulty part may, therefore, be delayed and does not necessarily coincide with the onset of the degraded mode operational procedures.

- (4) Clearly, safety risk rises (possibly considerably) during the time the malfunction is undetected. It then falls to an acceptable level, which may be lower or higher than the normal level of risk, as the modified service is introduced. This is not instantaneous, as it will take time to change the navigation plans of all the affected a/c, alert them, convey new instructions and allow them to adjust their flight paths, if necessary<sup>119</sup>. Furthermore, if it is necessary to reduce the number of a/c receiving the service in order to reduce the risk to an acceptable level, then it will take some time to establish the new level of traffic.
- (5) During a malfunction, two kinds of processes will be in use:
- (i) The process to identify, isolate, repair and replace the elements causing the malfunction; and
  - (ii) The operational process needed to mitigate the effects of the malfunction and its repair and to restore services to their normal levels once the malfunction has been repaired.
- (g) Preventative maintenance
- (1) In general, mechanical elements, such as radar heads, degrade with use and will, at some point, fail. In order to prevent their future failure, these elements are maintained periodically to restore them to such a condition that they will continue to operate until the point at which the next maintenance occurs.
  - (2) During maintenance, the range or level of services offered may necessarily need to be reduced as the functional system, now available, is incomplete. Consequently, two kinds of processes will be in use:
    - (i) The process to isolate and bring back the elements being maintained to their intended condition and then to return them to operational service; and
    - (ii) The operational process needed to mitigate the effects of the removal of the elements being maintained and to restore services to their normal levels once the maintenance has been completed.
- (h) Procedure development

The procedures governing the processes identified in (f) and (g) above, i.e. those associated with maintenance (i) and with operational use during maintenance (ii) are part of the change and must be proposed, designed, validated, their implementation verified and their effects on the behaviour of the service assessed. The circumstances of their use, their desired content and any refreshment training needed, together with the periodicity of refreshment, form the maintenance requirements for the change, i.e. they form the requirements for degraded modes of operation.

- (i) Maintenance of configuration
- (1) Although not generally regarded as a maintenance activity, it is, nonetheless, important to maintain the configuration of the change during the time it is operational.

---

<sup>119</sup> In the case of a service other than an air traffic service, the time taken relates to the time it takes to isolate the faulty part and introduce mitigating procedures i.e. ones that deliver a service, which although incomplete, is an acceptable service for the time it takes to repair the malfunction.



- (2) The validity of the assurance case is predicated on the declared configuration of the changed functional system if the configuration were to change the way the service behaves, e.g. via adjustments, modifications or patches (including software updates and configuration/parameter changes), introduced (perhaps with good intent) by errant personnel and malicious modifications such as those introduced by vandalism or malware. It will be uncertain and so the assurance case would become invalid and the behaviour of the change will not be assured. Such uncertain behaviour can be considered to be unacceptable and needs to be mitigated, i.e. the maintenance of configuration should be treated as preventive maintenance.
- (3) Maintenance of configuration will usually be covered by the management system/safety management system procedures of the service provider; however, as part of the change, these should be assessed to verify that they cover configuration management for the proposed change. The assessment should verify that the change does not include some new element or arrangement of elements, e.g. ones using new technology, whose configuration cannot be verified using the current management system/safety management system procedures.

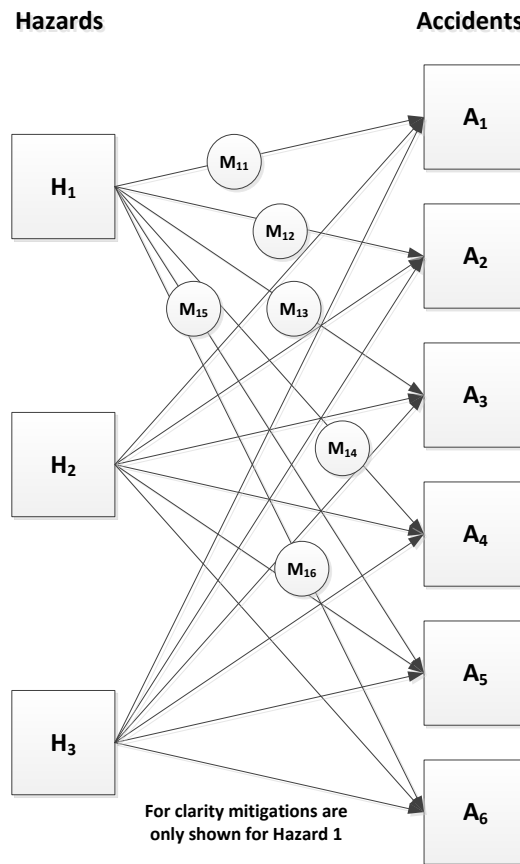
## 5. RISK ANALYSIS AND EVALUATION

### 5.1. RISK ANALYSIS IN TERMS OF SAFETY RISK

#### 5.1.1. Hazards and accidents

- (a) A hazard may lead to several accidents. For example, at a junction of a taxiway and a runway the hazard of an aircraft going outside a protected piece of airspace, e.g. failure of the aircraft to stop at an intersection of taxiways, when expected to do so, could lead to an accident with a low speed aircraft, a high speed aircraft or an airport vehicle. Also, an accident may be caused by several hazards. For example, in the same circumstances, the collision of two aircraft at the junction could be caused by a failure of both aircraft to stop at different intersections, when expected to do so. This leads to the general hazard/accident model shown below:

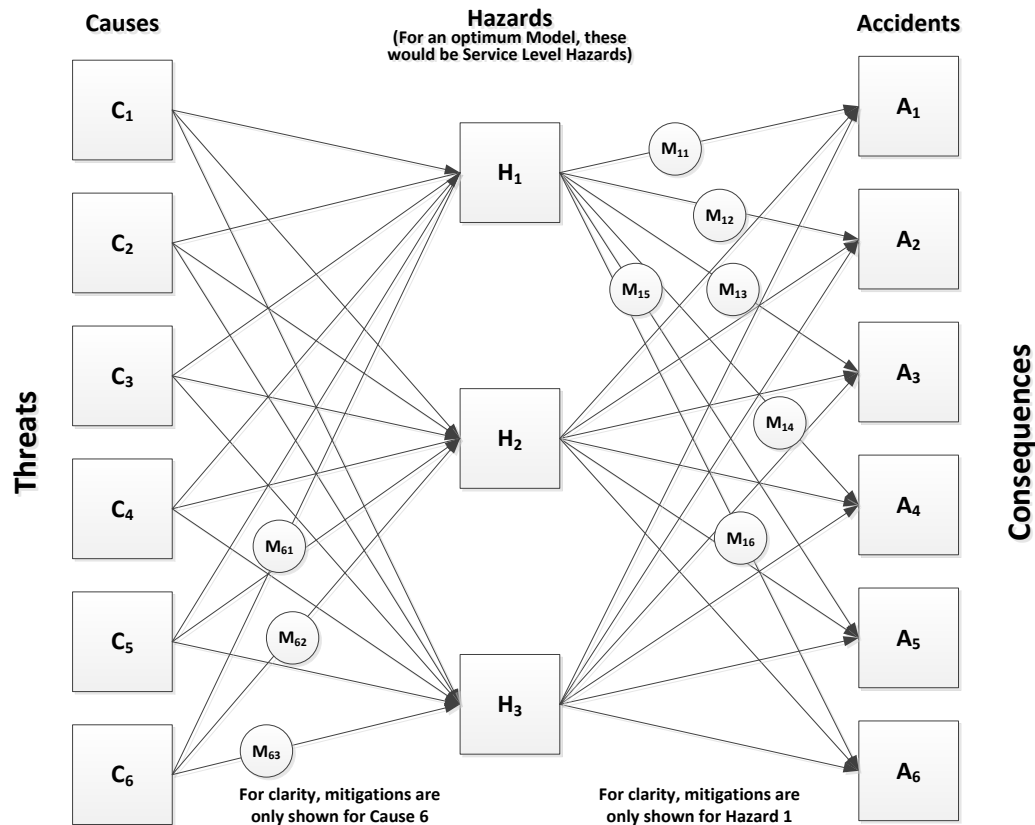




- (b) In general, there are many causes for a hazard and some of those causes may be common to a number of hazards, e.g. the same flawed procedure may be used for controlling taxiing aircraft over many different routes and so it may contribute to service level hazards (see (3) below) at particular points on each route or for particular circumstances during each transit over a different route. Consequently, a complete generalised model of the relationships between causes, hazards and accidents may be formed as illustrated below:







Note that causes are also hazards but are called ‘causes’ here to differentiate them from the hazard of interest (Service Level Hazard — H<sub>n</sub>).

- (c) In any reasonably sized change, there may be many causes, many hazards and many accidents. In these circumstances, it may be more convenient and less confusing to work on a single hazard at a time. The Bow Tie Model represents an appropriate way of doing this. The bow tie is a simplified representation of the conjunction of a fault tree and an event tree with the cause of accidents on the extreme left of the bow tie and the accidents on the extreme right of the bow tie. The Hazard of interest or hazard point (the knot in the bow tie) can be declared to be anywhere between these two points, i.e. where the fault tree stops and the event tree starts is a modelling decision. For optimum efficiency/effectiveness, the Hazard of interest should be declared at the point where a service is delivered (Service level hazard) as it gives the fewest hazards to manage. If the Hazard of interest is set too far to the left, resources may be wasted and mistakes may be made assessing an explosion of hazards that in fact have common higher level hazards. Positioning the hazard point too far to the right can result in real accident trajectories being missed. Therefore, positioning the centre of the Bow Tie at the right hazard is important for an efficient and correct risk analysis.
- (d) An accident trajectory is a chain of events starting with a hazardous event and terminating in an accident. At each event, it may be possible to arrest the progress along the accident trajectory and, thus, avoid the accident, i.e. these events may be used to trigger activities that reduce the effective probability or frequency of an accident. These activities are called ‘mitigations’ and are



shown above as a single mitigation. In reality, at each event, there could be considered to be an individual mitigation, each one of a different form. There can be two outcomes of a mitigation:

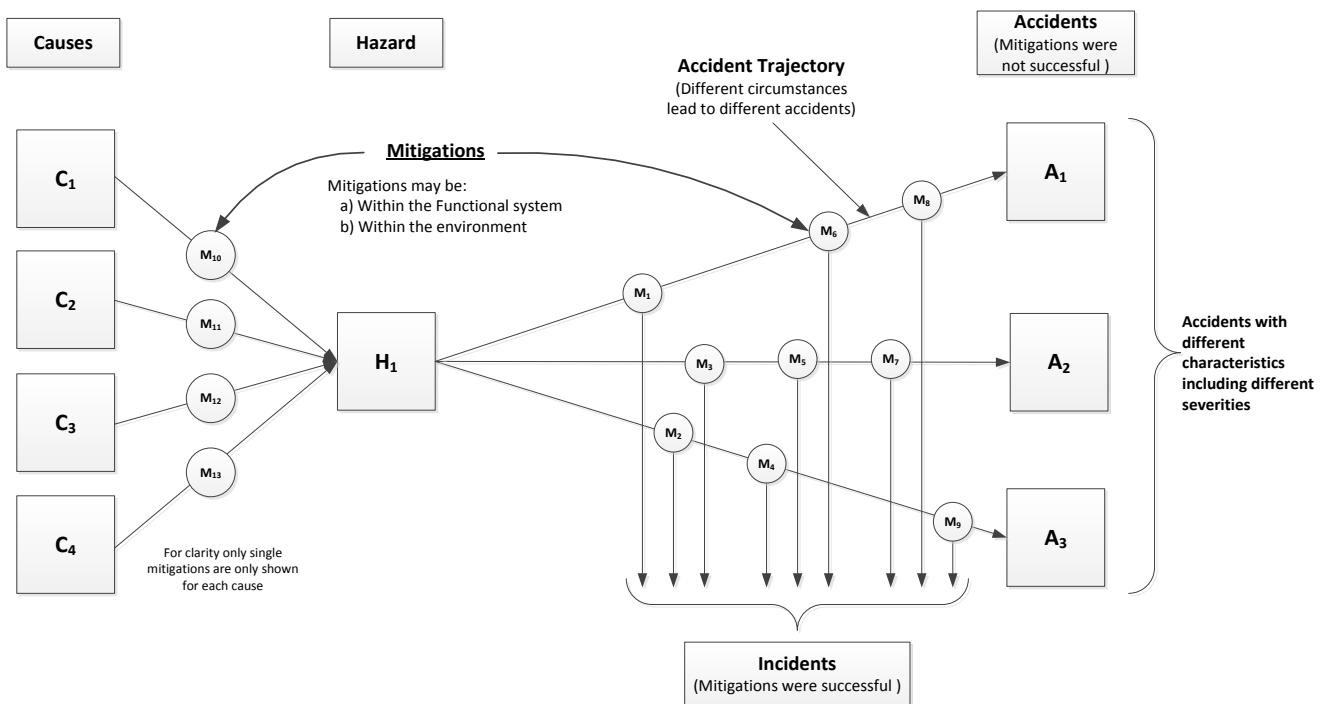
- it fails and so progress towards the accident continues; or
- it succeeds and so progress is arrested and the accident does not happen.

In the second case, an incident occurs.

Note 1: In these circumstances, an incident is bound to occur since the hazard itself is an unwanted event and any terminal event between the hazard and the accident should be considered as an incident.

Note 2: While an incident is considered to be a terminal event, it is, of course, possible for an incident to be the start of another, different, accident trajectory, e.g. an aircraft performing a go-around, as a result of one hazard, may fly into the path of another aircraft, thus, creating a new hazard, the result of which may, if not mitigated, be an accident involving the go-around aircraft and the other aircraft. In this respect, the Bow Tie Model is a simplification and care should be taken to account for such compound accident trajectories when using it.

Consequently, the full Bow Tie Model is as shown below:



**Full Cause/Hazard/Accident Model (Bow Tie Model)**  
 (for one hazard)

Mitigations between causes and hazards, shown above as a single mitigation, may also comprise a number of mitigations, although this expansion is not shown on the diagram. The successful outcome of these mitigations is not usually considered to be an incident because the hazardous event will not happen if the mitigation is successful.

- (e) Care should be taken when using the Bow Tie Model to remember that it represents only a single hazard and there will be many hazards associated with the change. Moreover, each accident may be a result of more than one hazard. Consequently, steps should be taken to assess the



implications of both common cause and common mode effects, for the complete part of the system involved in the change, when related to the risks identified in each Bow Tie Model used.

### 5.1.2. Severity schemes

The severity determination should take place according to a severity classification scheme. This section provides guidance on such schemes.

(a) Severity schemes resulting in a single value of risk

The accident/incident severity scheme commonly used in ATM/ANS is the one reproduced below:

Severity Class	Effect on operations
1 (Most severe)	Accident as defined in Article 2 of Regulation (EU) No 996/2010 <sup>120</sup>
2	Serious incident as defined in Article 2 of Regulation (EU) No 996/2010
3	Major incident associated with the operation of an aircraft, in which the safety of the aircraft may have been compromised, having led to a near collision between aircraft, with ground or obstacles.
4	Significant incident involving circumstances indicating that an accident, a serious or major incident could have occurred if the risk had not been managed within safety margins, or if another aircraft had been in the vicinity.
5 (Least severe)	No immediate effect on safety.

- (1) If this scheme is used, then only severity class 1 can be used in safety risk analysis and safety risk evaluation<sup>121</sup>. This is because only events that can be classified as severity class 1 could possibly cause harm to humans<sup>122</sup>. This is in contrast to the severity classification scheme used for aircraft certification, where the first three classes can cause death or physical injury to humans. In the scheme above, the risks evaluated would always be proportional to the frequency or probability of the harmful event and there would be no

<sup>120</sup> Regulation (EU) No 996/2010 of the European Parliament and of the Council of 20 October 2010 on the investigation and prevention of accidents and incidents in civil aviation and repealing Directive 94/56/EC (OJ L 295, 12/11/2010, p. 35).

<sup>121</sup> However, the whole table (rows 1 to 5) may be used in accident/incident analysis and rows 2 to 5 may be used in accident precursor analysis, which can be used to validate risk analysis. See (d), for a fuller treatment of validating risk analyses.

<sup>122</sup> It should be noted that when single-valued severity schemes are used, the loss of an aircraft usually replaces the concept of harm to humans.



possibility of comparing harmful events with different consequences. For example, a mid-air collision involving two large commercial airliners would have the same, i.e. it would be placed in the same, severity class as a similar accident, with the same probability of occurrence, involving small aircraft carrying one or two passengers each and so the safety risk of the two events would be the same.

- (2) Another instance where the consequences of harmful events, i.e. accidents that may harm humans, cannot be distinguished using this severity scheme is where the harmful events occur at very different speeds. For example, an accident to an aircraft on a low speed taxiway would have the same severity as an accident to the same aircraft in mid-air. The likely harm caused to the passengers would be very different in each case, but the risk would be the same<sup>123</sup>.
- (3) In these circumstances, risk analysis would actually be reduced to frequency/probability analysis.

(b) Multiple risk value severity schemes

- (1) The purpose of a severity classification scheme is to facilitate the management and control of risk. A severity class is, in effect, a container within which accidents can be placed if their severities are considered different and to fall within the bounds defined by the severity class. Each container can be given a value which represents the consequences, i.e. small for accidents causing little harm and big for accidents causing a lot of harm. The sum of the probabilities of all the accidents assigned to a severity class multiplied by the value that is related to the severity class is the risk associated with that class. If the value that represents severity for all classes is scalar, then the total risk is the sum of the risks in each severity class.
- (2) Note that a scalar is tangible property that is expressed as the product of a measurable numerical value and a physical unit, not merely a number. The quantity does not depend on the unit, e.g. for distance, 1 km is the same as 1 000 m, although the number depends on the unit. Examples of common scalars include cost, mass, volume, time, speed and temperature.
- (3) Severity classes facilitate the management and control of risk in a number of ways. At the simplest level, the distribution of accidents across the severity classes gives a picture of whether the risk profile of a system is well balanced. For example, many accidents in the top and bottom severity classes with few in between suggests an imbalance in risk, perhaps due to an undue amount of attention having been paid to some types of accident at the expense of others. More detailed management and control of risk includes:
  - (i) Severity classes may be used as the basis for reporting accident statistics. For example, in reports by a regulator to government.
  - (ii) Severity classes combined with frequency (or probability) classes can be used to define criteria for decision-making regarding risk acceptance. For example, decisions regarding low severity/low frequency risks might be made at a project level whereas

---

<sup>123</sup> That is, of course, assuming that the probability of the two events was the same.



acceptance of high severity/moderate frequency risks may be made only at the highest level of an organisation.

- (iii) The total risk associated with one or more severity classes can be managed and controlled so that it satisfies regulatory and/or shared managerial objectives. For example, the sum of the risk from all severity classes represents the total risk and may be used as a basis for making decisions about changes.
- (iv) Similarly, the risk associated with accident types of different levels of severity can be compared, giving the organisation the opportunity to manage the distribution of risk. For example, comparing runway infringement accidents with low speed taxiway accidents would allow an organisation to focus their efforts on mitigating the accident type with greatest risk.

(c) Attributes of multiple risk value severity schemes

- (1) Because of their role in managing and controlling risk, severity classes must be suitable for their intended application. What is good for one situation may not be good for another.
- (2) The criteria that can be used to assess the suitability of a multiple value severity scheme are given in point (f) of AMC1 ATS.OR.205(b). In addition, it should be noted that criterion 5 supports criterion 2 and the two may be regarded as a complementary pair. Criterion 2 states, in effect, that for any given accident it must be possible to assign it to a severity class, i.e. there should be no 'orphan' accidents and that it must not be possible to assign it legitimately to more than one severity class. Criterion 5 states that the assignment should be made on the basis of rules such that there can be no doubt or difference of opinion as to which severity class an accident should be assigned.
- (3) To illustrate the distinction between these criteria, consider a severity classification scheme that has two classes: (x) 1 death; (y) from 2 to 100 deaths. This does not satisfy criterion 2 for accidents involving aircraft since an accident involving 120 deaths cannot be assigned to a severity class. Criterion 2 would, however, be satisfied by a scheme with the two classes: (x) 1 death; (y) 2 or more deaths. The scheme would not satisfy criterion 5, however, without some rules. For example, an accident involving one death and five severe injuries as its immediate consequences might be assigned to severity class (x) on the basis of the single death. However, if it were judged that some of the serious injuries would be significantly life shortening, then it might be argued that these premature deaths should be counted as deaths due to the accident and the accident assigned to severity class (y). Similarly, when accident consequences are calculated, the assignment to a severity class might vary according to whether the most likely or maximum credible number of deaths is used.
- (4) Of course, it might not be possible for a specific scheme to have all six criteria strongly represented. If that is the case, then they need to be prioritised. For example, consistency with societal views of accident severity (criterion (6)) might need to be a high priority for an industry or activity that is the subject of much public (and media) attention.

(d) General multiple risk value severity scheme

An example of a general severity scheme that supports multiple levels of risk is given below.



Severity of harm			
Severity class	Harm to people <sup>124</sup>		
	Fatalities	Serious injuries	Minor injuries
1	101–1 000		
2	11–100	101–1 000	
3	1–10	11–100	101–1 000
4		1–10	11–100
5			1–10

Another example for classifying the severity of harm could be to use the established number of passenger capacity used for certification of aircraft (more than 9 pax and more than 19 pax) and for the operational rules for passenger evacuation (50 or more pax).

Severity of harm			
Severity class	Harm to people <sup>125</sup>		
	Fatalities	Serious injuries	Minor injuries
1	> 49		
2	10–49	> 49	
3	1–9	10–49	> 49
4		1–9	10–49
5			1–9

A further example for classifying the severity of harm is derived from EUROCAE ED-78A, and is shown below. This example uses a coarse scale that limits the number of distinct severity categories. This scheme does not, in ATM/ANS, fully satisfy criterion 2 (in point (f) of AMC1 ATS.OR.205(b)) since it would be difficult to allocate an accident, which caused a large number of injuries but few deaths, to a unique category. This could be resolved by providing a fuller description of the level of harm to be included in each category.

Severity of harm

<sup>124</sup> Strictly speaking, these injuries are additive, e.g. if an aircraft carrying 100 people collided with a large building, killing most of them and causing, additionally, several hundreds of serious injuries, then, in all probability, rather than severity class 2, the accident would be a severity class 1 accident.

<sup>125</sup> Strictly speaking, these injuries are additive, e.g. if an aircraft carrying 49 people collided with a large building, killing most of them and causing, additionally, several hundreds of serious injuries, then, in all probability, rather than severity class 2, the accident would be a severity class 1 accident.

Severity class	Harm to occupants <sup>126</sup>
1	Multiple fatalities
2	Serious or fatal injury to a small number of passengers or cabin crew
3	Physical distress, possibly including injuries
4	Physical discomfort
5	Inconvenience

In all the above examples, the relationship between the number of injuries and the number of deaths is not justified<sup>127</sup> here, but would have to be justified by any air traffic services provider proposing to use such a scheme.

Schemes such as these do not, in ATM/ANS, fully satisfy criterion 4 (in point (f) of AMC1 ATS.OR.205(b)) since it will not be easy to predict precisely how many deaths and injuries would result from an individual accident. However, the probable mix of traffic will be known (or can be established) and the type of accident predicted will lead to an approximation of the harm. For example, a mid-air collision between two large aircraft would fall into severity class 1, whereas a low speed taxiway accident between two GA aircraft is likely to fall into severity class 4 or 5, in the case of the first two schemes and into severity class 3 in the case of the last scheme.

(e) Severity schemes using equivalence classes

In order to simplify the scheme and to make it more appropriate for ATM/ANS use, it is feasible to use some other attribute of an accident to represent the number of people harmed, i.e. the attribute can be used as an equivalence class for harm to people. Typical equivalence classes could be:

- (1) aircraft size;
- (2) speed of accident; and
- (3) a combination of (i) & (ii).

For example:

<p><b>Severity of accident</b></p> <p>(using aircraft size as an equivalence class to harm)</p>
---

<sup>126</sup> Strictly speaking, class 4 and 5 could not be used in safety risk assessment.

<sup>127</sup> However, the ratio of injuries to deaths is commonly used in the railway industry.



Severity class	aircraft size
1	<p><b>Large</b>, e.g. any aircraft<sup>128</sup></p> <ul style="list-style-type: none"> <li>➤ with a maximum certificated take-off mass exceeding 5 700 kg, or</li> <li>➤ certificated for a maximum passenger seating configuration of more than 19, or</li> <li>➤ certificated for operation with a minimum crew of at least two pilots.</li> </ul>
2	<p><b>Medium</b>, e.g. any non-large aircraft<sup>129</sup></p> <p>with a maximum certificated take-off mass exceeding 3 175 kg, or certificated for a maximum passenger seating configuration of more than nine.</p>
3	<p><b>Small</b>, e.g. any other aircraft.</p>

<sup>128</sup> The 5 700 kg or 19 pax or 2 pilots is from the definition of complex motor-powered airplane in Regulation (EC) No 216/2008.

<sup>129</sup> The 3 175 kg or nine pax is from the definition of complex motor-powered helicopters in Regulation (EC) No 216/2008.





Another example could be to use aircraft size as per AC23.13091E as an equivalence class to harm as shown below:

<b>Severity of accident</b> (using aircraft size as per AC23.13091E as an equivalence class to harm)	
<b>Severity class</b>	<b>Class of airplane as per 23.1309-1E</b>
1	<b>Class IV</b> , e.g. commuter aircraft and above
2	<b>Class III</b> , e.g. SRE, STE, MRE, or MTE greater than 6 000 pounds
3	<b>Class II</b> , e.g. STE, MRE or MTE less or equal than 6 000 pounds
4	<b>Class I</b> , e.g. SRE less or equal than 6 000 pounds

These schemes could be used in constant speed environments, e.g. airways or TMAs, where there is a mix of traffic types. The risk associated with accidents of the same type would be evaluated according to the proportion of each size of aircraft in the environment and the probability of the accident and of the probability it would happen to an aircraft of the size allocated to the severity class.

In cases where the aircraft are largely of the same size, the severity scheme shown in (d)(1) could be used or the scheme above used, but only one row would be relevant.

<b>Severity of accident</b> (using accident speed as an equivalence class to harm)	
<b>Severity Class</b>	<b>Speed of accident</b>
1	<b>High speed</b> , e.g. Mid-air collision, CFIT, Runway
2	<b>Medium speed</b> , e.g. High speed taxiway
3	<b>Low speed</b> , e.g. Low speed taxiway

This scheme could be used where the speed range of aircraft is large, but the size of the aircraft is fairly constant, e.g. in an airport environment dealing only with small aircraft. If the environment is amenable to being split into non-overlapping speed zones, then this severity scheme would allow the organisation to manage the risks in the different zones appropriately.

In cases where the aircraft largely operate at roughly the same speed or the speed zones overlap, the severity scheme shown in (d)(1) could be used or the scheme above used, but only one row would be relevant.



### 5.1.3. Combining severity schemes

Severity schemes may be combined to give greater granularity, greater coverage or to make them more appropriate to the context in which they are used. The example given in section (d)(4) was an early example of a combined severity scheme. It combined the severity classes relating to death with two other severity classes relating to different levels of injury. This allows the severity classification scheme to be more appropriate in circumstances where accidents usually involve large numbers of people, but can also result in a mix of the types of harm caused, depending on the circumstances of the accident and often the vehicles involved.

(a) Mixed traffic environments

<b>Severity of accident</b> (using aircraft size and speed as an equivalence class to harm)				
<b>Severity class</b>	<b>A/C speed</b>			
	<b>High speed</b>	<b>Medium speed</b>	<b>Low speed</b>	
1	Large			<b>A/C Size</b>
2	Medium	Large		
3	Small	Medium	Large	
4		Small	Medium	
5			Small	

Where there is both a mixed speed and mixed aircraft size environment, e.g. a medium-sized aerodrome handling GA traffic as well as commuter and long-haul aircraft, then the scheme shown above gives a greater level of granularity and is more appropriate for the environment than either a speed-centred scheme or a size-centred scheme.

(b) Combining accident and incident schemes

- (1) The following scheme could be used where a service provider wishes to perform safety risk analysis, accident/incident analysis and precursor analysis using a consistent classification scheme that can be used for all the different forms of analysis.
- (2) Any of the severity schemes developed in sections (d)(4) and (d)(5) could be used in place of the accident speed scheme illustrated.



Severity class	Effect on operations	
1  (Most severe)	Accident as defined in Article 2 of Regulation (EU) No 996/2010 of the European Parliament and of the Council, e.g. <sup>130</sup> : <ul style="list-style-type: none"> <li>— one or more catastrophic accidents,</li> <li>— one or more mid-air collisions,</li> <li>— one or more collisions on the ground between two aircraft,</li> <li>— one or more Controlled Flight Into Terrain (CFIT), and</li> <li>— total loss of flight control.</li> </ul>	
	Severity Subclass	Speed of accident
	A	<b>High speed</b> , e.g. Mid-air collision, CFIT, Runway
	B	<b>Medium speed</b> , e.g. High speed taxiway
	C	<b>Low speed</b> , e.g. Low speed taxiway
2	Serious incident as defined in Article 2 of Regulation (EU) No 996/2010, e.g.: <ul style="list-style-type: none"> <li>— large reduction in separation, e.g. a separation of less than half the separation minima, without crew or ATC fully controlling the situation or able to recover from the situation.</li> <li>— one or more aircraft deviating from their intended clearance, so that abrupt manoeuvre is required to avoid collision with another aircraft or with terrain (or when an avoidance action would be appropriate).</li> </ul>	

<sup>130</sup> Examples are taken from ESARR 4.



3	<p>Major incident associated with the operation of an aircraft, in which the safety of the aircraft may have been compromised, having led to a near collision between aircraft, with ground or obstacles, e.g.:</p> <ul style="list-style-type: none"> <li>— large reduction, e.g. a separation of less than half the separation minima, in separation with crew or ATC controlling the situation and able to recover from the situation.</li> <li>— minor reduction, e.g. a separation of more than half the separation minima, in separation without crew or ATC fully controlling the situation, hence, jeopardising the ability to recover from the situation (without the use of collision or terrain avoidance manoeuvres).</li> <li>— AFIS officer is not in contact with (or aware of) one of the aircraft (or vehicles in case of runway incursion). A/c (or vehicle) needs to use avoidance manoeuvres (but not at the last minute) to be able to reduce the risk.</li> </ul>
4	<p>Significant incident involving circumstances indicating that an accident, a serious or major incident could have occurred if the risk had not been managed within safety margins, if there had not been enough time to resolve the situation or if another aircraft had been in the vicinity, e.g.:</p> <ul style="list-style-type: none"> <li>— Increasing workload of the ATCO, AFIS officer or aircraft flight crew, or slightly degrading the functional capability of the enabling CNS system.</li> <li>— minor reduction, e.g. a separation of more than half the separation minima, in separation with crew or ATC controlling the situation and fully able to recover from the situation.</li> <li>— Two (or more airplanes) in TIZ. No reduction in separation or risk of collision, but the aircraft flight crew or the AFIS officer is not aware of one of the aircraft.</li> </ul>
5 (Least severe)	<p>No immediate effect on safety, e.g.:</p> <p>No hazardous condition, i.e. no immediate direct or indirect impact on the operations.</p>

- (c) Rows 1A to 1C may be used in risk analysis.
- (d) The whole table (rows 1 to 5) may be used in accident/incident analysis.
- (e) Rows 2 to 5 may be used in accident precursor analysis, which may be used to validate risk analysis.

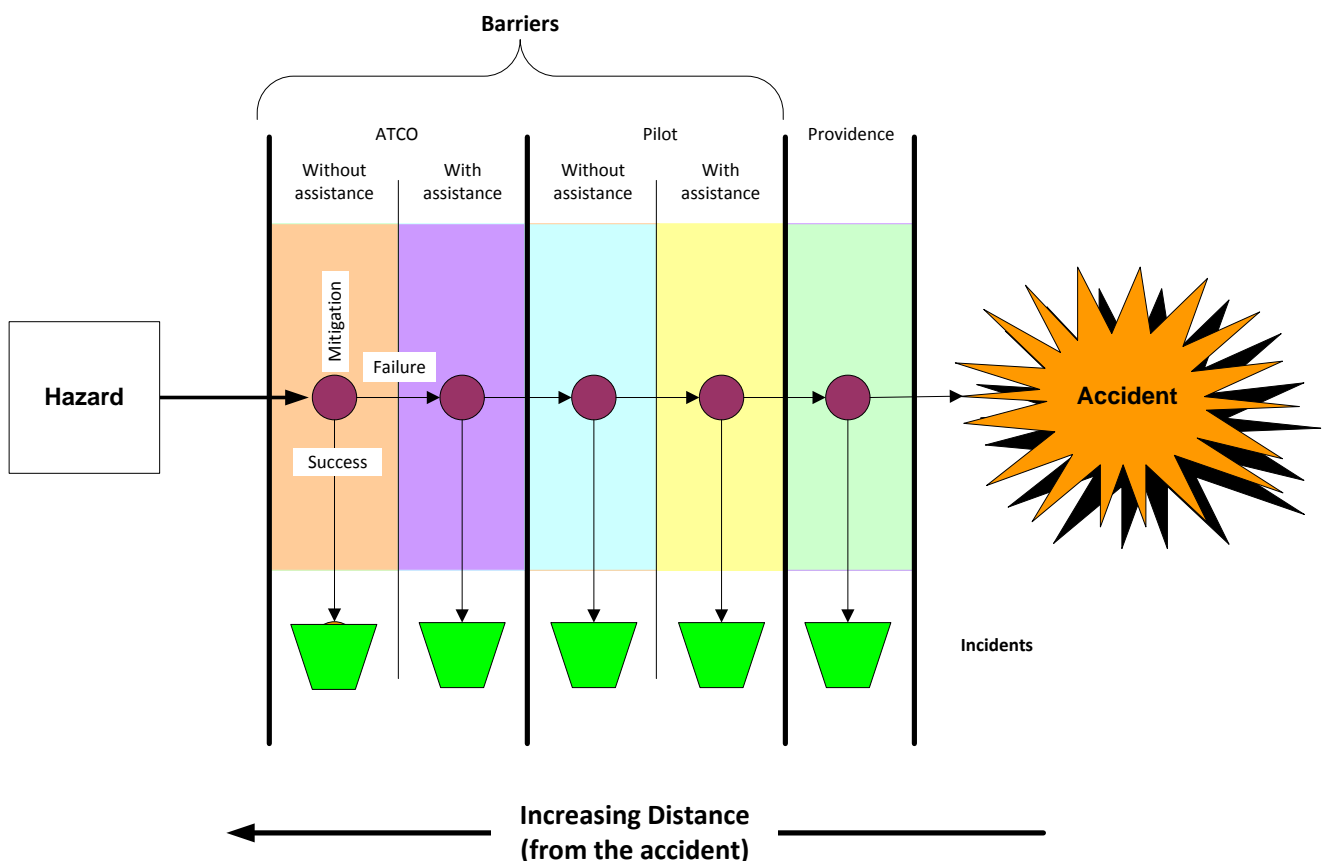
#### 5.1.4. Validating risk analyses

- (a) It can be seen from the Bow Tie Model above ((c)(4)), that accidents and incidents are terminal events, i.e. progress along the accident trajectory ceases at either an incident or an accident. It can also be seen that they involve different scalar properties. The accident scale is related to harm to people whereas the incident scale relates, in some way, to the closeness of an event to an accident. Consequently, the severity of harm to people cannot be related to the severity



associated with the closeness of an event to an accident and so, even though both may be related to risk, they are not comparable risks, i.e. two distinct measures of risk will exist.

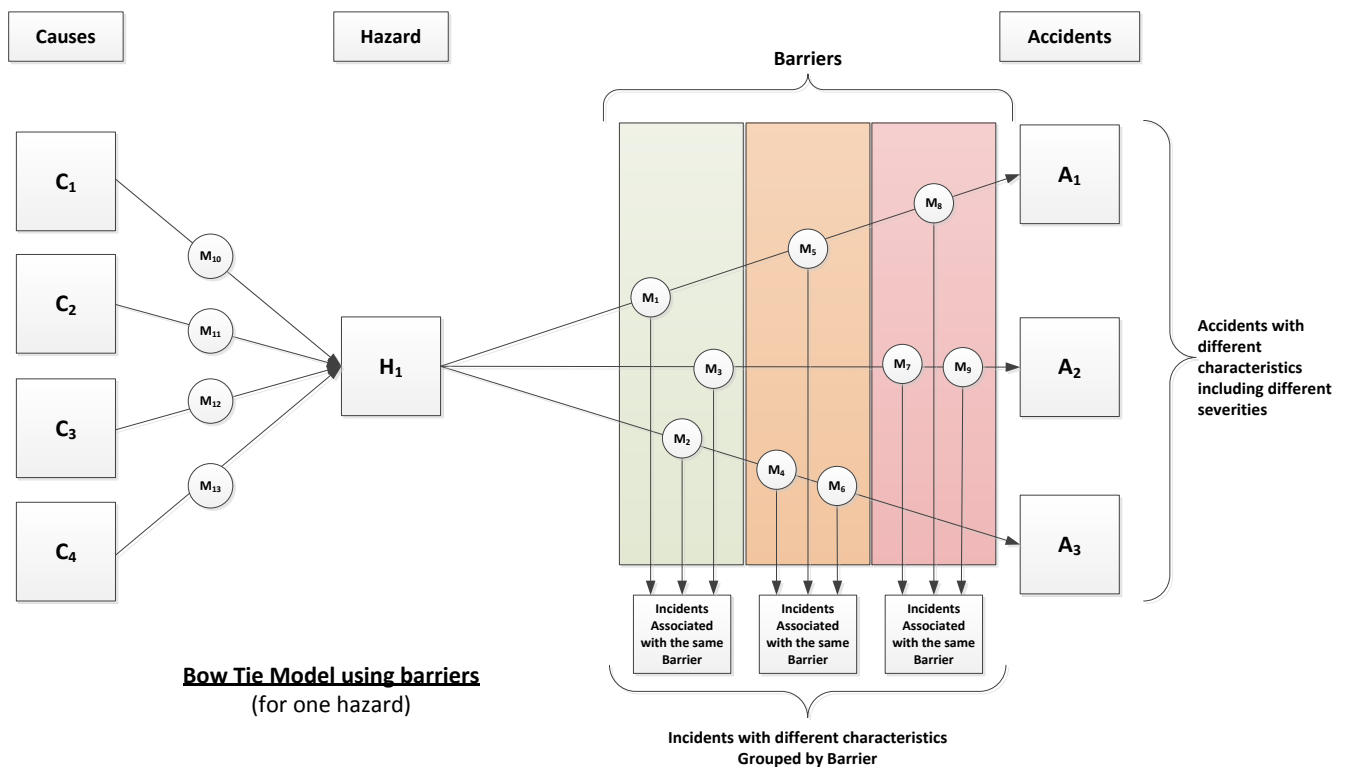
- (b) There are relatively few aircraft accidents from all causes and only a subset of them has been attributed to the services provided by a service provider. It is, therefore, unlikely that a service provider will be the cause of an aircraft accident in any given year. If the risk analysis for a change is to be based solely on safety risk, i.e. in relationship to an aircraft accident, it will be very difficult to generate any meaningful performance measures and so validate the risk analysis. Any measured data would have to be taken over decades in order to eradicate any statistical anomalies. Furthermore, even if the service provided by a service provider is the cause of an aircraft accident, this fact alone is not sufficient proof that they have not met the safety criteria, because, very much like the lottery, your number could be up tomorrow. It is, therefore, advisable to use measures different to accidents for the purposes of validating risk analyses.
- (c) The safety philosophy adopted in the air transport domain is one of fault tolerance, accepting that in general no system is perfect and so will always fail. This leads to the concept of a series of defensive barriers between a hazard and an accident, the protective nature of which is determined by the actions of mitigations. A generalised set of barriers for mid-air collision accident model is illustrated below:



- (d) The barriers are placed in the order shown because they notionally represent the barriers' 'distance' from an accident<sup>131</sup> In this context, 'distance' does not simply mean separation distance, but some notion of the likelihood of the accident if the barriers were to fail, e.g. the probability of an accident increases at each point along an accident trajectory towards the accident and so its 'distance' to the accident decreases. This should not be taken to preclude the use of separation distance.
- (e) Since in the circumstances where an aircraft is receiving a separation service, it is the ATCO who is responsible for the operation of the overall separation strategy, then he/she should have the most complete situational awareness and so be the first to spot a potential accident and resolve it ('Resolved by ATCO without assistance' on the diagram), even though the conflict may have been caused by the ATCO in the first place. If the potential for an accident is not spotted, then other systems may alert the ATCO to the potential for an accident and are, therefore, considered to be a barrier ('Resolved by ATCO with assistance' on the diagram). These systems are not necessarily 'mechanical', but could be a local ATCO or one from a different unit alerting the ATCO in charge to the circumstances. Hence, the second barrier is the 'ATCO with assistance'.
- (f) The pilot is likely to have an incomplete picture of the situation, but, nonetheless, may be aware of becoming too close to another aircraft or object. He/She may, therefore, either alert the ATCO to the potential for an accident or take avoiding action and then tell the ATCO what he/she has done. This is represented by the third barrier, 'resolved by pilot' on the diagram. In a similar manner to the second barrier, there are aircraft systems (which may include the co-pilot or the pilot of another aircraft) that alert the pilot of the impending accident with TCAS being one example. These are included in the third barrier in the diagram.
- (g) Failure of the first three barriers still does not entail an accident. Providence, shown as 'Resolved by Providence' on the diagram, will play a part in avoiding the accident. Research has suggested that in some airspaces the probability of a collision, when both ATCO and pilot barriers have failed, is approximately 300:1. Its strength relies on the generally low density of the airspace and on airspace policy.
- (h) The Bow Tie Model may be modified in order to show the relationship between the mitigations designed into an accident trajectory and the incidents resulting from the success of those mitigations, i.e. a specific incident within a specific barrier, as shown below:

<sup>131</sup> In reality, accidents and incidents do not necessarily develop sequentially (in a timeline) as suggested by the barrier model. Moreover, barriers might also occur in a different order in real incidents and accidents (e.g. the pilot can resolve a situation 'earlier' than shown in the figure above). This does not affect the generality of the model.





- (i) Incident rates are, therefore, associated with accident rates. Provided that the relationships between the incidents associated with each barrier and the accidents are well understood, and since such incidents will be far more frequent than the associated accidents, they may be used to overcome the difficulty, identified in (2), of validating the risk analysis and in giving sufficient confidence that the predicted accident rates will be achieved. Moreover, if either risk or proxies are being used in risk analysis, the design frequency of the incidents will be known and could, therefore, become some of the monitoring requirements that show continuing satisfaction of the safety criteria (ATS.OR.205(b)(7)).
- (j) Although it should be a design aim to balance the incident rates associated with different barriers, a change that makes a mitigation stronger will result in the incidents associated with the mitigation occurring at a higher rate than before. This may seem to unbalance the relationship between incident rate and distance from the accident. However, this should be of only minor concern since the risk has in fact decreased, which is a positive outcome.
- (k) The diagram shows that for some accident trajectories there may be no mitigations or more than one mitigation. The reason that there may be no mitigations is that there is a common cause associated with the hazard and the normal mitigation means, e.g. if the hazard was caused by some corruption in surveillance that also had an impact on the Short Term Conflict Alert (STCA), then there may be no mitigations in the second barrier for that particular accident.
- (l) The reason that there may be more than one mitigation within a barrier is that there may be more than one independent means of arresting the accident progression within the barrier, e.g. the use of an STCA and someone else (another ATCO or a pilot) independently alerting the ATCO to the conflict.



- (m) The ease with which a compelling and comprehensible safety case can be produced will be significantly enhanced by designing and evaluating mitigations for the change that may be used to predict the incident rate, i.e. to design for known precursors, and so it is recommended that all air traffic services providers use the concepts proposed here in their design processes.

## 5.2. RISK EVALUATION SCHEMES

### 5.2.1. Risk evaluation schemes

- (a) Risk evaluation, whether using risk or proxies, can take two forms:
- (1) Each accident is allocated a fixed target value of risk or each proxy is allocated a fixed target value of the measure associated with the proxy and the change is assessed against these targets, or
  - (2) The risk is evaluated using:
    - (i) the actual risk of each accident summed with other risks relating to the same safety criterion to form a total risk value for the associated safety criterion; or
    - (ii) the proxy value associated with each accident summed with other proxy values relating to the same safety criterion to form a total proxy value for the associated safety criterion; or
    - (iii) A combination of both the above methods.

The value of each risk or proxy value is not constrained in any other way.

- (b) The use of a fixed target for the risk associated with each accident is convenient because it is simple to use and efficient in application. However, it has the following drawbacks:
- (1) It reduces design freedom;
  - (2) The choice of target must be justified, i.e. since it effectively divides the total acceptable risk of the operation into a number of accidents (possibly of different severities), then the total number of accidents (of each severity) needs to be known.
  - (3) Targets need to be set with a significant degree of conservatism. If the targets are to be used over a significant number of changes without adjusting their values, in order to preserve the convenience and ease of use of the scheme, they must be set very conservatively. This is so that they can absorb the variations in the number of accidents that can occur at each change.
- (c) The evaluation of actual risk allows for a large degree of design freedom, simply by placing no constraints on the design other than to ensure that the risk of the change is ultimately acceptable, via compliance with the various safety criteria. However, it has the following drawbacks:
- (1) It may lead to a number of design iterations. This would occur if the design were not sufficiently conservative and so make it likely that it would not meet the safety criteria during the first iteration.
  - (2) Some constraints on the variation in risks across the range of equivalent accidents may be necessary in order to give a well-balanced distribution of risk or to alleviate societal concerns. For example, it may not be appropriate to allow a single accident to occur very





much more often than other accidents in the same severity class even though the total risk is acceptable.

The design of mitigations that achieve known predictable incident rates is still a recommended feature of the design of the change when this form of risk evaluation is used.

- (d) Some fixed risk evaluation schemes do not use safety risk, but use the notion of 'distance' from an accident as the severity scale and may set targets for incidents as well as accidents. Such schemes have additional drawbacks:
- (1) The target for accidents is not safety risk-based and so risk-based comparisons cannot be performed making it difficult to alleviate societal concerns.
  - (2) The scalar used for 'distance' from accidents needs to be defined and justified.
  - (3) Additional constraints are placed on the design due to the need to design the change such that it satisfies not only the accident target, but also the incident targets between the hazard and the accident. In other words, since the relationship between incidents and accidents is predefined in these schemes, the design of the change is constrained by these relationships.

## 6. RISK-BASED SELECTION MODEL

- (a) The review of a safety case.
- (1) As the change to the functional system will only start affecting the operational service<sup>132</sup> once the safety case is complete and in some cases approved, the review of the change is, in fact, a review of the safety case.
  - (2) The change may or may not be adequately safe. Similarly, the safety case may correctly identify the actual risk of the change or it may not. If the argument in the safety case is complex or of an unfamiliar scope, scale or form to the service provider, then there is some likelihood that the safety case will contain errors i.e. the inferences or supporting evidence in the safety case will be insufficient to justify the claim being made by it. In this GM such a safety case is called an unsound safety case. The table below describes the desired outcome for all possible states of the change and its associated safety case.

---

<sup>132</sup> For a full explanation of how changes are implemented and how at various stages of implementation they may affect the operational service, see Section 3.2 of this Appendix.



		Change	
		Adequately safe (Risk is acceptable)	Not adequately safe (Risk is not acceptable)
<b>Safety case</b>	Safety case claim: 'The change is adequately safe.'	Review is unnecessary.	Review cannot happen.
	Sound: The inferences and supporting evidence justify the claim.	The aim of the selection criteria is to minimise the number of reviews here.	Selection criteria are not relevant because the change will be abandoned and the safety case will not be submitted for review.
		No action needed — the desired state.	State cannot happen.
	Unsound: The inferences or supporting evidence are insufficient to justify the claim i.e. the actual risk of the change is not correctly identified (it may be higher or lower than predicted or its value may be more or less certain).	Review may be useful because it may help to prevent future safety cases being unsound.	Review is necessary <sup>133</sup> if the severity of the consequences <sup>134</sup> of the change is reasonably high.  Otherwise, the review may be useful because it may help to prevent future safety cases being unsound.
		The aim of the selection criteria is to select a sufficient number of these safety cases <sup>135</sup> .	The aim of the selection criteria is to maximise the number of reviews here
		Fix the safety case.	Fix the change and the safety case <sup>136</sup> .

**Table 4 — The possible states of a change**

- (3) The need for an independent review is based on the notion that two heads are better than one. There is some likelihood (small though it may be) of an unsafe change being developed, but the accompanying safety case claiming that the change is safe. While the air traffic services provider will use skilled and dedicated staff in the development and review

<sup>133</sup> The change is not adequately safe but the safety case has been submitted for review so the air traffic services provider believes the change to be adequately safe.

<sup>134</sup> The risk of the change is unknown at the time the selection decision is made. The reason the consequences are known is explained in (e)

<sup>135</sup> The change is safe but this is unknowable at the time of review.

<sup>136</sup> Since the change is defined in the safety case, fixing the change necessitates fixing the safety case as well.



of the change and its associated safety case, mistakes may still be made that remain undiscovered. A CA who views things from a different perspective and is not immersed in the change may uncover the mistakes, i.e. if a solution is looked at from different perspectives, any problems with it are more likely to be discovered. The culture of a developer of a change and that of the regulator are sufficiently different that the interaction between the two parties may help uncover any flaws that remain even after the review interactions that will have already taken place within the developer. Moreover, because the CA deals with many air traffic services providers, it is likely to have a wider experience of different changes.

- (4) The purpose of the review is to establish if the change is only as risky as predicted by the safety case and if the claimed risk is acceptable or not. Changes are selected for review well before the safety case exists and so the objective of the selection criteria is to identify those safety cases that, when they arrive for review, may not correctly identify the actual risk, providing the actual risk of the change is great enough to be of concern. Selection, which is based on the 'risk posed by the change', uses the combination of the probability that the argument in the safety case will be complex or unfamiliar<sup>137</sup> and the severity of the consequences associated with the change as the selection criterion.
- (5) Coming to a decision as to whether to review a change or not is a process that may need more information than is present in the notification. The decision may, therefore, not be available for some time after notification;
- (6) The decision to review is expected to be taken well before the full safety assessment has been performed and before the safety case is available because:
  - (i) interactions between the air traffic services provider will take place after the decision has been taken and before the safety case is presented for review. These interactions are described in GM1 ATM/ANS.AR.C.035 & ATM/ANS.OR.A.045 General;
  - (ii) these interactions themselves take time. The time they will take cannot be estimated accurately as the extent of the interactions may not have been completely foreseen by either the CA or the air traffic services provider. Therefore, a significant period should be allocated in the project for this interaction;
  - (iii) the interactions may change the safety argument (its inferences and the evidence needed) and so time needs to be available for this activity; and
  - (iv) since the activities described above only occur once a decision has been made, it is likely to be more efficient to interact with the CA while the change is being developed and the safety assessment is being performed, than to wait until the safety assessment has been completed before seeking the decision as to whether to review the safety case or not.

---

<sup>137</sup> As explained in (d) below, the soundness of the argument in the safety case is related to the probability that the argument will be complex or unfamiliar.

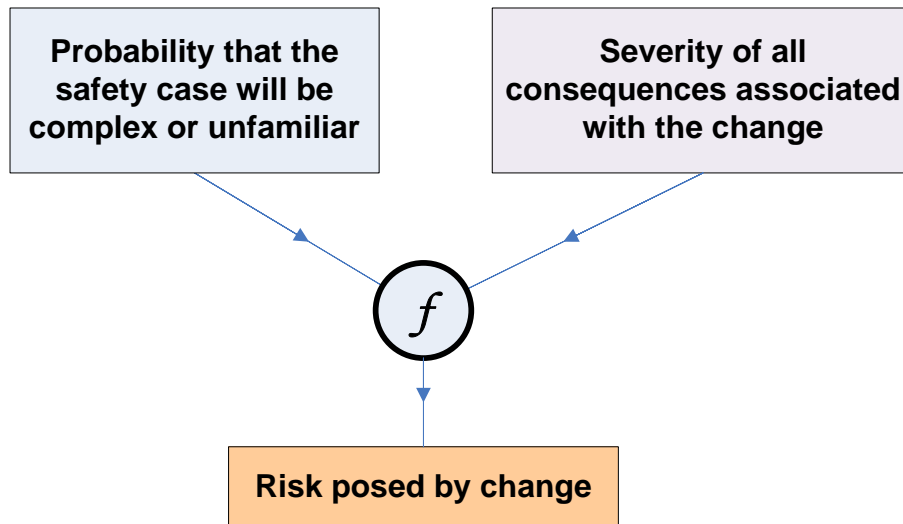


Consequently, the information on which the CA has to make the decision as to whether to review the safety case or not will be coarse-grained and early i.e. without the depth or completeness that the safety case will finally have when developed.

(b) The risk posed by a change

- (1) In any change, it is unlikely that all the risk associated with the services offered by an air traffic services provider will be subjected to the change. In other words, there are always some elements of the air traffic services provider's operational system that will be completely unaffected i.e. not directly or indirectly affected, by the change, and the risk associated with these elements is not altered by the change.
- (2) An example of this is that while the operational misuse of a VOR poses a considerable risk, this is not the risk in question when one is being re-sited. In this instance, it is the risks due to dismantling and re-assembling the VOR and those due to its new position that are the issue. These are a subset of all the risks connected with the VOR and, hence, it is these risks that could be considered to be the risk associated with the change. However, as identified above, this risk is not known to a sufficient degree of accuracy at the time the decision is to be made.
- (3) It should be noted that the need to review the safety case is not based on the net risk after the change. In most cases, the purpose of the change is to restore the risk level to what it was before the change or even to reduce the risk, and so the net risk associated with the change is zero or it has a negative value. Clearly, if the selection criteria used this risk, then there would be no need of a review in almost all cases. However, a change that is intended to have a zero or negative net risk could clearly have significant consequences associated with it, e.g. the removal of an ATC centre from one location to another.
- (4) The risk associated with the change, i.e. the severity of the consequences associated with the changed part of the functional system together with the probability of their occurrence, while being an appropriate risk to use for modulating the review, is not appropriate for selection purposes — it is unknown at selection time.
- (5) Moreover, there is no benefit in reviewing a change that deals with a great deal of risk if the safety case is sound and the resultant risk of the service is correctly predicted to be acceptable.
- (6) Similarly, there is little benefit in reviewing a change, even though the safety case may be unsound if the severity of the consequences associated with the change are small, as indicated in Table 4.
- (7) Selection for review should, therefore, be based on a combination of the likelihood that the safety case may be complex or unfamiliar and the severity of the consequences associated with the change. This is a risk function and is referred to as the '**risk posed by the change**'. However, it can only be based on the coarse-grained data available at the time the decision needs to be made, i.e. close to the time of notification.
- (8) The definition of the risk posed by a change developed above is shown, in Figure 1 below:.





**Figure 29:** The risk posed by a change

(c) Selection Process criteria

The process for evaluating the risk posed by a change should satisfy the following criteria:

- (1) it should be rational, in line with the CA's goal to promote safety;
- (2) its procedures should be of a kind that inspectors find familiar and clear in their meanings;
- (3) it should be applicable, using the information (about each change request or background information) available at each new change request, when the process is first introduced; and
- (4) it should be able to evolve and improve with the information that becomes available over time, in part through the application of the process itself. What kind of information this is in detail will depend on the details of the process, but will certainly include:
  - (i) whether a change, once implemented, proves to be unacceptable, and/or its safety is queried by the CA due to evidence arising after the implementation of the change, and whether that change request had been reviewed or not; and
  - (ii) whether a change that has been reviewed has, as a result of the review, been subject to queries by the CA and/or changes before being approved or rejected or withdrawn by the air traffic services provider.

(d) The probability that an complex or unfamiliar safety case will be developed

- (1) The actual risk associated with the change stems from:
  - (i) changes in the number of hazards;
  - (ii) changes in hazard rates;
  - (iii) changes in mitigations;
  - (iv) changes in mitigation probability;



- (v) changes in accident trajectories<sup>138</sup>; and
- (vi) changes to the circumstances of an accident trajectory, perhaps leading to new accidents

both during operation and during the transition from the current service to the new service.  
 Note: In this list, 'change' means: addition, removal or a change in value/nature of some property of the system.

- (2) Three different aspects of the change and the organisations performing the change can affect the likelihood that an air traffic services provider will misidentify or misevaluate these risks:

- (i) The complexity of the change<sup>139 140</sup>
  - (A) Its size;
  - (B) Its difficulty (technical & managerial);
  - (C) Its novelty; and
  - (D) Its span (the range of different services impacted).

- (ii) The capability of the air traffic services provider<sup>141</sup>

A change that is unfamiliar to the air traffic services provider, in that it is larger, more difficult or has more interactions with other providers, than the changes normally undertaken, or it is novel, is likely to reduce its ability to produce a sound safety case. The capabilities that might be affected are:

- (A) Its technical capability — to manage the difficulty, novelty and span of the individual changes to be made to the functional system; and
- (B) Its managerial capability — to manage the number and range of different organisations involved in the change.
- (C) Its operational capability — to manage the implementation and introduction of the change, possibly across a number of service providers and airspaces.

- (iii) The effectiveness of the air traffic services provider's safety management

The effectiveness of the air traffic services provider's safety management will have an impact on the allocation of the resources needed to develop an safety case for a unfamiliar change.

- (A) The stability of the organisation; and
- (B) The quality of its SMS,

<sup>138</sup> When modelling an accident, an accident trajectory is a chain of events starting with a hazardous event and terminating in an accident.

<sup>139</sup> These properties may relate to the change, the system being changed or both.

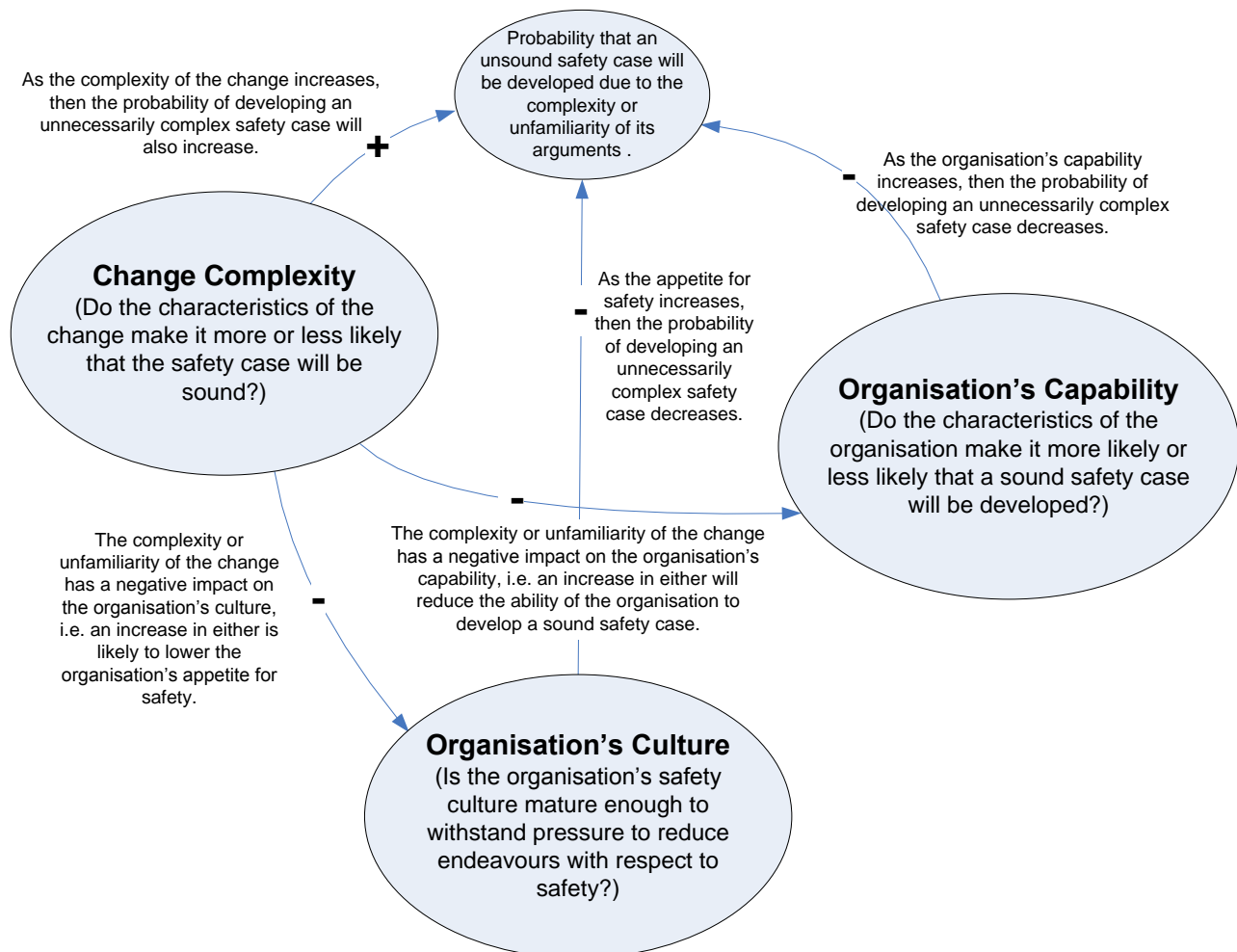
<sup>140</sup> The complexity of the change implies the complexity of the argument

<sup>141</sup> Including the implied capability to develop a sound safety case using these technical/managerial/organisational capabilities.



both relate to the appropriateness of the assessment of the necessary resources, which may be compromised by the unfamiliarity of the argument needed for a sound safety case to be made.

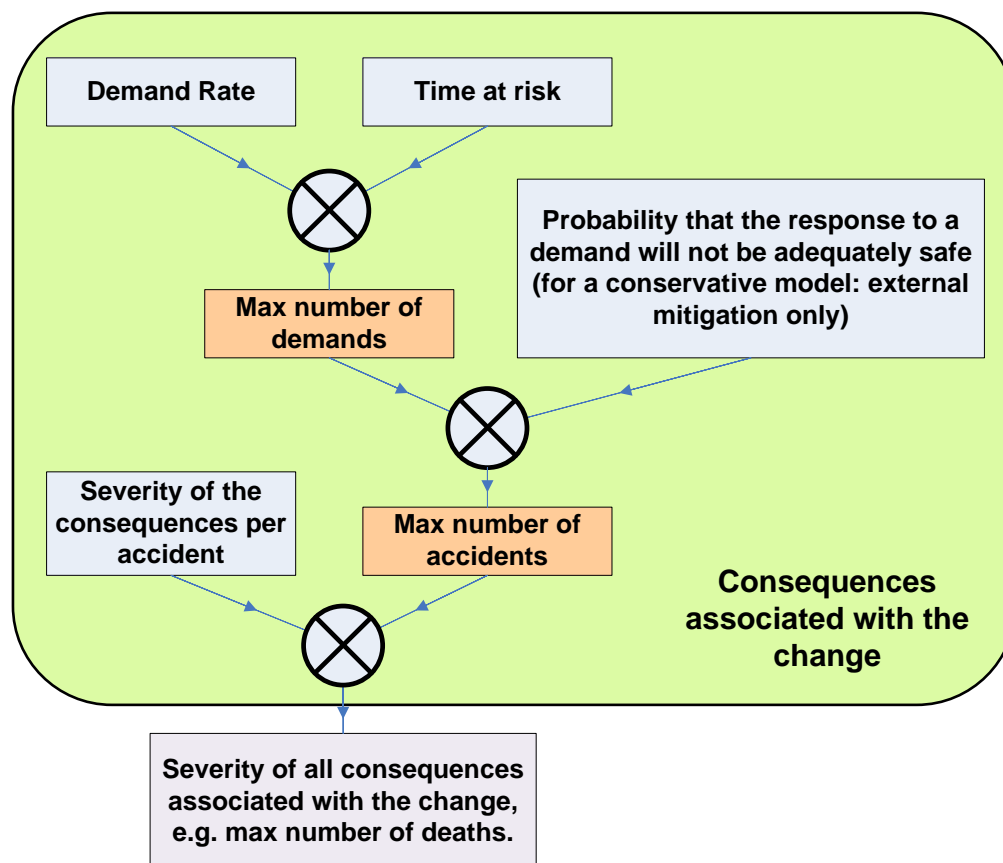
The unfamiliarity of the necessary argument may lead to it being overly complex or overly simple with the result of flaws being made in the arguments and evidence used to justify the overall claim of the safety case. A complex change may lead to a complex argument, which due to its complexity, increases the likelihood of flaws entering the argument. The way these aspects interact is shown in Figure 30 below:



**Figure 30:** The probability of developing an unsound safety case

- (e) The severity of the consequences associated with the change
- (1) The assessment of the severity of the consequence is made at a very early stage in the development of the change and, therefore, will be based on coarse data. It should, therefore, be conservative.
  - (2) In the decision process, such a conservative estimate of the severity of the consequences associated with the change can be established by making the assumption that any demand on the part of the system being changed leads to a response that is not adequately safe and is only mitigated by those parts of the system unaffected by the change, i.e. the normal

mitigations to be provided by the change itself do not work. Another form of mitigation can be provided by assuming that the unsatisfactory nature of the change will be identified at some point and the change reversed. The time taken to detect and reverse the change can be thought of as the 'time at risk'. The consequence model is shown in Figure 3 below. The data needed for it is available once the scope of the change has been identified as it relies only on data from the current system and possibly a projection associated with the future demand rate if it is to be different from the current demand rate.



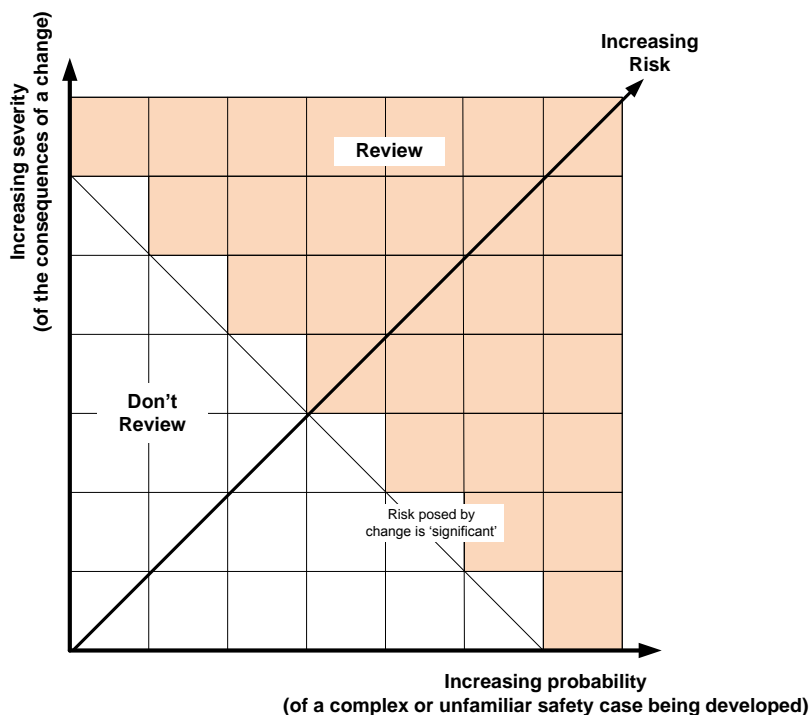
**Figure 31:** The consequences of a change

- (3) The proposed approach may seem unusual in that it combines a pessimistic bound (largest estimated expected loss in case of unsound safety case) with a probability (of the safety case being unsound, so that the change may not be adequately safe). However, estimating the expected value of loss would require a much deeper analysis than is possible at the early stage when the decision to review or not is required; it may require most of a complete safety case for the proposed change to the functional system. Given the limited information and, thus, high level of uncertainty, assessing based on worst-case loss is a defensible decision criterion. Worst-case loss plausibly correlates with expected loss, and this avoids the risk of underestimating it. Similar approaches are used elsewhere e.g. in the nuclear industry, where conservative estimates are used, together with claim limits to prevent excessive optimism.
- (f) Establishing the risk function
- (1) The risk posed by a change should be a scalar measure associated with the change and will be some combination of the two inputs: the probability of a complex or unfamiliar



argument i.e. implying an unsound safety case (meaning the change may not be adequately safe), and the severity of the consequences of the proposed change. Unless strong arguments against it exist, assuming the function to be a product is a reasonable starting point. The selection criterion, a function of risk, is then a hyperbole in the Cartesian plane, or a straight line if the scales are logarithmic. The diagram below illustrates the logarithmic approach: if both inputs are assessed on coarse scales (which is inevitable when involving judgement as inputs), then the result is that the risk posed by a change (the output of the model) is the sum of the inputs, which is an intuitive measure (distance from the origin, in a log-log graph).

- (2) In practice, the selection process may use a risk matrix in which risk parameters are represented according to a coarse-grained measurement scheme, and the selection criteria establishes the boundary beyond which safety cases will be selected for review, as shown below:



**ACCEPTABLE MEANS OF COMPLIANCE AND GUIDANCE MATERIAL  
TO ANNEX I — DEFINITIONS OF TERMS USED IN ANNEXES II TO XIII**



**ACCEPTABLE MEANS OF COMPLIANCE AND GUIDANCE MATERIAL  
TO ANNEX II — REQUIREMENTS FOR COMPETENT AUTHORITIES — PROVISION OF SERVICES AND  
ATM NETWORK FUNCTIONS  
(Part-ATM/ANS.AR)**

**SUBPART B — MANAGEMENT (ATM/ANS.AR.B)**

**AMC1 ATM/ANS.AR.B.015(a)(8) Record keeping**

**RECORD KEEPING FOR FUNCTIONAL SYSTEMS CHANGE MANAGEMENT PROCEDURES**

The CA should keep a record of all the change management procedures, modifications and deviations it has approved in accordance with ATM/ANS.AR.C.030(a) and those that have been rejected, together with a rationale. The CA should be able to cross-reference them to the requirement of the associated requirement in the Regulation that they intend to comply with.

**SUBPART C — OVERSIGHT, CERTIFICATION, AND ENFORCEMENT (ATM/ANS.AR.C)**

**AMC1 ATM/ANS.AR.C.010(a) Oversight**

**CHANGES TO THE FUNCTIONAL SYSTEM**

The audits should include oversight of changes to the functional system in order to:

- (a) verify that changes made to the functional system:
  - (1) comply with ATM/ANS.OR.A.045;
  - (2) have been managed in accordance with the procedures identified in ATM/ANS.OR.B.010(a) that have been approved; and
  - (3) are being verified against the monitoring criteria that were identified in the assurance argument as a result of complying with ATM/ANS.OR.C.005(b)(2) or ATS.OR.205(b)(6), as appropriate; and
- (b) verify that if, as a result of the monitoring referred to in (a)(3), the argument, referred to in ATS.OR.205(a)(2) and ATM/ANS.OR.C.005(a)(2), is found to be unsound, then the service provider has initiated a change or has revised the argument such that the inferences or evidence are now sufficient to justify the claim.

**GM1 ATM/ANS.AR.C.030 Approval of change management procedures for ATM/ANS functional systems**

**GENERAL**

The review by the CA is focussed on the change management procedures and not on the project management part of these procedures that are not required by the regulations, even though they may be useful for the smooth execution of the project dealing with the change. Consequently, not all parts of a procedure may be approved by the CA. The approved parts should be identified in the record (see AMC1 ATM/ANS.AR.B.015(a)(8)) and communicated to the service provider.



**AMC1 ATM/ANS.AR.C.030(a) Approval of change management procedures for functional systems**  
MEANS AND METHOD OF SUBMITTING PROCEDURES

The CA should agree with the service provider the means and method of submitting the procedures, modifications and deviations referred to in ATM/ANS.AR.C.030(a). Until an agreement is reached, the CA will prescribe the means and method of submission.

**AMC1 ATM/ANS.AR.C.030(b) Approval of change management procedures for functional systems**  
APPROVAL OF PROCEDURES

The CA should approve the change management procedures provided in accordance with ATM/ANS.OR.B.010 only when the CA has performed (a) to (g) below.

- (a) The CA should check that the procedures used by a service provider to manage changes cover the life cycle of a change as defined in ATM/ANS.OR.C.005(a)(1) or ATS.OR.205(a)(1).
- (b) When reviewing the content of the procedures, modifications and/or deviations referred to in ATM/ANS.AR.C.030(a), the CA should use the compliance matrix provided by the service provider referred to in AMC1 ATM/ANS.OR.B.010(a).
- (c) The CA should check that the procedures make mandatory provisions that require actions to be undertaken and all required evidence to be produced to comply with requirements laid down in ATM/ANS.OR.A.045, ATM/ANS.OR.C.005, ATS.OR.205 and ATS.OR.210 or alternative means of compliance, if any. As part of this oversight activity, the CA should check that the compliance matrix covers all the aforementioned requirements.
- (d) The CA should check that the procedures identify the roles and responsibilities of the service provider in the change management processes.
- (e) The CA should check that the service provider's change management procedures state that it is not allowed to use new, modified or deviating change management procedures until approval is granted.
- (f) The CA should check that the service provider's change management procedures state that any change selected for review must not enter into operational service before the approval is granted.
- (g) The CA should provide a response to the service provider's notification of change referred to in ATM/ANS.OR.A.045(a) without undue delay.

**AMC1 ATM/ANS.AR.C.035(a) Decision to review the notified change to the functional system**  
MEANS AND METHOD OF SUBMITTING NOTIFICATION OF CHANGES TO FUNCTIONAL SYSTEMS

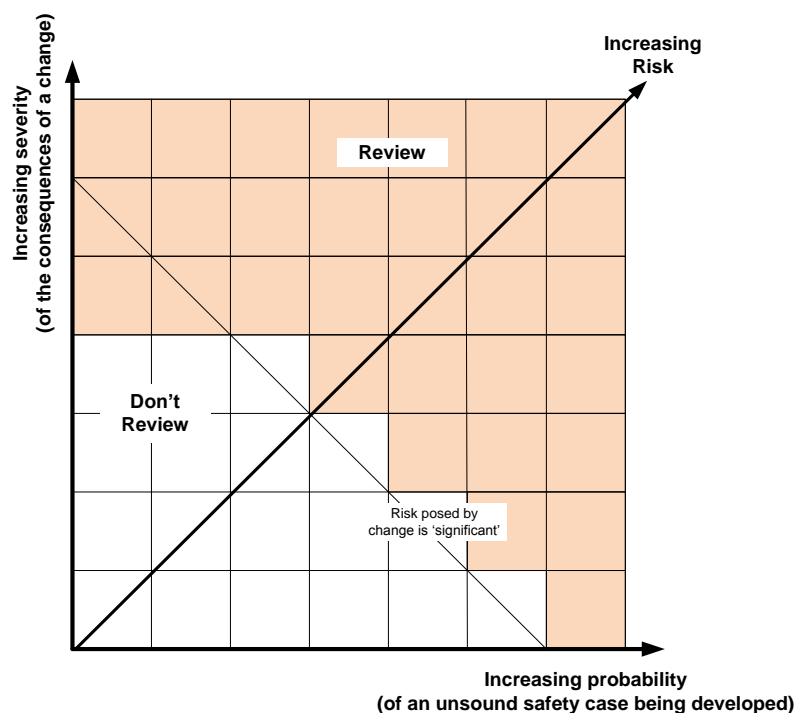
The CA should agree with the service provider the means and method of submitting the notification of changes and additional information referred to in ATM/ANS.OR.A.045(a). Until an agreement is reached, the CA will prescribe the means of submission.



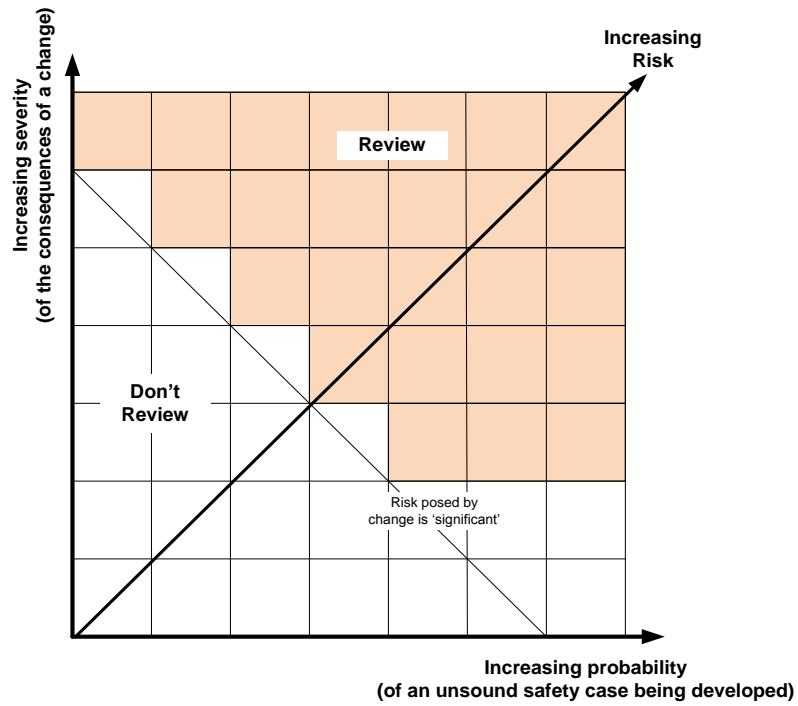
**GM1 ATM/ANS.AR.C.035(c) Decision to review the notified change**

## OTHER SELECTION CRITERIA

- (a) Some changes may not necessarily need to be reviewed providing that, even though they relate to safety, they can be considered as routine by the provider as they have been consistently assessed, implemented and proved safe in the past and, therefore, the CA has sufficient confidence that the provider will address them in a similar manner.
- (b) The selection criterion for review may deviate from a simple threshold on the scalar risk metric (distance from the origin), to deal with concerns due to the coarse grain and high uncertainty of the inputs. For instance, a separate threshold on the 'severity' axis may be used to specify, for instance:
- (1) that changes with very high potential severity should always be reviewed, irrespective of the probability of the safety case being unsound (Figure 32 below). This criterion may well respond to common perceptions and could be justified by the fact that judgements of low probabilities based on limited information are often unreliable, and errors in the judgment of risk are proportional to the error on probability and the size of the loss; and
  - (2) that changes with minor potential severity need not be reviewed, irrespective of the probability of the safety case being unsound (Figure 33 below) (though the process may retain the option for the CA to review the change, since the estimate itself of potential severity may be suspected of being erroneous).
- (c) It is also possible that deviations be required on the basis of some of the component factors that affect either probability or severity, e.g. exempting changes based on small size of change and high competence of the air traffic services provider.
- (d) In order to validate the process or provide data for the evolution of the process, it may be advisable to randomly select changes to review and then assess whether the safety case is sound or not and whether or not the case would have been selected for review using the current criteria for the selection process.



**Figure 32:** Criteria that may be used when severity is high



**Figure 33:** Criteria that may be used when severity is low

**ACCEPTABLE MEANS OF COMPLIANCE AND GUIDANCE MATERIAL**  
**to ANNEX III — COMMON REQUIREMENTS FOR SERVICE PROVIDERS**  
**(Part-ATM/ANS.OR)**

**SUBPART A — GENERAL COMMON REQUIREMENTS (ATM/ANS.OR.A)**

**AMC1 ATM/ANS.OR.A.045(a) Changes to the functional system**

**NOTIFICATION DATA**

The notification of a change is not considered complete until the following information is provided:

- (a) Name of the organisation notifying the change;
- (b) Unique identifier of change;
- (c) Version number of notification;
- (d) Title of the change;
- (e) Date of the submission of the original of this change notification;
- (f) Scheduled date of entry into service (even if only approximate);
- (g) Details of the change and its impact;
- (h) The list of the service providers and other aviation undertakings that are affected by the change as identified in ATM/ANS.OR.A.045 (a)(3);
- (i) Entity in charge of the assurance case; and
- (j) Identity of a point of contact for communications with the CA.

**GM1 ATM/ANS.OR.A.045(a) Changes to the functional system**

**NOTIFICATION DATA**

- (a) A change should be notified as soon as the data defined in AMC1 ATM/ANS.OR.A.045(a) is available. The decision to review a change by the CA will be based, in most circumstances, on the notification data. Exceptions to this are cases where the CA is not familiar with the type of change or the complexity of the change requires a more thorough consideration.
- (b) Early and accurate notification facilitates the interactions between the provider and the CA and, thus, maximises the likelihood of introducing a change into service in due time and according to the service provider's initial schedule when the CA has decided to review an assurance case. Therefore, it is advisable that the change description identified in AMC1 ATM/ANS.OR.A.045(a) is completed as soon as possible and contains the following data:
  - (1) Purpose of the change;
  - (2) Reasons for the change;
  - (3) Place of implementation;
  - (4) New/modified functions/services brought about by the change;
  - (5) High-level identification of the constituents of the functional system being changed, and what is modified in their functionality;



- (6) Consequence of the change, i.e. the harmful effects of the hazards associated with the change — see (f) below and also the definition of ‘risk’ in Annex I (80).
- (c) The information provided in (b) may speed up the decision whether to review or not the proposed change because it will allow the CA to gain complete knowledge of the change and, consequently, reduces the need for additional information. However, lack of some of this data should not delay the service provider submitting the notification if to do so is likely to impede the introduction of the change. It should be noted that early interaction with its CA may help to complete the missing data.
- (d) The service provider should take into account that an early, clear and accurate change notification will assist the CA in making the decision to review or not the change and may prevent any inconvenience such as:
- (1) the CA having to ask for more information about the change, as a necessary precursor to identifying the additional information it will seek in order to make its decision as required in ATM/ANS.OR.A.045(a)(2);
  - (2) the CA deciding to review a change unnecessarily because the notification is not clear enough; or
  - (3) the delay in the CA deciding whether to review a change, caused by the lack of information, having an impact on the proposed date of entry into service.
- (e) It is recognised that the understanding of the change will improve as the change process progresses and the interaction between the CA and the ATM/ANS provider strengthens. An update of the notification is required when the information provided in the previous notification is no longer valid or when the information previously missing becomes available. When additional information — other than the data specified in AMC1 ATM/ANS.OR.A.045(a) — is supplied at the CA’s request, then no update of the notification is required.
- (f) For air traffic services providers, the consequences of the change specified in (b)(6), should be expressed in terms of the harmful effects of the change, i.e. the effects of the hazards associated with safety risks. These could be the result of a preliminary safety assessment, if available, or an early hazard analysis that concentrates on the service level effects. For service providers other than air traffic services providers, the consequences should be expressed in terms of what aspects of the performance of the service are impacted by the change.
- (g) The point of contact, as required in item (j) in AMC1 ATM/ANS.OR.A.045(a), provides a focal point for the CA to contact when seeking complementary information about the change when required. The aim is to improve communications between the provider and the CA about the change.
- (h) All notified changes should be unambiguously identified. The service provider and its CA should agree on a means of referencing so as to associate a unique identifier to a given notified change.

## **GM2 ATM/ANS.OR.A.045(a) Changes to the functional system**

### **ROUTINE CHANGES**

- (a) The service provider has to keep a record of these changes and the notification to the CA may be done in a simpler manner, e.g. using forms less detailed as specified in AMC1 ATM/ANS.OR.A.045(a) or notifying these changes collectively after being implemented at regular periods of times agreed between the provider and the CA.





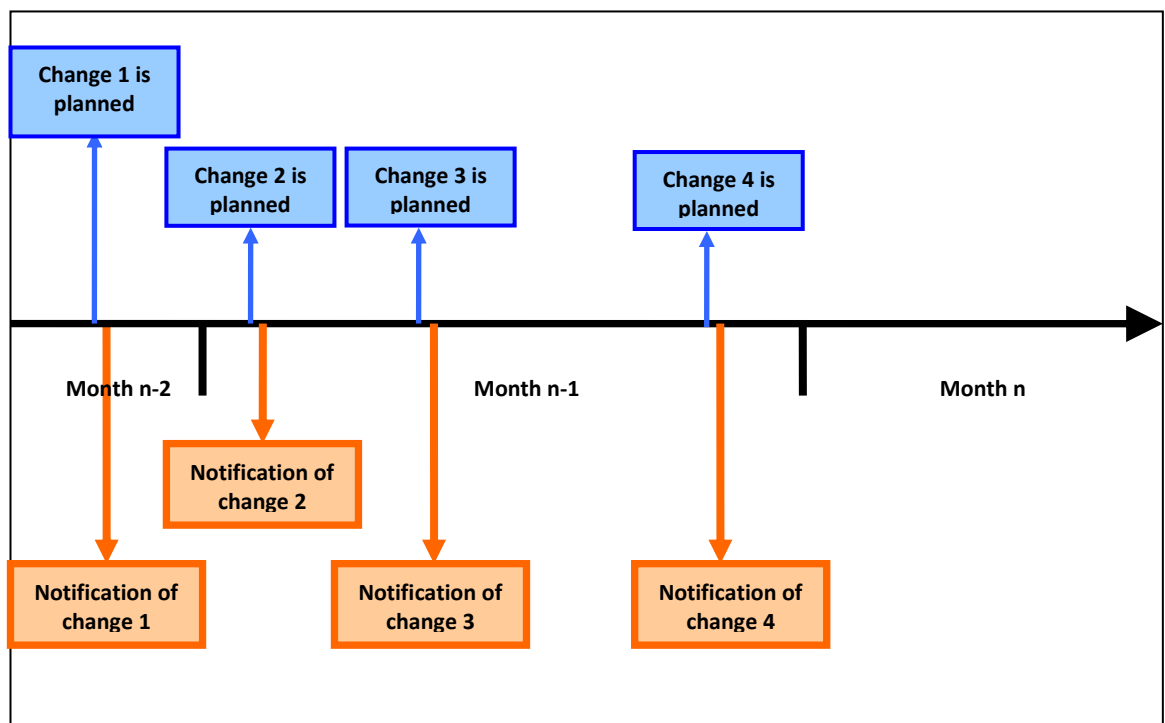
- (b) A service provider and its CA should coordinate so as to reach a common agreement on these types of changes that may not be reviewed by the CA. The list of such changes should be documented and formalised. The formalised agreement becomes part of the change management procedures identified in ATM/ANS.OR.B.010. Consequently, the list will be reviewed by the CA as part of the audits it performs that are described in ATM/ANS.AR.C.010(a). The relevant audit activity is detailed in AMC1 ATM/ANS.AR.C.010(a)(a)(2).

**GM3 ATM/ANS.OR.A.045(a) Changes to the functional system**  
 MEANS OF NOTIFICATION

- (a) There are different means of notifying changes to the CA. An appropriate means has to be selected and agreed with the CA, which depends on various parameters such as:
  - (1) the size of the service provider;
  - (2) the number of changes it undertakes;
  - (3) the type of changes that are likely to be notified; and
  - (4) the way the CA and/or the service provider is (are) organised.
- (b) The following cases are given as examples and are not, by any means, exhaustive.

(1) Individual notification

The service provider notifies the CA of each change it plans to undertake as soon as a substantial part of the ‘notification data’, as defined in AMC1 ATM/ANS.OR.A.045(a), is available.



This type of notification is usually well-suited for:

- (i) small service providers; or

- (ii) service providers undertaking a small number of changes; or
- (iii) service providers for which change notification is directly undertaken by the individual operational units.

The CA has to respond to each notification in order to inform the service provider which changes are going to be reviewed and which are not, if any.

One of the advantages of this notification means is that the CA can start the review decision process early.

(2) Periodic notification

The service provider notifies changes to the CA on a regular basis, for instance on a quarterly basis. The service provider notifies the changes it has planned during the previous period. The notification consists of a list of changes and their associated notification data transmitted by the means agreed with the CA.

This type of notification is well-suited for:

- (i) large service providers; or
- (ii) service providers undertaking a significant number of changes; or
- (iii) service providers that have a specific entity dealing with the management of changes and that can centralise the notifications for the operational units.

The CA has to respond to each notification in order to inform the service provider which changes are going to be reviewed and which are not, if any. The periodic notification allows the CA to produce one single answer listing the changes subject to review, facilitating the response process.

In addition, the periodic notification allows the CA to organise periodic meetings to collectively review the list of changes and make an appropriate decision if they will be reviewed or not.

(3) Short lead time notifications

When notification occurs close to the scheduled date of entry into service, the service providers and the CA may make the appropriate arrangements to allow individual notifications to be submitted out of the periodic notification period so as to be able to deal with changes on time. This type of short lead time notification is a departure from the periodic notification procedure and should be duly justified with valid reasons. These deviations should be exceptional and not become the norm; otherwise, the service provider and the CA should agree on amending the change management process.

The air traffic services provider may submit an explanation of the impact on safety and other service providers may submit an explanation of the impact on performance that a delayed entry into service would have, compared to the initial planned date to allow the CA to balance the safety risk of not reviewing the change with the business and/or safety risk of delaying the entry into service of the change due to its review.

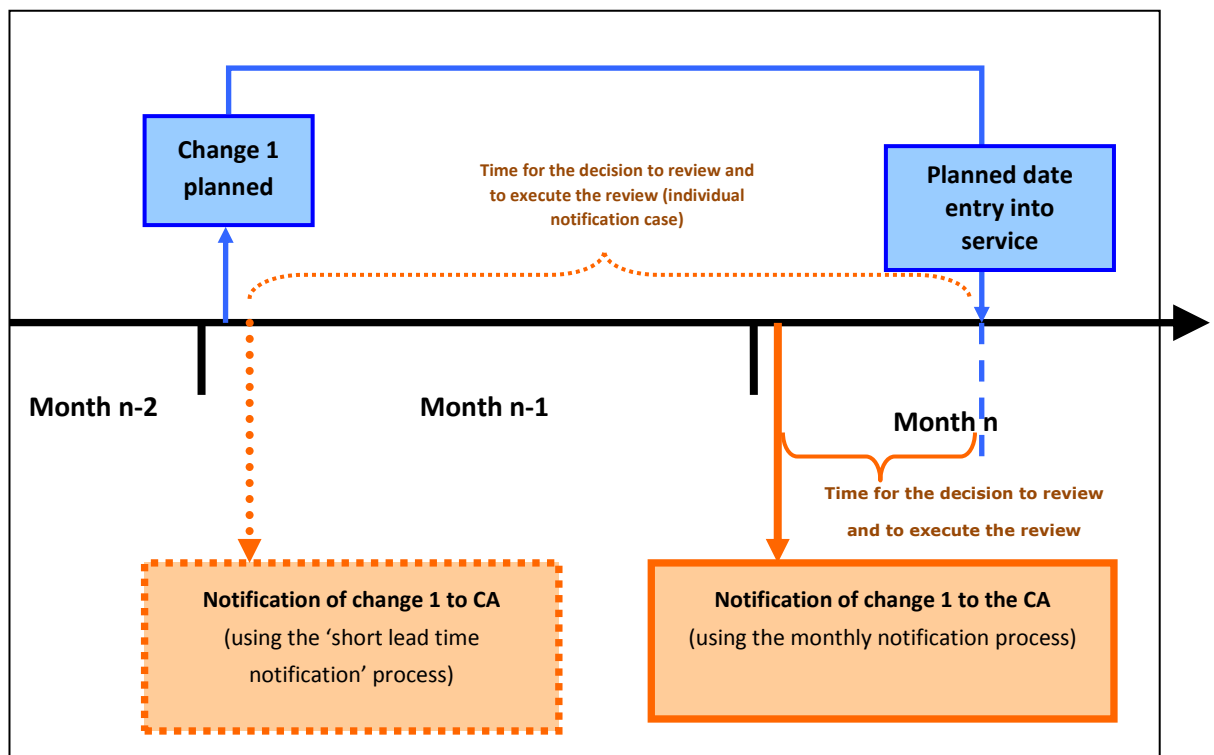
Whatever the type of notification used by the service provider, short lead time notifications have to be tagged so that they can be easily spotted by the CA. This may be done adding the following fields to the notification data listed in AMC1 ATM/ANS.OR.A.045(a):



10		<i>Short Lead Time Notification</i>
	1	The reason why the change was not notified earlier to the CA.
	2	The safety impact of not implementing the change at the initially planned date of entry into service, i.e. due to the likely delay introduced by a review by the CA. For air traffic services providers, a risk-based argument justifying the timing of the change and explaining the safety consequences of a possible delay in the entry into service should be provided. Note that a potential delay might not have any safety consequences.

That way, the CA knows that the time frame will be tight if it chooses to review the associated change. A specific alert such as a direct phone call to a predetermined point of contact can be useful in preparing the CA for this kind of notifications and thus optimising the CA’s response.

The short lead time notification process is particularly suitable when the periodic notification process is used. For example, on the basis of a monthly notification, a change which is decided by the service provider at the beginning of the month and planned for the middle of the next month would be notified to the CA only two weeks before its planned date of entry into service.



**GM4 ATM/ANS.OR.A.045(a) Management of change to a functional system**  
 REGISTER OF NOTIFIED CHANGES

It is advisable that the fields of the notification form are searchable in the register.



**GM5 ATM/ANS.OR.A.045(a) Management of change to a functional system**

**EXAMPLE OF NOTIFICATION FORM FOR AN AERODROME FLIGHT INFORMATION SERVICES (AFIS) PROVIDER**

<p><b>AFIS change notification form</b></p> <p>[To be filled in as soon as the requested information is known.]</p> <p>[If needed, insert more guidance here for the use of this notification form]</p>		
<b>1. CHANGE IDENTIFICATION</b>	<b>Date of submission:</b>	<b>Version: Vx.y</b>
<p>[Title and reference number specific to the change]</p> <p>[The form version has to be incremented for any data update concerning the notification]</p> <p>[Example: AFIS_xxx_CHGT-1234 'title'- V1.1]</p>		
<b>2. CHANGE SUMMARY</b>		
Entity assuring project management for this change:  (and responsible for the decision for its entry into service)	<input type="checkbox"/> AFIS	
	<input type="checkbox"/> Other entity [Precise which entity: other ANSP, aerodrome operator, military organism, airspace users, etc.]	
Change description	Indicate here: <ul style="list-style-type: none"> <li>— The reasons for having decided the change</li> <li>— Description of the change and its components:                         <ul style="list-style-type: none"> <li>• Technical systems (HW, SW)</li> <li>• Human factors (trainings, competency, HMI, etc.)</li> <li>• Procedures (working methods, ATS procedures, maintenance procedures, etc.)</li> </ul> </li> <li>— Interfaces of the change:                         <ul style="list-style-type: none"> <li>• with the ATM/ANS functional system managed by the AFIS</li> <li>• with the remainder of the ATM/ANS functional system (other ANSP, etc.)</li> <li>• with external entities (aerodrome operators, etc.)</li> </ul> </li> </ul>	
Scheduled date of entry into service		
<b>3. OTHERS AFFECTED BY THE CHANGE</b>		



Service providers	<p><i>Indicate here the list of service providers affected by the change</i></p> <ul style="list-style-type: none"> <li>• <i>service provider that is affected by the change</i></li> <li>• <i>service provider that is affected by the change</i></li> <li>...</li> <li>• <i>service provider that is affected by the change</i></li> </ul>
Aviation undertakings	<p><i>Indicate here the list of aviation undertakings affected by the change</i></p> <ul style="list-style-type: none"> <li>• <i>aviation undertaking that is affected by the change</i></li> <li>• <i>aviation undertaking that is affected by the change</i></li> <li>...</li> <li>• <i>aviation undertaking that is affected by the change</i></li> </ul>
<b>4. POINT OF CONTACT</b>	
Identity of a person to contact in case further information is needed	
Name/function :	
Phone(s) :	
E-mail :	

**AMC1 ATM/ANS.OR.A.045(a)(3) Changes to the functional system**

NOTIFICATION TO USERS OF THE SERVICE

Having notified a change, the service provider should:

- (a) individually inform all known service providers potentially affected by the notified change; and
- (b) inform all aviation undertakings potentially affected by the change either individually or via a representative body of aviation undertakings or by publishing details of the planned change in a dedicated publication of the service provider.

**GM1 ATM/ANS.OR.A.045(a)(3) Changes to the functional system**

DEDICATED PUBLICATION FOR PROPOSED CHANGES

The final users of services potentially affected by a change to a functional system may not be known by the service provider proposing the change. However, this should not prevent the provider from seeking notification using other means than direct communication with the interested parties. In that case, the changes may be published in a dedicated site where the users of the service can periodically check for current proposed changes to the functional system that may affect them. For example, the service provider may dedicate a website to publish the notifications.

**AMC1 ATM/ANS.OR.A.045(b) Changes to the functional system**

MODIFICATION OF A NOTIFIED CHANGE

- (a) The service provider proposing a change should update the notification data when the information provided in a previous notification about the same change is no longer valid or when the information previously missing becomes available. The service provider should inform the other service providers



and aviation undertakings of this update, when they are affected by the new data, and CAs that were initially informed about the change.

- (b) The cancellation of a previously notified change is considered a modification of a notified change. Therefore, the service provider should notify this update to the CAs, and inform other service providers and aviation undertakings that were initially informed about the change.

#### **AMC1 ATM/ANS.OR.A.045(d) Changes to the functional system**

##### ENTRY INTO OPERATIONAL SERVICE OF A CHANGE SELECTED FOR REVIEW

Where the CA has decided to review the assurance case of a proposed change, the service provider should not start the implementation of any part of the change that has the potential to affect the behaviour of the service currently being provided until it has been approved by the CA.

#### **GM1 ATM/ANS.OR.A.045(c); (d) Changes to the functional system**

##### TRANSITION INTO OPERATION

Even where the CA has not decided to review the assurance case of a proposed change, the service provider should not start the implementation of any part of the change that has the potential to affect the functionality or performance of the service until it has produced a valid assurance case in accordance with either ATS.OR.205(d) or ATM/ANS.OR.C.005(d) as appropriate. For a complete description of the different transitions of a change into operations, see Section 3.2 of Appendix I to GM1 to Article 5 & Article 6(c).

#### **GM2 ATM/ANS.OR.A.045(c); (d) Changes to the functional system**

##### CHANGES IMPLEMENTED PRIOR TO RECEIVING APPROVAL

Some changes might stem from the need to implement immediate action and, therefore, their implementation cannot be delayed until they receive approval or communication that the change is not being reviewed from the CA. Examples of these changes are changes due to urgent unforeseen circumstances<sup>142</sup> that would, if uncorrected, lead to an immediate unsafe condition, e.g. presence of volcanic ash. The service provider is in any case responsible for the safe provision of the service.

#### **AMC1 ATM/ANS.OR.A.045(e) Changes to the functional system**

##### CHANGES AFFECTING MULTIPLE SERVICE PROVIDERS — OVERARCHING SAFETY ARGUMENT

A change as defined in ATM/ANS.OR.A.045(e) may involve more than one service provider changing their functional systems. In this case, the change will consist of a set of changes to different ATM/ANS functional systems or their context. However, no matter how many individual changes to service providers' functional systems are part of the change, they should be coordinated. An overarching safety argument, coherent with the arguments of the individual changes, that claims the complete change is safe should be provided.

#### **GM1 ATM/ANS.OR.A.045(e) Changes to the functional system**

##### CHANGES AFFECTING MULTIPLE SERVICE PROVIDERS AND AVIATION UNDERTAKINGS — GENERAL

- (a) Any change proposed by a service provider as defined in AMT/ANS.OR.A.045(a) affects other service providers and/or aviation undertakings when:

<sup>142</sup> These circumstances are not foreseen in the design and, thus, not considered either in maintenance processes or in contingency plans. However, in the normal case, corrective repairs of equipment malfunction must be considered in the design and procedures to deal with them included in the maintenance processes. They are not changes that require notification.



- (1) the proposed change may alter the service delivered to other service providers and aviation undertakings as users of that service; or
  - (2) the proposed change may alter the operational context in which the services of other service providers and aviation undertakings are delivered or in which the aviation undertakings are operating.
- (b) The changes referred in AMT/ANS.OR.A.045(e), are those changes that require coordination to be implemented due to the presence of dependencies between the service providers that planned the change and other affected service providers and/or other aviation undertakings. The coordination is essential to ensure a correct safety assessment when there are dependencies.

**GM2 ATM/ANS.OR.A.045(e) Changes to the functional system**

## AFFECTED STAKEHOLDERS — SERVICE PROVIDERS AND AVIATION UNDERTAKINGS

- (a) Other service providers included in AMT/ANS.OR.A.045(e) refer to European service providers other than the service provider proposing the change, that are regulated in accordance with Regulation (EC) No 216/2008 and its Implementing Rules;
- (b) Aviation undertakings affected by the change included in AMT/ANS.OR.A.045(e) can be understood as the stakeholders and professional associations with dependencies with the changed service, and may include the following:
- (1) service providers that do not fall under the remit of Regulation (EC) No 216/2008 and its Implementing Rules, e.g. non-European service providers;
  - (2) aerodrome operators;
  - (3) aircraft operators;
  - (4) military authorities;
  - (5) airframe and equipment manufacturers;
  - (6) maintenance organisations;
  - (7) Regulatory bodies, e.g. European Commission, EASA, NAAs; and
  - (8) other bodies not regulated by Regulation (EC) No 216/2008 and its Implementing Rules, e.g. power supplier organisations, professional associations or passenger associations.

**GM3 ATM/ANS.OR.A.045(e) Changes to the functional system**

## CHANGE AFFECTING MULTIPLE SERVICE PROVIDERS AND AVIATION UNDERTAKINGS — COORDINATION

- (a) The provisions in ATM/ANS.OR.A.045(e) apply to all the affected service providers involved in the change, and, therefore, they must coordinate dependencies as well as shared assumptions and shared risk mitigations as required by ATM/ANS.OR.A.045(e). They must only use the agreed and aligned assumptions and mitigations that are related to more than one service provider or aviation undertakings in their safety or safety support cases, as required by AMT/ANS.OR.A.045(f).
- (b) Assumptions and risk mitigations used during the assessment of the change that are not shared by the affected service providers can be handled independently by each service provider, and do not need agreement.
- (c) This coordination means that the affected service providers:



- (1) have jointly identified the scope of their responsibilities with regard to the change, and in particular their safety responsibilities, e.g. what part of the change will be covered in whose safety (support) assessment case;
  - (2) have jointly identified the dependencies;
  - (3) have jointly identified the hazards associated with the change in the common context;
  - (4) have mutually agreed on the assumptions for the change that jointly relate to them; and
  - (5) have mutually agreed on the mitigations for risks that require joint implementation.
- (d) Service providers would need to achieve a common understanding about:
- (1) consequences in the shared operational context; and
  - (2) chains of causes/consequences.
- (e) Service providers would jointly need to identify their dependencies to be able to assess the change to their functional systems.
- (f) Where necessary in relation to the dependences identified in accordance with GM1 ATM/ANS.OR.A.045(e)(1), the service providers may perform together:
- (1) identification of hazards/effects;
  - (2) assessment of risks;
  - (3) evaluation of risks;
  - (4) planning and assessment of risk mitigations; and
  - (5) verification.
- (g) The level of interaction and coordination between service providers and aviation undertakings will vary depending on the particular needs of the change at hand.

**GM1 ATM/ANS.OR.A.045(e)(2) Changes to the functional system****CHANGE AFFECTING MULTIPLE SERVICE PROVIDERS AND AVIATION UNDERTAKINGS — ASSUMPTIONS AND RISK MITIGATIONS**

In order to satisfy ATM/ANS.OR.A.045(e)(2), the affected service providers coordination will identify those assumptions and risk mitigations that relate to:

- (a) more than one service provider;
- (b) a service provider and one or more aviation undertakings; or
- (c) multiple service providers and aviation undertakings.

**GM4 ATM/ANS.OR.A.045(e) Changes to the functional system****COORDINATION WITH AFFECTED AVIATION UNDERTAKINGS**

- (a) The provisions in AMT/ANS.OR.A.045(e) do not apply to aviation undertakings. However, any service provider affected by a change should seek the participation of aviation undertakings when assumptions and risk mitigations used in the safety (support) assessment are shared with those aviation undertakings. Such aviation undertakings are those described in ATM/ANS.OR.A.045(e) as 'affected' by the change.





- (b) The feasibility mentioned in the provisions of ATM/ANS.OR.A.045(e)(1) refers to the fact that this Regulation does not apply to aviation undertakings and, therefore, there are no means of enforcement available to make them participate in the alignment and agreement of assumptions and risk mitigations. If this was not the case, a service provider who did not align and agree the assumptions and risk mitigations with an aviation undertaking would have infringed the Regulation, even though it was the aviation undertaking that decided not to cooperate.
- (c) When the number of aviation undertakings affected by the change is large, the service providers may not need to involve every individual stakeholder. If a body can represent the views of a group of affected aviation undertakings, it may suffice to involve that representative body to obtain the supporting evidence to move forward with the assessment of the change.

**GM1 ATM/ANS.OR.A.045(f) Changes to the functional system**

## LACK OF COORDINATION

- (a) If an aviation undertaking decides not to cooperate, the service providers, who have identified dependencies with the aviation undertaking, in accordance with ATM/ANS.OR.A.045(e)(1), need to consider the impact of having the assumptions and risk mitigations not agreed with that aviation undertaking. They should propose a way forward by doing one or more of the following:
- (1) making the assumptions themselves and providing evidence that supports them;
  - (2) adding additional mitigating measures so that the change remains acceptably safe;
  - (3) modifying the scope of the change, or even reconsidering and cancelling the change.
- (b) Service providers affected by a lack of cooperation with an aviation undertaking may wish to inform their CA about those aviation undertakings that are not participating and their form of non-participation, in order to seek the assistance of the CA in trying to persuade the aviation undertaking to participate.

**SUBPART B — MANAGEMENT (ATM/ANS.OR.B)****GM1 ATM/ANS.OR.B.005(a)(4) Management system**

## IDENTIFICATION OF CHANGES TO FUNCTIONAL SYSTEMS

This process is used by the service provider to correctly identify proposed changes. The changes dealt with in this GM are the proposed changes to the functional system. These can be triggered internally by changing circumstances that are related to the service provider of concern or externally by changing circumstances that are related to others or to the context in which the service operates, i.e. in situations where the service provider does not have managerial control over them. The triggers are called ‘change drivers’.

- (a) Identification of internal circumstances
- (1) The procedure to identify changes needs to be embedded in all parts of the organisation that can modify the functional system, i.e. the operational system used to support the services provided. Examples of proposed changes to the functional system as a response to changing circumstances under the control of the organisation, therefore, include:
    - (i) changes to the way the components of the functional system are used;
    - (ii) changes to equipment, either hardware or software;



- (iii) changes to roles and responsibilities of operational personnel;
  - (iv) changes to operating procedures;
  - (v) changes to system configuration, excluding changes during maintenance, repair and alternative operations that are already part of the accepted operational envelope;
  - (vi) changes that are necessary as a result of changing circumstances to the operational context under the managerial control of the provider that can impact the service, e.g. provision of service under new conditions;
  - (vii) changes that are necessary as a result of changing circumstances to the local physical (operational) environment of the functional system; and
  - (viii) changes to the working hours and/or shift patterns of key personnel which could impact on the safe delivery of services.
- (2) These changes are often identified by the service provider using business processes, which will be used to identify changes planned for the medium and long term. Such processes can include:
- (i) annual business plans;
  - (ii) strategic safety boards;
  - (iii) equipment replacement projects;
  - (iv) airspace reorganisation plans;
  - (v) introduction of new operational concepts, e.g. Free Flight;
  - (vi) accident and incident investigation reports; and
  - (vii) safety monitoring and safety surveys.

(b) Identification of external circumstances

The service provider should have processes in place to react appropriately to notifications received from those service providers that supply services to them. In addition, changes to the context that can impact on the service provided and are not under the managerial control of the service provider should be identified and treated as potential triggers. Furthermore, the service provider should negotiate contracts with unregulated service providers in accordance with ATM/ANS.OR.B.015 'Contracted activities' that place a responsibility on such organisations to inform them of planned changes to their services.

**AMC1 ATM/ANS.OR.B.005(d) Management system**  
REACTION TO UNDERPERFORMANCE OF FUNCTIONAL SYSTEMS

If the cause of the underperformance is found to be:

- (a) a flaw in the functional system, the service provider should initiate a change to the functional system either to remove the flaw or mitigate its effects;
- (b) a flawed argument associated with a change to that functional system, the service provider should either:
  - (1) provide a valid argument; or



- (2) where the service provider considers it more feasible, initiate a change to the functional system.

**AMC1 ATM/ANS.OR.B.010(a) Change management procedures**

## GENERAL

- (a) The procedures, and the modification of the procedures, used by a service provider to manage changes should cover the complete lifecycle of a change.
- (b) The service provider should show that the procedures address all the actions and all the evidence needed in order to comply with the requirements laid down in ATM/ANS.OR.A.045, ATS.OR.205, ATS.OR.210, and ATM/ANS.OR.C.005, as appropriate. For that purpose, the service provider should use a compliance matrix, which shows:
- (1) which part of a procedure addresses which part of the Regulation (i.e. the requirement of the Implementing Rule); and
  - (2) the rationale explaining how the procedures demonstrate compliance with the Regulation.
- (c) The service provider should ensure that the roles and responsibilities for the change management processes are identified in the procedures.
- (d) Procedures should be submitted in a manner agreed between the service provider and the CA. Until an agreement is reached, the CA will prescribe the means of submission.
- (e) The procedure that defines the notification process for changes includes:
- (1) the point of contact in charge of the notification of changes, e.g. person, or part of the organisation and the role;
  - (2) the means used for notification, e.g. fax, email, mail, use of database or others.
- (f) The management of change procedures (ATM/ANS.OR.B.010(a)) should include a change identification procedure. This procedure, which is a precursor of the change notification process, should seek out potential changes, confirm that there is a real intent to implement them (propose the change) and, if so, initiate the notification process.

**GM1 ATM/ANS.OR.B.010(a) Change management procedures**

## GENERAL

- (a) The scope of procedures spans the identification of proposed changes, the approval of the change, as well as the monitoring criteria to ensure that the change will remain acceptably safe as long as it is in operation. The monitoring of the change is part of the activities related to the management system of the service providers, but it is not covered by the change management procedures themselves. The procedures that manage changes to functional systems do not include the process to identify the circumstances that will trigger the change. This is part of the management system (see ATM/ANS.OR.B.005(a)(4)). However, the procedures that manage changes to functional systems do include the identification of the scope of the change, i.e. the identification of what parts of the functional system are to be changed.
- (b) The change management procedures should address the following:
- (1) procedural-oriented content, which details:



- (i) the roles and activities with regard to change management, safety assessment and safety support assessment;
  - (ii) the identification of the parts of the functional system affected by the proposed change;
  - (iii) the type of safety assessment or safety support assessment that has to be used for the identified type of changes;
  - (iv) the competence of the persons performing change management, safety assessments and safety support assessments;
  - (v) the identified triggers for performing a safety assessment and a safety support assessment;
  - (vi) the means<sup>143</sup> of change notification;
  - (vii) the means of identifying any organisations or aviation undertakings using the service potentially affected by the change; and
  - (viii) the means of informing those identified in (vii).
- (2) Method-oriented content, which details description of the safety assessments and safety support assessments methods and mitigation methods used by the service provider.
- (c) For each change management procedure or part of a change management procedure approved, the agreement on notification of any change over them should be documented and formalised. In any case, the service provider should keep records of these changes.

---

<sup>143</sup> 'Means' include the form of notification.



**GM2 ATM/ANS.OR.B.010(a) Change management procedures**

EXAMPLE OF COMPLIANCE MATRIX FOR CHANGE MANAGEMENT PROCEDURES APPROVAL

The following is provided as an example of a compliance matrix in which the service provider shows the compliance status of their change management procedures, i.e. those required by AMC1 ATM/ANS.OR.B.010(a).

<b>Service provider</b>	[Name of the provider]								
<b>Provided services</b>	ATS: <input type="checkbox"/>	C: <input type="checkbox"/>	N: <input type="checkbox"/>	S: <input type="checkbox"/>	MET: <input type="checkbox"/>	AIS: <input type="checkbox"/>	DAT: <input type="checkbox"/>	ASM: <input type="checkbox"/>	ATFCM: <input type="checkbox"/>
<b>Date</b>	MM/DD/YYYY								
<b>Version of the form</b>	Vx.y								
<b>Submitted procedure(s)</b>	Procedure 'XYZ' — version 'a.b' of MM/DD/YYYY								
	Procedure 'JKL' — version 'c.d' of MM/DD/YYYY								
	[...]								



Requirement in the Regulation	Acceptable Means of Compliance	Procedure	Rationale	Status	Competent Authority comment
ATM/ANS.OR.A.045(c)	None	Procedure 'JKL' — version 'c.d' — §4	§4 states that the transition into operation of any functional change will occur following the completion of the activities required by the procedures XYZ, MNO, and ABC	Non-approved	To be assessed
ATM/ANS.OR.A.045(d)	AMC1 ATM/ANS.OR.A.045(d)	Procedure 'XYZ' — version 'a.b' — §3	§3 stresses that a change subject to CA review should not be allowed to be put into service before formal approval has been granted.	Approved	None



**GM3 ATM/ANS.OR.B.010(a) Change Management Procedures**  
LIAISON WITH THE COMPETENT AUTHORITY

A service provider may liaise with the CA before submitting new complex change management procedures or before significant modification to an existing and previously approved change management procedure, so as to be able to explain the critical issues related to the procedures and the rationale for them.

**AMC2 ATM/ANS.OR.B.010(a) Change management procedures**  
REGISTER OF NOTIFIED CHANGES

As part of the change management procedures the service provider should keep a register of the records of all notified changes.

- (a) The register should include:
- (1) the status of the implementation of the change, i.e. planned, under review, under implementation, implemented, or cancelled;
  - (2) the notification;
  - (3) (a link to) the location of the actual record, including a reference to all information passed to the CA as per ATM/ANS.OR.A.045(a)(2).
- (b) In addition, when the changes are selected for review, the register should also include:
- (1) the review decision from the competent authority; and
  - (2) a link to records of the change approval by the competent authority.

**SUBPART C — SPECIFIC ORGANISATIONAL REQUIREMENTS FOR SERVICE PROVIDERS OTHER THAN AIR TRAFFIC SERVICES PROVIDERS****GM1 ATM/ANS.OR.C.005(a)(1) Safety support assessment and assurance of changes to the functional system**  
GENERAL

- (a) The safety support assessment should be conducted by the service provider itself. It may also be carried out by another organisation, on its behalf, provided that the responsibility for the safety support assessment remains with the service provider.
- (b) A safety support assessment needs to be performed when a change affects a part of the functional system managed by a service provider other than an air traffic services provider and it is being used in the provision of its services. The safety support assessment or the way it is conducted does not depend on whether the change is a result of a business decision or a decision to improve the service performance.



**GM2 ATM/ANS.OR.C.005(a)(1) Safety support assessment and assurance of changes to the functional system**

## PROVISION OF SAFETY SUPPORT ASSESSMENTS BY COMPOUND PROVIDERS

Guidance on the need to carry out safety support assessment is given below for organisations that consist of more than one provider.

- (a) Only air traffic services providers can perform a safety assessment. If an air traffic services provider uses a service provided by a service provider other than an air traffic services provider, and both are within the same organisation, a safety assessment can also be performed. Service providers other than air traffic services providers cannot be responsible for or perform a safety assessment for the use of their services. Service providers other than air traffic services providers can only perform a safety support assessment to determine that the new or changed service behaves only as specified in a specified context.
- (b) A safety support assurance must be carried out by a service provider other than an air traffic services provider, for changes to the way the ATM/ANS services that cross the organisation's boundary behave.
- (c) If the organisation chooses not to perform a safety support assessment for changes to its internally delivered ATM/ANS services, i.e. ones that do not cross the organisation's boundaries, the effect of the changes on the services that cross the organisation's boundary must be included in an assessment of those services.
- (d) In some cases, it may be seen to be of commercial benefit for safety support cases to be produced by a service provider other than an air traffic services provider, for changes to the ways the services it provides internally behave, i.e. ones that do not cross the organisation's boundary and, therefore, do not require a safety support assessment.

**GM3 ATM/ANS.OR.C.005(a)(1) Safety support assessment and assurance of changes to the functional system**

## SAFETY SUPPORT ASSESSMENT

- (a) A safety support assessment is needed<sup>144</sup> whenever the functional system of a service provider other than an air traffic services provider changes. This may be as a result of:
  - (1) the provider proposing a change to:
    - (i) its functional system;
    - (ii) the services it provides;
    - (iii) the context in which its functional system operates; or
    - (iv) the context in which the service is provided;
  - (2) the services used by the provider in the delivery of its services being planned to change; or/and
  - (3) a change to the context in which the service provider's functional system operates as a result of a proposed change by another service provider, another organisation regulated by Regulation (EC) No 216/2008 or an unregulated body.

<sup>144</sup> For an explanation of why this is the case, see Section 2.3 of Appendix I to GM1 to Article 5 & Article 6(c).





- (b) The size of the safety support case report will depend on:
- (1) the scope of the change;
  - (2) the nature and number of arguments; and
  - (3) the necessary and sufficient evidence needed to provide appropriate confidence that the safety support assurance is valid (complete and correct).

If there is sufficient data to show that the service behaves as specified in a given context, a safety support assessment can be very small. In these cases, it could be a few sheets of paper.

#### **GM4 ATM/ANS.OR.C.005(a)(1) Safety support assessment and assurance of changes to the functional system**

##### SCOPE OF THE CHANGE

- (a) The description of the elements being changed includes the nature, functionality, location, performance, maintenance tasks, training and responsibilities of these elements, where applicable. The description of interfaces and interactions, between machines and between humans and machines, should include communication means, e.g. language, phraseology, protocol, format, order and timing and transmission means, where applicable. In addition, it includes the description of the context in which they operate.
- (b) There are two main aspects to consider in evaluating the scope of a change:
- (1) The interactions within the changed functional system.
  - (2) The interactions within the changing functional system, i.e. those that occur during transitions from the current system to the changed system.

As each transition can be treated as a change to the functional system, the identification of both has a common approach described below.

- (c) The scope of the change is defined as the set of the changed components and affected components. In order to identify the impacted components and the changed components, it is necessary to:
- (1) know which components will be changed;
  - (2) know which component's behaviour might be affected by the changed components, although they are not changed themselves; and
  - (3) identify indirectly affected components by:
    - (i) identifying new interactions introduced by the changed or directly affected components;
    - (ii) identifying interactions with changed or directly affected components via the context.

Further directly and indirectly impacted components will be identified as a result of applying the above iteratively to any directly and indirectly impacted components that have been identified previously.

The scope of the change is the set of changed, directly impacted and indirectly impacted components identified when the iteration identifies no new components.

- (d) The context in which the changed service is intended to be provided (see ATM/ANS.OR.C.005(a)(1)(iii)) includes the interface through which the service will be delivered to other service providers.



**GM3 ATM/ANS.OR.C.005(a)(1) Safety support assessment and assurance of changes to the functional system**

## TRAINING

If the change modifies the way people interact with the rest of the functional system, then they will require training before the change becomes operational. Care should be taken when training operational staff before the change is operational, as the training may change the behaviour of the operational staff when they interact with the existing functional system before any other part of the change is made, and so the training may have to be treated as a transitional stage of the change. For example, as a result of training, ATCOs may come to expect information or alerts to be presented differently. People may also need refreshment training periodically in order to ensure that their performance does not degrade over time. The training needed before operation forms part of the design of the change, while the refreshment training is part of the maintenance of the functional system after the change is in operation. For more guidance on this issue, see degraded modes in Section 4.3.1 of Appendix I to GM1 to Article 5 & Article 6(c).

**GM4 ATM/ANS.OR.C.005(a)(1) Safety support assessment and assurance of changes to the functional system**

## INTERACTIONS

The identification of changed interactions is necessary in order to identify the scope of the change because any changed behaviour in the system comes about via a changed interaction. Changed interaction happens via an interaction at an interface of the functional system and the context in which it operates. Consequently, identification of both interfaces and interactions is needed to ensure that all interactions have identified interfaces and all interfaces have identified interactions. From this, all interactions and interfaces that will be changed can be identified.

**AMC1 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system**

## FORM OF ASSURANCE

Service providers other than air traffic services providers, should ensure that the assurance required by ATM/ANS.OR.C.005(a)(2) is documented in a safety support case.

**GM1 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system**

## SPECIFICATION

‘Continues to behave only as specified in the specified context’ means that assurance needs to be provided that the monitoring requirements of ATM/ANS.OR.C.005(b)(2) are suitable for demonstrating that the service behaves only as specified in the specified context during operation.



**GM2 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system**

## ASSURANCE LEVELS

The use of assurance level concepts, e.g. design assurance levels (DAL), software assurance levels (SWAL), hardware assurance levels (HWAL), can be helpful in generating an appropriate and sufficient body of evidence to help establish the required confidence in the argument.

**AMC2 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system**

## COMPLETENESS OF THE ARGUMENT

The argument is considered to be complete when it shows that:

- (a) the safety support assessment of ATM/ANS.OR.C.005(b) has produced a service specification and context specification where:
  - (1) the service has been defined in terms of functionality, performance and the form of the interfaces;
  - (2) the specification of context correctly and completely records the conditions under which the specification of the service is true;
  - (3) the interaction of components, under failure conditions or failures in services delivered to the components, have been assessed for their impact on the service and, where necessary, degraded modes of service have been defined; and
  - (4) the specification encompasses the interaction with the environment;
- (b) safety support requirements have been placed on the elements changed and on those elements affected by the change;
- (c) the behaviour necessitated by the safety support requirements is the complete behaviour expressed by the service specification;
- (d) all safety support requirements have been traced from the service specification to the level of the architecture at which they have been satisfied;
- (e) each component satisfies its safety support requirements; and
- (f) the evidence is derived from known versions of the components and the architecture and known sets of products, data and descriptions that have been used in the production or verification of those versions.

**GM3 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system**

## COMPLETENESS OF THE ARGUMENT

*The structure of paragraphs within this GM relates directly to the structure of paragraphs in AMC2 ATM/ANS.OR.C.005(a)(2) and not to the IR.*

*This GM provides guidance only on the completeness of the argument; it does not deal with the confidence necessary to demonstrate that the change is sufficiently trustworthy.*

- (a) Sufficiency of specifications



The way the service specification is arrived at is not of particular interest in a safety support case and so it is not dealt with here. A specification that is sufficient implies that the service meets the providers intent, i.e. it is valid. Two necessary conditions for a sufficient specification are provided here:

(1) Assessment of failure conditions

- (i) Failures or failure conditions are malfunctions of behaviour. This means either the loss or corruption of some intended behaviour, e.g. behaviour that is considered to be:
  - (A) more than (quantity, information);
  - (B) less than (quantity, information);
  - (C) additional to;
  - (D) faster than;
  - (E) slower than;
  - (F) part of;
  - (G) reverse of;
  - (H) other than;
  - (I) not;
  - (J) earlier than;
  - (K) later than;
  - (L) before; or
  - (M) after

that which was intended. If the behaviour of the service is altered in any way during malfunctions, the altered behaviour needs to be included in the specification. This is further explained in the GM on degraded modes of operation (GM1 ATM/ANS.OR.C.005(b)(1) & (2)).

- (ii) Some failures may not result in a degraded service.
- (iii) Some failures may not be relevant in the context of use.
- (iv) Strictly speaking, the failure and failure conditions described here are malfunctions of the services delivered by a component and may be caused by failures of components, errors in design or failures of services used by the component.
- (v) When a redundancy within a component is no longer available, the behaviour of the component is considered to have changed, e.g. the reliability of the component will have changed and an indication of the loss of redundancy will have been provided.

(2) Interaction with the environment

It is necessary to argue that the behaviour of the implementation, i.e. the system as built, matches the specification and there is no additional (unspecified) behaviour. This implies verification of service behaviour, which is required by ATM/ANS.OR.C.005(b)(2) and stated here in a more specific way.



- (b) Safety support requirements
- (1) Safety support requirements are requirements whose implementation will affect the context of operation. However, if it is hard to argue that a valid requirement is not a safety support requirement, it may be better to treat it as a safety support requirement.
  - (2) In the terminology used within this GM, requirements are design artefacts that lead to an implementation, while specifications are the result of verifying an implementation in a given context. Consequently, when verified and no difference is found between the observed behaviour and the required behaviour of the system, the requirements become the specification.
  - (3) The highest-level safety support requirements represent the desired behaviour of the change at its interface with the operational context. These, ultimately become the specification, once the implementation is verified. The important aspects of safety support requirements are their properties, their relationships, their completeness, their consistency and their validity.
  - (4) Safety support requirements are introduced for the following reasons:
    - (i) In almost all cases, verification that a system behaves as specified cannot be accomplished, to an acceptable level of confidence, at the level of its interface with its operational environment.
    - (ii) In order to be able to verify the system, it should be decomposed into verifiable parts. Verification relies on requirements placed on these parts via a hierarchical decomposition of the top-level requirements, in accordance with the constraints imposed by the chosen architecture.
    - (iii) At the lowest level, this decomposition places requirements on elements, where verification that the implementation satisfies its requirements can be achieved by testing.
    - (iv) At higher levels in the architecture, during integration, verified elements of different types are combined into subsystems/components, in order to verify more complete parts of the system.
    - (v) While they cannot be fully tested, other verification techniques may be used to provide sufficient levels of confidence that these subsystems/components do what they are supposed to do.
    - (vi) Consequently, since decomposing the system into verifiable parts relies on establishing requirements for those parts, then safety support requirements are necessary.
  - (5) The way safety support requirements are arrived at is not of particular interest in a safety support case because a safety support case is the argument for the trustworthiness of the specification and is not about how the specification was developed.
  - (6) The architecture does not have requirements. During development, the need to argue satisfaction of system level requirements, which cannot be performed at the system level for any practical system, drives the architecture because verifiability depends on the decomposition of the system into verifiable parts.
  - (7) Demonstration that safety support requirements at system level are met allows them to be transformed into the safety support specification.



## (c) Completeness of safety support requirements

- (1) The concept underpinning AMC2 ATM/ANS.OR.C.005(a)(2) is that, provided each subsystem/component/element meets its requirements, the system will behave as specified. This will be true provided (2), (3) and (4) below are met.
- (2) The activity needed to meet objective (c) of AMC2 ATM/ANS.OR.C.005(a)(2) consists of obtaining sufficient confidence that the set of requirements is complete and correct, i.e. that:
  - (i) the architectural decomposition leads to a complete and correct set of requirements being allocated to each subsystem/component/element;
  - (ii) each requirement is a correct, complete and unambiguous statement of the desired behaviour, and does not contradict another requirement or any other subset of requirements; and
  - (iii) the requirements allocated to a subsystem/component/element necessitate the complete required behaviour of the subsystem/component/element in the target environment.
- (3) This should take into account specific aspects such as:
  - (i) the possible presence of functions within the subsystem/component/element that produce unnecessary behaviour. For instance, in the case where a previously developed part is used, activities should be undertaken to identify all the possible behaviours of the part. If any of these behaviours is not needed for the foreseen use, then additional requirements may be needed to make sure that these functions are not solicited or inadvertently activated in operation or that the effects of any resulting behaviour are mitigated;
  - (ii) subsystem/component/element requirements that are not directly related to the desired behaviour of the functional system. This kind of requirement can, for instance, ask that the subsystem/component/element be developed in a given syntax or be designed in a certain way. These requirements often relate to technical aspects of the subsystem/component/element. Activities should be undertaken to ensure that each of these requirements is a correct, complete and unambiguous statement of the desired effect, and does not contradict another requirement or any other subset of requirements.
- (4) In the context of a service delivered by a service provider other than an air traffic services provider, the complete behaviour is not complete in the sense that it comprises all possible behaviours of the service in all possible contexts, but is complete in the sense that the specification is only true for the defined context. This restriction to the context of the use of the service makes safety support assessment and assurance of changes to the functional system a practical proposition.

## (d) Traceability of requirements

The traceability requirement can be met by tracing to the highest level element in the architectural hierarchy that has been shown to satisfy its requirements, by verifying it in isolation. It is likely and completely acceptable that this point will be reached at a different architectural level for each element.

## (e) Satisfaction of safety support requirements



- (1) The component view taken must be able to support verification, i.e. the component must be verifiable — see guidance in (b).
  - (2) Care should be taken in selecting subsystems that are to be treated as components for verification to ensure that they are small and simple enough to be verifiable.
  - (3) The context argument needs to demonstrate that the context in which a component is verified does not compromise the claim that the specification is true over a specified context, i.e. the component verification context is correctly related to the context claimed for the operation of the functional system.
- (f) Configuration identification
- (1) This is only about configuration of the evidence and should not be interpreted as configuration management of the changed functional system. However, since the safety support case is based on a set of elements and the way they are joined together, the safety support case will only be valid if the configuration remains as described in the safety support case. This guidance has been given in ‘Maintenance of configuration’ and is provided in GM1 ATM/ANS.OR.C.005(b)(1) & (2).
  - (2) Evidence for the use of the same component in different parts of the system or in different systems should probably not rely on testing in a single context since it is unlikely that the contexts for each use will be the same or can be covered by a single set of test conditions. This applies equally to the reuse of evidence gathered from testing subsystems.

#### **GM4 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system**

##### **SAFETY SUPPORT REQUIREMENTS**

The complete behaviour is limited to the scope of the change. Safety support requirements only apply to the parts of a system affected by the change. In other words, if parts of a system can be isolated from each other and only some parts are affected by the change, then these are the only parts that are of concern and so will have safety support requirements attached to them.

The following list contains examples, not exhaustive, of safety support requirements that specify:

- (a) for equipment, the complete behaviour, in terms of functions, accuracy, timing, order, format, capacity, resource usage, robustness to abnormal conditions, overload tolerance, availability, reliability, confidence and integrity;
- (b) for people, their complete expected behaviour and performance in terms of tasks, accuracy, response times, acceptable workload, resilience to distraction, self-awareness, ‘team-playerness’, adaptability, reliability, confidence, skills, and knowledge in relation to their tasks;
- (c) for procedures, the circumstances for their enactment, the resources needed to perform the procedure (i.e. people and equipment), the sequence of actions to be performed and the timing and accuracy of the actions; and
- (d) interactions between all parts of the system.

#### **AMC3 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system**

##### **DETERMINATION OF THE SPECIFICATION OF THE CHANGED SERVICE**



When determining the changes in the service specification that have resulted from the change to the functional system, service providers other than air traffic services providers, should ensure that:

- (a) the properties specified for the service can be observed and measured either directly or indirectly with a degree of certainty commensurate with the level of confidence sought from assurance; and
- (b) the specification of the changed service must cover everything that has changed in the service provided when operated within the declared operational context.

**AMC4 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system**

DETERMINATION OF THE OPERATIONAL CONTEXT FOR THE CHANGE

- (a) When determining the operational context for the change service providers, other than an air traffic services provider, should ensure that:
  - (1) the specification of the operational context can be shown to be true for all circumstances and environments in which the changed service is intended to operate;
  - (2) the operational context is completely and coherently specified; and
  - (3) The specification of the operational context is internally consistent; and
- (b) The operational context must be specified so that its adherence to (1) and (2) is observable and measurable either directly or indirectly with a degree of certainty commensurate with the level of confidence sought from assurance.

**AMC1 ATM/ANS.OR.C.005(b)(1) Safety support assessment and assurance of changes to the functional system**

VERIFICATION

Service providers other than air traffic services providers should ensure that verification activities of the safety support assessment process include:

- (a) verification that the full scope of the change is addressed throughout the whole assessment process, i.e. all the elements that are changed and those elements of the functional system or environment of operation that depend upon them and on which they depend;
- (b) verification that the way the service behaves complies with and does not contradict any requirements placed on the changed service by another part of the regulations or conditions attached to the providers certificate;
- (c) verification that the specification of the way the service behaves is complete and correct;
- (d) verification that the specification of the operational context is complete and correct;
- (e) verification that the specification was for the service analysed in the context specified by the operational context; and
- (f) verification, to the intended degree of confidence, that the implementation behaves only as specified in the given operational context.

**GM1 ATM/ANS.OR.C.005(b)(1) Safety support assessment and assurance of changes to the functional system**





## NO SAFETY SUPPORT REQUIREMENTS AT SYSTEM LEVEL

- (a) As the complete behaviour of the change is reflected in the specification of the service and the context, no safety support requirements need to be placed at system or change level. Nevertheless, safety support requirements can be placed on the elements affected by the change. This is addressed in AMC2 ATM/ANS.OR.C.005(a)(2).
- (b) Safety hazards, safety criteria, safety risk analysis and safety risk evaluation are not relevant to the safety support assessment because the service provider does not know how the service will be used.

**GM1 ATM/ANS.OR.C.005(b)(1) Safety support assessment and assurance of changes to the functional system**

## VERIFICATION

This requirement is seeking verification because it is a simple cross-check of available material, i.e. that the specification reflects the requirements of other parts of this Regulation.

## (a) Behaviour

ATM/ANS.OR.C.005(b)(1)(ii) requires that the service meets its specification. Consequently, the specification must be complete and valid, i.e. it includes the behaviour addressed in ATM/ANS.OR.C.005(b)(1)(iii) and any additional behaviour in the specified context.

## (b) Compliance with other requirements

- (1) ATM/ANS.OR.C.005(b)(1)(iii) requires the service providers to identify all parts of this Regulation that impose behaviour on the changed service and also includes any conditions attached to the certificate. They have to identify only those parts of this Regulation that describe required behaviour relevant to the changed service. The identified behaviour shall be included in the specification of the changed service.

Note that the Regulation or conditions attached to the certificate may render compliance with technical standards and ICAO SARPS mandatory.

- (2) Compliance with other non-mandatory standards may also be a necessary condition for other reasons.
- (3) ATM/ANS.OR.C.005(b)(1)(iii) does not state that the service only meets the requirements of the other parts of this Regulation. It may do other things as well, as described in (5) below.
- (4) In ATM/ANS.OR.C.005(b)(1)(iii) 'does not contradict' is used to express the concern that behaviour beyond that required by a standard might cause the behaviour required by the standard to be undermined.
- (5) The behaviour of a service is likely to include behaviour unspecified in standards; such behaviour may come from:
  - (i) the behaviour of degraded modes of operation;
  - (ii) additional behaviour not required by the standard, but put there for commercial purposes, e.g. competitive edge; or
  - (iii) other behaviour identified by the customer, e.g. an air traffic services provider.



- (6) Consequently, the total behaviour that must be specified includes mandatory behaviour and additional behaviour whether wanted or not wanted.

**AMC1 ATM/ANS.OR.C.005(b)(2) Safety support assessment and assurance of changes to the functional system**

**MONITORING**

Service providers, other than an air traffic services provider, should ensure that within the safety support assessment process for a change, the monitoring criteria that are to be used to demonstrate that the safety support case remains valid during the operation of the changed functional system, i.e. that the changed service continues to meet its specification, are identified and documented. These criteria should be such that:

- (a) they indicate that the assumptions made in the safety support case remain valid; and
- (b) if the properties being monitored remain within the bounds set by these criteria, the service will be behaving as specified.

**GM1 ATM/ANS.OR.C.005(b)(2) Safety support assessment and assurance of changes to the functional system**

**MONITORING OF INTRODUCED CHANGES**

- (a) Monitoring is intended to maintain confidence in the safety support case during operation of the changed functional system. Monitoring is, therefore, only applicable following the entry into service of the change. This is further explained in paragraph (c)(11) in Section 3.2 of Appendix I to GM1 to Article 5 & Article 6(c), where the monitoring referred to here is called 'permanent monitoring'.
- (b) Monitoring is likely to be of internal parameters of the functional system that provide a good indication of the performance of the service. These parameters may not be directly observable at the service level, i.e. at the interface of the service with the operational environment. For example, where a function is provided by multiple redundant resources, the availability of the function will be so high that monitoring it may not be useful. However, monitoring the availability of individual resources, which fail much more often, may be a useful indicator of the performance of the overall function.



**ACCEPTABLE MEANS OF COMPLIANCE AND GUIDANCE MATERIAL  
TO ANNEX IV — SPECIFIC REQUIREMENTS FOR THE PROVISION OF AIR TRAFFIC SERVICES  
(PART-ATS)**

**SUBPART A — ADDITIONAL ORGANISATION REQUIREMENTS FOR THE PROVISION OF AIR TRAFFIC SERVICES  
(ATS.OR)**

**GM1 ATS.OR.205(a)(1) Safety assessment and assurance of changes to the functional system**

GENERAL

- (a) The safety assessment should be conducted by the provider itself. It may also be carried out by another organisation, on its behalf, provided that the responsibility for the safety assessment remains with the air traffic services.
- (b) A safety assessment needs to be performed when a change affects a part of the functional system managed by the provider of air traffic services and that is being used in the provision of its (air traffic) services. The safety assessment or the way it is conducted does not depend on whether the change is a result of a business decision or a decision to improve safety.

**GM2 ATS.OR.205(a)(1) Safety assessment and assurance of changes to the functional system**

SCOPE OF THE CHANGE

- (a) The description of the elements being changed includes the nature, functionality, location, performance, maintenance tasks, training and responsibilities of these elements, where applicable. The description of interfaces and interactions, between machines and between humans and machines, should include communication means, e.g. language, phraseology, protocol, format, order and timing and transmission means, where applicable. In addition, it includes the description of the context in which they operate.
- (b) There are two main aspects to consider in evaluating the scope of a change:
  - (1) The interactions within the changed functional system;
  - (2) The interactions within the changing functional system, i.e. those that occur during transitions from the current functional system to the changed functional system.

As each transition can be treated as a change to the functional system, the identification of both have a common approach described below.
- (c) The scope of the change is defined as the set of the changed components and affected components. In order to identify the affected components and the changed components, it is necessary to:
  - (1) know which components will be changed;
  - (2) know which component's behaviour might be directly affected by the changed components, although they are not changed themselves;
  - (3) identify indirectly affected components by:
    - (i) identifying new interactions introduced by the changed or directly affected components; and/or
    - (ii) identifying interactions with changed or directly affected components via the environment.



- (4) Furthermore, directly and indirectly affected components will be identified as a result of applying the above iteratively to any directly and indirectly affected components that have been identified previously.

The scope of the change is the set of changed, directly impacted and indirectly impacted components identified when the iteration identifies no new components.

- (d) The context in which the changed service is intended to operate (see ATS.OR.205(a)(1)(iii)) includes the interface through which the service will be delivered to its users.

### **GM3 ATS.OR.205(a)(1) Safety assessment and assurance of changes to the functional system** TRAINING

If the change modifies the way people interact with the rest of the functional system, then they will require training before the change becomes operational. Care should be taken when training operational staff before the change is operational, as the training may change the behaviour of the operational staff when they interact with the existing functional system before any other part of the change is made, and so may have to be treated as a transitional stage of the change. For example, as a result of training, ATCOs may come to expect information or alerts to be presented differently. People may also need refreshment training periodically in order to ensure that their performance does not degrade over time. The training needed before operation forms part of the design of the change, while the refreshment training is part of the maintenance of the functional system after the change is in operation. For more guidance on this issue, see degraded modes in Section 4.3 of Appendix I to GM1 to Article 5 & Article 6(2).

### **GM4 ATS.OR.205(a)(1) Safety assessment and assurance of changes to the functional system** DESCRIPTION OF THE SCOPE — MULTI-ACTOR CHANGE

In the case where the change is a multi-actor change, in accordance with ATM/ANS.OR.A.045(e), the interfaces and interactions described in GM1 ATS.OR.205(b)(1)(iii) include the interfaces with the other providers and organisations that are also affected by the change. Information related to cooperatively identifying the scope of multi-actor changes may be found in EUROCAE ED-78A.

### **GM1 ATS.OR.205(b)(1)(iii) Safety assessment and assurance of changes to the functional system** INTERACTIONS

The identification of changed interactions is necessary in order to identify the scope of the change because any changed behaviour in the system comes about via a changed interaction. Changed interaction happens via an interaction at an interface of the functional system and the context in which it operates. Consequently, identification of both interfaces and interactions is needed to be sure that all interactions have identified interfaces and all interfaces have identified interactions. From this, all interactions and interfaces that will be changed can be identified.

### **AMC1 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system** FORM OF ASSURANCE

The air traffic services provider should ensure that the assurance required by ATS.OR.205(a)(2) is documented in a safety case .

### **GM1 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system** SAFETY CRITERIA



'Safety criteria will remain satisfied' means that the safety criteria continue to be satisfied in operation after the change is implemented and put into operation. The safety case needs to provide assurance that the monitoring requirements of ATS.OR.205(b)(6) are suitable for demonstrating, during operation, that the safety criteria remain satisfied and, therefore, the argument remains valid.

### **GM2 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system** ASSURANCE LEVELS

The use of assurance level concepts, e.g. design assurance levels (DAL), software assurance levels (SWAL), hardware assurance levels (HWAL), can be helpful in generating an appropriate and sufficient body of evidence to help establish the required confidence in the argument.

### **AMC2 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system** COMPLETENESS OF THE ARGUMENT

The argument is to be considered to be complete when it shows that:

- (a) the safety assessment in ATS.OR.205(b) has produced a sufficient set of non-contradictory valid safety criteria;
- (b) safety requirements have been placed on the elements changed and on those elements affected by the change;
- (c) the behaviour necessitated by these safety requirements meets the safety criteria;
- (d) all safety requirements have been traced from the safety criteria to the level of the architecture at which they have been satisfied;
- (e) each component satisfies its safety requirements;
- (f) each component's behaviour, within the context in which it is intended to operate, does not adversely affect safety; and
- (g) the evidence is derived from known versions of the components and the architecture and known sets of products, data and descriptions that have been used in the production or verification of those versions.

### **GM3 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system** COMPLETENESS OF THE ARGUMENT

*The structure of paragraphs within this GM relates directly to the structure of paragraphs in AMC2 ATS.OR.205(a)(2) and not to the IR. This GM provides guidance only on the completeness of the argument it does not deal with the confidence necessary to demonstrate that the change is sufficiently safe.*

- (a) Sufficiency of safety criteria
  - (1) A sufficient set of safety criteria is one where the safety goal of the change is validly represented by the set of individual safety criteria, each criterion of which must be valid in its own right and not contradict another criterion or any other subset of criteria. A valid criterion is a correct, complete and unambiguous statement of the desired property. An individual valid criterion does not necessarily represent a complete safety criterion. An example of an invalid criterion is that the max take-off weight must not exceed 225 Tonnes because weight is measured in Newtons and not in Tonnes. An example of an incomplete criterion is that the accuracy must be 5 m because no



reliability attribute is present. This implies it must always be within 5 m, which is impossible in practice.

- (2) Optimally, a sufficient set of criteria would consist of the minimum set of non-overlapping valid criteria and it is preferable to a set containing overlapping criteria.
  - (3) Criteria that are not relevant, i.e. ones that do not address the safety goal of the change at all, should be removed from the set as they contribute nothing, may contradict other valid criteria and may serve to confuse.
  - (4) There are two forms of overlap: complete overlap and partial overlap.
    - (i) In the first case, one or more criteria can be removed and the set would remain sufficient, i.e. there are unnecessary criteria.
    - (ii) In the second case, (partially overlapping criteria) if any criterion were to be removed, the set would not be sufficient. Consequently, all criteria are necessary; however, validating the set would be much more difficult. Showing that a set of criteria with significant overlap do not contradict each other is extremely difficult and consequently prone to error.
  - (5) It may, in fact, be simpler to develop an architecture that supports non-overlapping criteria than to attempt to validate a partially overlapping set of criteria.
- (b) Safety requirements are requirements hierarchically decomposed from safety criteria. They proscribe and prescribe behaviour that will ensure safety.
- (1) Safety criteria represent the desired safety behaviour of the change at its interface with the operational context. The important aspects of safety criteria are their properties, their relationships, their completeness, their consistency and their validity.
  - (2) Safety requirements are introduced for the following reasons:
    - (i) In almost all cases, verification that a system behaves as specified cannot be accomplished, to an acceptable level of confidence, at the level of its interface with its operational environment.
    - (ii) In order to be able to verify the system, it should be decomposed into verifiable parts. Verification relies on requirements placed on these parts via a hierarchical decomposition of the top level requirements, in accordance with the constraints imposed by the chosen architecture.
    - (iii) At the lowest level, this decomposition places requirements on elements, where verification that the implementation satisfies its requirements can be achieved by testing.
    - (iv) At higher levels in the architecture, during integration, verified elements of different types are combined into subsystems/components, in order to verify more complete parts of the system.
    - (v) While they cannot be fully tested, other verification techniques may be used to provide sufficient levels of confidence that these subsystems/components do what they are supposed to do.



- (vi) Consequently, since decomposing the system into verifiable parts relies on establishing requirements for those parts, then safety requirements are necessary.
- (3) The architecture does not have requirements. During development, the need to argue satisfaction of safety criteria, which cannot be performed at the system level for any practical system, drives the architecture because verifiability depends on the decomposition of the system into verifiable parts.
- (c) Satisfaction of safety criteria
  - (1) The concept underpinning AMC2 ATS.OR.205(a)(2) is that, provided each element meets its safety requirements, the system will meet its safety criteria. This will be true provided (2) and (3) below are met.
  - (2) The activity needed to meet this objective consists of obtaining sufficient confidence that the set of safety requirements is complete and correct, i.e. that:
    - (i) the architectural decomposition of the elements leads to a complete and correct set of safety requirements being allocated to each sub-element;
    - (ii) each safety requirement is a correct, complete and unambiguous statement of the desired behaviour and does not contradict another requirement or any other subset of requirements; and
    - (iii) the safety requirements allocated to an element necessitate the complete required safety behaviour of the element in the target environment.
  - (3) This should take into account specific aspects such as:
    - (i) the possible presence of functions within the element that produce unnecessary behaviour. For instance, in the case where a previously developed element is used, activities should be undertaken to identify all the possible behaviours of the element. If any of these behaviours is not needed for the foreseen use, then additional requirements may be needed to make sure that these functions will not be solicited or inadvertently activated in operation or that the effects of any resulting behaviour are mitigated;
    - (ii) element requirements that are not directly related to the desired behaviour of the functional system. This kind of requirement can, for instance, ask that the element be developed in a given syntax or be designed in a certain way. These requirements often relate to technical aspects of the element. Activities should be undertaken to ensure that each of these requirements is a correct, complete and unambiguous statement of the desired effect and does not contradict another requirement or any other subset of requirements.
- (d) Traceability of requirements

The traceability requirement can be met by tracing to the highest level element in the architectural hierarchy that has been shown to satisfy its requirements, by verifying it in isolation. It is likely and completely acceptable that this point will be reached at a different architectural level for each element.
- (e) Satisfaction of safety requirements



- (1) The component view taken must be able to support verification, i.e. the component must be verifiable.
  - (2) Care should be taken in selecting subsystems that are to be treated as components for verification to ensure that they are small and simple enough to be verifiable.
- (f) Adverse effects on safety
- (1) Interactions of all changed components or components affected by the change, operating in their defined context, have to be identified and assessed for safety in order to be able to show that they do not adversely affect safety. This assessment must include the failure conditions for all components and the behaviour of the services delivered to the component including failures in those services.
  - (2) Interactions in complex systems are dealt with in ATM/ANS.OR.A.045(e)(1).
- (g) Configuration identification
- (1) AMC2 ATS.OR.205(a)(2)(f) is only about configuration of the evidence and should not be interpreted as configuration management of the changed functional system. However, since the safety case is based on a set of elements and the way they are joined together, the safety case will only be valid if the configuration remains as described in the safety case. Guidance on 'Maintenance of configuration' is provided in Section 4.3 of Appendix I to GM1 to Article 5 & Article 6(c)
  - (2) Evidence for the use of the same component in different parts of the system or in different systems should probably not rely on testing in a single context since it is unlikely that the contexts for each use will be the same or can be covered by a single set of test conditions. This applies equally to the reuse of evidence gathered from testing subsystems.

#### **GM4 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system**

##### **SAFETY REQUIREMENTS**

The following list contains examples, not exhaustive, of safety requirements that specify:

- (a) for equipment, the complete behaviour, in terms of functions, accuracy, timing, order, format, capacity, resource usage, robustness to abnormal conditions, overload tolerance, availability, reliability, confidence and integrity;  
  
The complete behaviour is limited to the scope of the change. Safety support requirements only apply to the parts of a system affected by the change. In other words, if parts of a system can be isolated from each other and only some parts are affected by the change, then these are the only parts that are of concern and so will have safety support requirements attached to them
- (b) for people, their complete expected behaviour and performance in terms of tasks, accuracy, response times, acceptable workload, reliability, confidence, skills, and knowledge in relation to their tasks;
- (c) for procedures, the circumstances for their enactment, the resources needed to perform the procedure (i.e. people and equipment), the sequence of actions to be performed and the timing and accuracy of the actions; and
- (d) interactions between all parts of the system.





**GM1 ATS.OR.205(b) Safety assessment and assurance of changes to the functional system**

## PROPORTIONALITY OF SAFETY ASSESSMENT

Air traffic services providers may carry out safety assessment in a way that is commensurate with the type and nature of the change and its impact on safety.

**GM2 ATS.OR.205(b) Safety assessment and assurance of changes to the functional system**

## SAFETY ASSESSMENT METHODS

- (a) The air traffic services provider can use a standard safety assessment method or it can use its own safety assessment method to assist with structuring the process. However, the application of a method is not a guarantee of the quality of the results. It is therefore not sufficient for a safety case to claim that the assurance provided is adequate due to compliance with a standard or method.
- (b) There are databases available that describe different safety assessment methods, tools and techniques<sup>145</sup> that can be used by the air traffic services provider. The provider must ensure that the safety assessment method is adequate for the change being assessed and that the assumptions inherent in the use of the method are recognised and accommodated appropriately.

**AMC1 ATS.OR.205(b)(1) Safety assessment and assurance of changes to the functional system**

## COMPLETENESS OF HAZARD IDENTIFICATION

The air traffic services provider should ensure that hazard identification:

- (a) targets complete coverage of any condition, event, or circumstance related to the change, which could, individually or in combination, induce a harmful effect;
- (b) has been performed by personnel trained and competent for this task; and
- (c) need only include hazards that are generally considered as credible.

**AMC2 ATS.OR.205(b)(1) Safety assessment and assurance of changes to the functional system**

## HAZARDS TO BE IDENTIFIED

The following hazards should be identified:

- (a) New hazards, i.e. those introduced by the change relating to the:
  - (1) failure of the functional system; and
  - (2) normal operation of the functional system; and
- (b) Already existing hazards that are affected by the change and are related to:
  - (1) the existing parts of the functional systems; and
  - (2) hazards outside the functional system, for example those inherent to aviation.

**GM1 ATS.OR.205(b)(1) Safety assessment and assurance of changes to the functional system**

## HAZARD IDENTIFICATION

- (a) Completeness of hazard identification

<sup>145</sup> For example, <http://www.nlr.nl/downloads/safety-methods-database.pdf> or <http://www.scsc.org.uk/>



In order to achieve completeness in the identification of hazards, it might be beneficial to aggregate hazards and to formulate them in a more abstract way, e.g. at the service level. This might in turn have drawbacks when analysing and evaluating the risk of the hazards. The appropriate level of detail in the set of hazards and their formulation, therefore, depends on the change and the way the safety assessment is executed.

(b) Sources of hazards

- (1) Hazards introduced by failures or nominal operations of the ATM/ANS functional systems may include the following factors and processes:
  - (i) design factors, including equipment, procedural and task design;
  - (ii) operating practices, including the application of procedures under actual operating conditions and the unwritten ways of operating;
  - (iii) communications, including means, terminology, order, timing and language and including human–human, human–machine and machine–machine communications;
  - (iv) installation issues;
  - (v) equipment and infrastructure, including failures, outages, error tolerances, nuisance alerts, defect defence systems and delays; and
  - (vi) human performance, including restrictions due to fatigue and medical conditions, and physical limitations.
- (2) Hazards introduced in the context in which the ATM/ANS functional system operates may include the following factors and processes:
  - (i) wrong, insufficient or delayed information and inadequate services delivered by third parties;
  - (ii) personnel factors, including working conditions, company policies for and actual practice of recruitment, training, remuneration and allocation of resources;
  - (iii) organisational factors, including the incompatibility of production and safety goals, the allocation of resources, operating pressures and the safety culture;
  - (iv) work environment factors such as ambient noise, temperature, lighting, annoyance, ergonomics and the quality of man–machine interfaces; and
  - (v) external threats such as fire, electromagnetic interference and sources of distraction.
- (3) The hazards introduced in the context in which the ATM/ANS services are delivered may include the following factors and processes:
  - (i) errors, failures, non-compliance and misunderstandings between the airborne and ground domains;
  - (ii) traffic complexity, including traffic growth, fleet mix and different types of traffic;
  - (iii) wrong, insufficient or delayed information delivered by third parties;
  - (iv) inadequate service provisioning by third parties; and



- (v) external physical factors, including terrain, weather phenomena, volcanoes and animal behaviour.
- (c) Methods to identify hazards
  - (1) The air traffic services provider may use a combination of tools and techniques, including functional analysis, what if techniques, brain storm sessions, expert judgement, literature search (including accident and incident reports), queries of accident and incident databases in order to identify hazards.
  - (2) The air traffic services provider needs to make sure that the method is appropriate for the change and produces (either individually or in combination) a valid (necessary and sufficient) set of hazards. This may be aided by drawing up a list of the functions associated with part of the functional system being changed. The air traffic services provider needs to make sure their personnel that use these techniques are appropriately trained to apply these methods and techniques.

**AMC1 ATS.OR.205(b)(2) Safety assessment and assurance of changes to the functional system**

## DETERMINATION OF THE SAFETY CRITERIA FOR THE CHANGE

When determining the safety criteria for the change being assessed, the air traffic services provider should, in accordance with ATS.OR.210, ensure that:

- (a) the safety criteria support a risk analysis that is:
  - (1) relative or absolute, i.e. refers to:
    - (i) the difference in safety risk of the system due to the change (relative); or
    - (ii) the difference in safety risk of the system and a similar system (can be absolute or relative); and
    - (iii) the safety risk of the system after the change (absolute); and
  - (2) objective, whether risk is expressed numerically or not;
- (b) the safety criteria are measurable to an adequate degree of certainty;
- (c) the set of safety criteria can be represented totally by safety risks, by other measures that relates to safety risk or a mixture of safety risks and these other measures.
- (d) the set of safety criteria should cover the change; the safety criteria selected are consistent with the overall safety objectives established by the air traffic services provider through its Safety Management System and represented by its annual and business plan and Safety Key Performance Indicators; and
- (e) where a safety risk or a proxy cannot be compared against its related safety criteria without acceptable uncertainty, the safety risk should be constrained and actions should be taken, in the long term, so as to manage safety and ensure that the air traffic services provider's overall safety objectives are met.

**AMC1 ATS.OR.205(b)(3) Safety assessment and assurance of changes to the functional system**

## COMPLETENESS OF RISK ANALYSIS

The air traffic services provider should ensure that the risk analysis is carried out by personnel trained and competent to perform this task and should also ensure that:



- (a) a complete list of harmful effects in relation to the identified:
  - (1) hazards, when the safety criteria is expressed in terms of safety risk; or
  - (2) proxies, when the safety criteria is expressed in relation to proxies; and
  - (3) hazards introduced due to implementation is produced; and
- (b) the risk contributions of all hazards and proxies are evaluated;
- (c) risk analysis is conducted in terms of risk or in terms of proxies or a combination of them, using specific measurable quantities that are related to operational safety risk; and
- (d) results can be compared against the safety criteria.

**AMC2 ATS.OR.205(b)(3) Safety assessment and assurance of changes to the functional system**  
SEVERITY CLASSIFICATION OF ACCIDENTS LEADING TO HARMFUL EFFECTS

When performing a risk analysis in terms of risk, the air traffic services provider should ensure that the harmful effects of all hazards are allocated a safety severity category and that, where there is more than one safety severity category of harm, any severity classification scheme satisfies the following criteria:

- (a) The scheme is independent of the causes of the accidents that it classifies, i.e. the severity of the worst accident does not depend upon whether it was caused by an equipment malfunction or human error;
- (b) The scheme permits unique assignment of every harmful effect to a severity category;
- (c) The severity categories are expressed in terms of a single scalar quantity and in terms relevant to the field of their application;
- (d) The level of granularity (i.e. the span of the categories) is appropriate to the field of their application;
- (e) The scheme is supported by rules for assigning a harmful effect unambiguously to a severity category; and
- (f) The scheme is consistent with the air traffic services providers views of the severity of the harmful effects covered and can be shown to incorporate societal views of their severity.

**AMC1 ATS.OR.205(b)(4) Safety assessment and assurance of changes to the functional system**  
RISK EVALUATION

The air traffic services provider should ensure that the risk evaluation includes:

- (a) an assessment of the identified hazards for a notified change, including possible mitigating means, in terms of risk or in terms of proxies or a combination of them;
- (b) a comparison of the risk analysis results against the safety criteria taking the uncertainty of the risk assessment into account; and
- (c) the identification of the need for risk mitigation or reduction in uncertainty or both.

**AMC2 ATS.OR.205(b)(4) Safety assessment and assurance of changes to the functional system**  
RISK MITIGATION



When the risk evaluation results show that the safety criteria cannot be satisfied, then the air traffic services provider should either abandon the change or propose additional means of mitigating the risk. If risk mitigation is proposed, then the air traffic services provider should ensure that it identifies:

- (a) all of the elements of the functional system, e.g. training, procedures, that need to be reconsidered; and
- (b) for each part of the amended change, those parts of the safety assessment (requirements from (a) to (f)) that need to be repeated in order to demonstrate that the safety criteria will be satisfied.

**GM1 ATS.OR.205(b)(4) Safety assessment and assurance of changes to the functional system**  
RISK ANALYSIS IN TERMS OF SAFETY RISK

(a) Risk analysis

When a risk assessment of a set of hazards is executed, in terms of risk:

- (1) the frequency or probability of the occurrence of the hazard should be determined;
- (2) the possible sequences of events from the occurrence of a hazardous event to the occurrence of an accident, which may be referred to as accident trajectories, should be identified. The contributing factors and circumstances that distinguish the different trajectories from one another should also be identified, as should any mitigations between a hazardous event and the associated accident<sup>146</sup>;
- (3) the potential harmful effects of the accident, including those resulting from a simultaneous occurrence of a combination of hazards, should be identified;
- (4) the severity of these harmful effects should be assessed, using a defined severity scheme according to point (f) of AMC2 ATS.OR.205(b)(3); and
- (5) the risk of the potential harmful effects of all the accidents, given the occurrence of the hazard, should be determined, taking into account the probabilities that the mitigations may fail as well as succeed, and that particular accident trajectories will be followed when particular contributing factors and circumstances occur.

(b) Severity schemes

The severity determination should take place according to a severity classification scheme. This section provides guidance on such schemes (more comprehensive guidance can be found in Section 5.1.2 of Appendix I to GM1 to Article 5 & Article 6(2)).

The purpose of a severity classification scheme is to facilitate the management and control of risk. A severity class is, in effect, a container within which accidents can be placed if their severities are considered different. Each container can be given a value which represents the consequences, i.e. small for accidents causing little harm and big for accidents causing a lot of harm. The sum of the probabilities of all the accidents assigned to a severity class multiplied by the value that is related to the severity class, is the risk associated with that class. If the value that represents severity for all classes is scalar, then the total risk is the sum of the risks in each severity class.

<sup>146</sup> Note that the diagram in (a) shows a single accident trajectory, of which there may be many associated with a hazard. This notion is developed in the next section.



(1) Single-risk value severity schemes

Such schemes use a single severity category to represent harm to humans. Other categories representing other kinds of harm e.g. damage to aircraft and loss of separation, may be present but do not represent harm to humans. In these circumstances, risk analysis would actually be reduced to frequency/probability analysis.

(2) Multiple-risk value severity schemes

Multiple-risk value severity schemes, which use a number of severity categories to classify different levels of harm, facilitate the management and control of risk in a number of ways. At the simplest level, the distribution of accidents across the severity classes gives a picture of whether the risk profile of a system is well balanced. For example, many accidents in the top and bottom severity classes with few in between suggests an imbalance in risk, perhaps due to an undue amount of attention having been paid to some types of accident at the expense of others. More detailed management and control of risk includes:

- (i) Severity classes may be used as the basis for reporting accident statistics.
- (ii) Severity classes combined with frequency (or probability) classes can be used to define criteria for decision-making regarding risk acceptance.
- (iii) The total risk associated with one or more severity classes can be managed and controlled. For example, the sum of the risk from all severity classes represents the total risk and may be used as a basis for making decisions about changes.
- (iv) Similarly the risk associated with accident types of different levels of severity can be compared, for example comparing runway infringement accidents with low speed taxiway accidents would allow an organisation to focus their efforts on mitigating the accident type with greatest risk.

- (c) Air traffic services providers should coordinate their severity schemes when performing multi-actor changes to ensure adequate assessment. This includes coordination with air traffic services providers outside of the EU.

**GM2 ATS.OR.205(b)(4) Safety assessment and assurance of changes to the functional system**

**SAFETY ANALYSIS IN TERMS OF PROXIES**

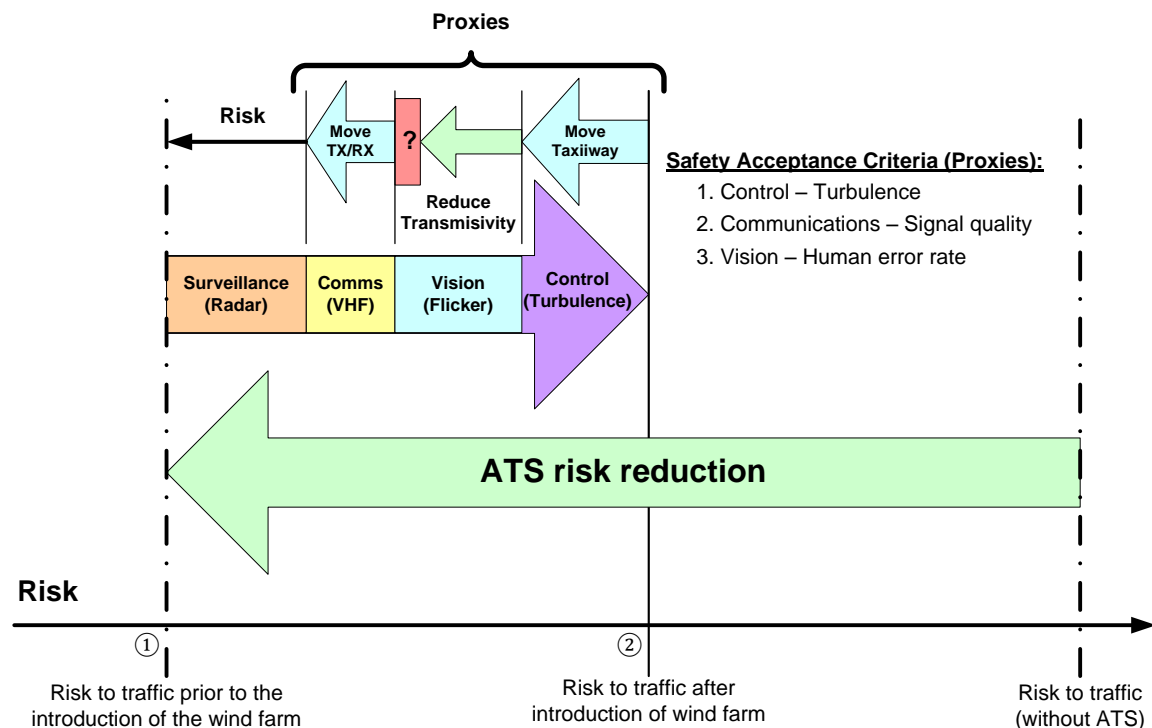
- (a) AMC1 ATS.OR.205(b)(2) point (c) allows safety assessment to be performed in terms of risk, proxies or a combination of risk and proxies. In this section, two examples are given to assist in the selection and use of proxies in safety analysis.

(b) Use of proxies when assessing the safety of a wind farm installation

- (1) A wind farm is to be introduced on or near an aerodrome. It is assumed that before the introduction of the wind farm, the safety risk of the air traffic services being provided at the aerodrome was acceptable. To return to this level after the introduction of the farm, the change would also be acceptable.

A diagram showing the effects this has on the risk at the aerodrome is shown below:





**Figure 34: Evaluation of risks after the introduction of wind farm**

- (2) The risk due to the introduction of the wind farm from will rise from ① to ②, if not mitigated, because:
- (i) turbulence will increase and so may destabilise manoeuvring of aircraft;
  - (ii) the movement of the blades will cause radio interference (communications radio and surveillance radar) and so communications may be lost or aircraft may be hidden from view on the radar screen; and
  - (iii) the flicker in the peripheral vision of ATCOs, caused by the rotation of the blades, may capture attention and increase their perception error rate.
- (3) The problem of analysing the safety impact can be split into these areas of concern since they do not interact or overlap and so satisfy the independence criterion (b) of AMC2 ATS.OR.210(a). However, whilst it can be argued that each is a circumstantial hazard and that in each case a justifiable qualitative relationship can be established linking the hazard with the resulting accident (so satisfying the causality criterion (a) of AMC2 ATS.OR.210(a) ) the actual or quantitative logical relationship is, in each case, extremely difficult to determine. Conditions for seeking proxies have, therefore, been established:
- Performing a risk evaluation using actual risk may not be worthwhile due to the considerable cost and effort involved; and
  - The first two criteria for proxies have been satisfied.

Consequently, it may be possible to find proxies that can be used more simply and effectively than performing an analysis based on risk.

(4) The solutions proposed below are for illustrative purposes only. There are many other solutions and, for each change, several should be investigated. In this example, the following proxies, which satisfy the measurability criterion (c) of AMC2 ATS.OR.210(a), are used to set safety criteria:

(i) Turbulence can be measured and predicted by models so the level of turbulence can be a proxy.

In this example, let's assume the only significant effect of turbulence is to light aircraft using a particular taxiway. It is possible to predict the level of turbulence at different sites on the aerodrome and an alternative taxiway is found where the level of turbulence after the introduction of the wind farm will be less than that currently encountered on the present taxiway. This can be confirmed during operation after the change by monitoring.

(ii) Signal quality can be also be predicted by models and measured so it can be used as a proxy.

In this example, it is possible to move the communications transmitter and receiver aerials so that communications are not affected by interference. Sites can be found using modelling and the signal quality confirmed prior to moving the aerials by trial installations during periods when the aerodrome is not operating.

(iii) Human error rate in detecting events on the manoeuvring area can be measured in simulations and can be used as a proxy.

It is suggested that increasing the opaqueness of the glass in the control tower will reduce the effects of flicker on the ATCOs, but there is no direct relationship between the transmissivity and the effects of flicker. It is, therefore, decided to make a simulation of the control tower and measure the effects of flicker on human error rate using glass of different levels of transmissivity.

However, there is a conflict between increasing the opaqueness of the glass to reduce the effects of flicker and decreasing it to improve direct vision, which is needed so that manoeuvring aircraft can be seen clearly. In other words, the simulation predicts a minimum for the human error rate that relates to a decrease, as the effects of flicker decrease, followed by an increase, as the effects of a lack of direct vision increase. This minimum is greater than the human error rate achieved by the current system and so the risk of the wind farm, in respect of flicker, cannot be completely mitigated. This is shown by the red box with a question mark in it on the diagram.

(5) Finally, the argument for the performance of surveillance radars is commonly performed using risk. This can be repeated in this case since the idea is to filter the effects of the interference without increasing the risk. Moreover, if necessary, a system may be added (or a current one improved) to reduce the risk simply and economically and the effects of the additional system may be argued using risk.

(6) Since risks can be combined, the safety impacts of the changes to the surveillance radar by filtering the effects of the interference together with the addition of another system or the improvement of the current system can be established by summing the risks associated with these two kinds of change.

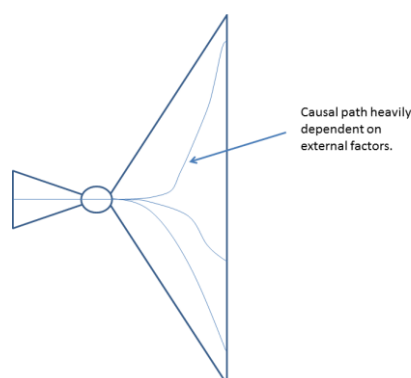
(7) In these circumstances, it is not possible to argue objectively that the risk of introducing the wind farm has been mitigated, as risks cannot be summed with proxies. This demonstrates the





difficulties of using proxies. However, it may be possible to argue convincingly, albeit subjectively, that installing another system or improving the current system improves the current level of risk by a margin large enough to provide adequate compensation for the unmitigated effects of flicker.

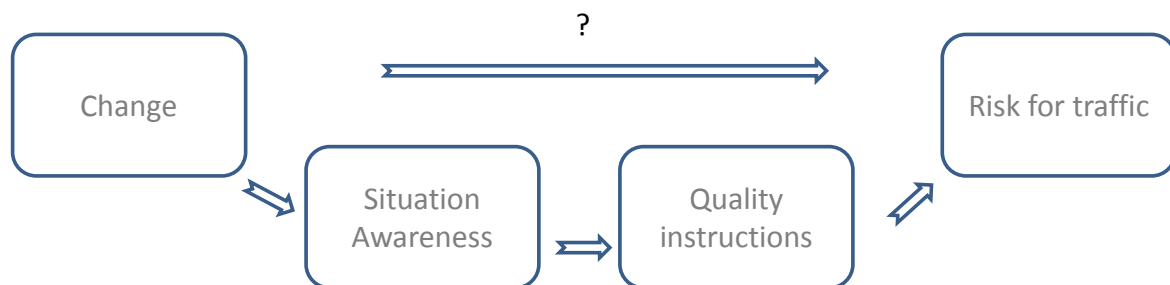
- (8) In summary, this example shows how proxies and risks can be combined in a single assurance case to argue that a change to a functional system can be introduced safely. It also demonstrates that the strategies available to demonstrate safety are not generic, but are dependent on identifying analysable qualities or quantities related to specific properties of the system or service that are impacted by the change.
- (c) Use of proxies when changing to electronic flight strips
- (1) An air traffic services provider considers the introduction of a Digital Strip System in one of its Air Traffic Control Towers to replace the paper Flight Progress Strips currently in use. This change is expected to have an impact on several aspects of the Air Traffic Control service that is provided such as the controller's recollection of the progress of the flight, the mental modeling of the traffic situation and the communication and task allocation between controllers. A change of the medium, from paper to digital, might, therefore, have implications on the tower operations, and, hence, on the safety of the air traffic. The actual relation between the change of the strip medium and the risk for the traffic is, however, difficult to establish.
- (2) The influence of the quantity on the risk is globally known, but cannot easily be quantified. One difficulty is that strip management is at the heart of the Air Traffic Control operations: the set of potential sequences of events from a strip management error to an accident or incident is enormous. This set includes, for example, the loss of the call sign at the moment a ground controller needs to intervene in a taxiway conflict, and whether this results in an incident depends for example on the visibility. This set also includes the allocation of a wrong Standard Instrument Departure (SID) to an aircraft, and whether this results in an accident depends for example on the runway configuration.



**Figure 35:** Notional Bow Tie Model of a strip management error

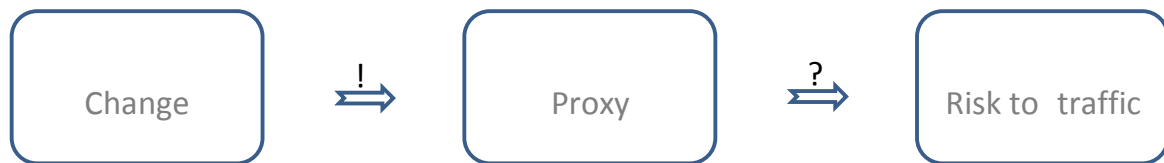
- (3) The Bow Tie Model of a strip management error has, figuratively speaking, a vertically stretched right part. This expresses that a hazard — such as the loss of a single strip — may have many different outcomes which heavily depend on factors that have nothing to do with the cause of the hazard — factors such as the status of the aircraft corresponding to the absent strip, that aircraft's position on the aerodrome, the traffic situation and the visibility.

- (4) Another difficulty with the relationship between the change of the medium and the risk to the air traffic is that several human and cultural aspects are involved. The difficulty lies in the largely unknown causal relationship between these human and cultural aspects and the occurrences of accidents and incidents. As an example of this, it is noted that strip manipulation — like moving a strip into another bay, or making a mark to indicate that a landing clearance is given — assists a controller in distinguishing the potential from the actual developments. The way of working with paper strips generates impressions in a wider variety than digital strips by their physical nature: handling paper strips has tactile, auditory and social aspects. This difference in these aspects may lead to a difference in the quality of the controller's situation awareness which may lead to a difference in the efficacy of the controller's instructions and advisories, which may lead to a difference in the occurrence of accidents and incidents. However, the relation between the change of the medium and the risk for the air traffic is difficult to assess and would require a great deal of effort, time and experimentation to quantify.



**Figure 36:** Relation between the change of flight strip and the risk

- (5) There is probably a relation between the change of the flight progress strip medium and the risk for air traffic: a new Human–Machine Interface may have an effect on the situation awareness of some individual controllers in some circumstances, which might have an effect on whether, when and what instructions are given, and this in turn influences the aircraft movements, and, hence, the risks. The question by what amount risks increase or decrease is very hard to answer.
- (6) Performing a risk evaluation using actual risk may not be worthwhile due to the difficulties and considerable cost and effort involved in assessing the risk of the change directly. Therefore, the use of proxies might be preferred. A quantity is only considered an appropriate proxy if it satisfies the criteria in point AMC2 ATS.OR.210(a):
- (i) **Causality:** The quantity used as proxy can be expected to be influenced by the change, and the risk can be expected to be influenced by the quantity. In addition to this causal relationship, a criterion can be formulated and agreed upon that expresses by which amount the value of the quantity may shift due to the change. Note that the influence of the proxy on the risk cannot easily be quantified, otherwise it might be more beneficial to use risk as a measure and the quantity as an auxiliary function.
  - (ii) **Measurability:** The influence of the change on the quantity can be assessed before as well as after the change.
  - (iii) **Independence:** When the proxy selected does not cover all hazards, a set of proxies should be used. Any proxy of that set should be sufficiently isolated from other proxies to be treated independently.



**Figure 37:** Relation between proxy and risk

- (7) There is a relationship between the change and the proxy, and there is a relationship between the proxy and the risk to traffic. The first relationship can be assessed (indicated by the '!'), while the second cannot (indicated by the '?'). An acceptance criterion is typically formulated for the amount the proxy value might increase or decrease.
- (8) Proxy 1: Head-down time. The head-down time is a good proxy as it satisfies the conditions of:
- (i) Causality: It is known that less head-down time leads to a higher risk but there is no well-established or generally accepted statement in literature in terms of: '*x % more head-down time implies y% more accidents*', leave alone for the specific circumstances of the specific ATC tower. The causal relationship indicated in Figure 3 can be established because:
    - (A) the head-down time can be expected to change as the manipulation, writing and reading of digital strips might cost more, or perhaps less, attention and effort than the handling of paper strips;
    - (B) the loss of head-up time of ground and runway controllers implies less surveillance, at least less time for the out-of-the-window-view in good visibility, and this implies a later or less probable detection of conflicts; and
    - (C) an example of an acceptance criterion reads: '*The introduction of the Digital Strip System does not lead to a significant increase in the head down time*'.
  - (ii) Measurability: The influence of the change on the head-down time can be assessed before the change by means of real-time human-in-the-loop experiments in which controllers are tasked to handle equal amounts of traffic in equal circumstances, one time using paper strips and another time using digital strips. The percentage of head-down time can then be determined by observing the controllers by cameras and eye-trackers.
- (9) Proxy 2: Fraction of erroneous Standard Instrument Departure (SID) allocations. The fraction of erroneous SID allocations is a good proxy as it satisfies the conditions of:
- (i) Causality: It can be imagined that an erroneous SID selected in the Flight Management System (FMS) might lead to accidents, but the precise conditional probability is small and difficult to estimate as it depends on several external factors such as the flight paths of the correct and incorrect SIDs, the presence of other traffic, the timing and geometry of the trajectories, the cloud base or the vigilance of the controller. The causal relationship indicated in Figure 3 can be established because:
    - (A) the number of incorrect SIDs indicated on electronic strips can be expected to be less than on paper strips, because of the possibilities of systematic checks with respect to runway allocation, runway configuration, SID allocation of the predecessor and destination in the flight plan;

- (B) the allocation of an incorrect SID to an aircrew might lead to a situation in which the aircraft manoeuvres in an unanticipated way, possibly leading to a conflict with another aircraft, for example departing from a parallel runway; and
  - (C) an example of an acceptance criterion reads: *'The introduction of the Digital Strip System should lead to a decrease of the fraction of erroneous SID allocations of more than 20 %'*.
- (ii) Measurability: The influence of the change on the fraction of erroneous SID allocations can be assessed before the change by means of an analysis of the causes and occurrences of such errors and the estimated efficacy of the systematic checks. The fractions can be assessed after the change by the statistics of the event reports.
- (10) Finally, the last condition of independence of proxies is also satisfied. For the purpose of this example, the proxies in (5) and (6) form a set of independent proxies that are complete, i.e. they cover all identified hazards introduced by the replacement of paper strips by a Digital Strip System.

**AMC1 ATS.OR.205(b)(5) Safety assessment and assurance of changes to the functional system**  
VERIFICATION

The air traffic services provider should ensure that verification activities of the safety assessment process include:

- (a) verification that the full scope is addressed throughout the whole assessment process, i.e. all the elements of the functional system or environment of operation that are changed and those unchanged elements that depend upon them and on which they depend are identified;
- (b) verification that the design is completed and correct;
- (c) verification that the design was the one analysed; and
- (d) verification that the implementation is that of the design and behaves only as specified.

**GM1 ATS.OR.205(b)(5) Safety assessment and assurance of changes to the functional system**  
OUTCOME OF RISK EVALUATION

The purpose of risk evaluation is to evaluate the risk of the change and to compare that against the safety criteria with the following outcomes in mind:

- (a) A possible (desired) outcome is that the assessed risk satisfies the safety criteria. This implies that the change is assessed as sufficiently safe to implement.
- (b) Another possible outcome is that the assessed risk does not satisfy the safety criteria. This might lead to the decision to refine the risk analysis, to the decision to add mitigating means, or to the decision to abandon the change.



**GM2 ATS.OR.205(b)(5) Safety assessment and assurance of changes to the functional system**

## RISK EVALUATION — UNCERTAINTY

- (a) The outcome of a risk analysis is uncertain due to modelling, estimates, exclusion of rare circumstances or contributing factors, incident and safety event underreporting, false or unclear evidence, different expert opinions, etc. The uncertainty may be indicated explicitly, e.g. by means of an uncertainty interval, or implicitly, e.g. by means of a reference to the sources the estimates are based upon.
- (b) Where possible sequences of events, contributing factors and circumstances are excluded in order to simplify the risk estimate, which may be necessary to make the estimate of risks feasible, arguments and evidence justifying this should be provided in the safety case. This may result in increasing the uncertainty of the risk estimations.

**GM3 ATS.OR.205(b)(5) Safety assessment and assurance of changes to the functional system**

## RISK EVALUATION — FORMS OF RISK EVALUATION

The risk evaluation can take several forms, even within the safety assessment of a single change, depending on the nature of the risk analysis and the safety criteria:

- (a) If a set of safety requirements has been created and can be unambiguously and directly related to the safety criteria, then risk evaluation takes the form of justifying that these requirements satisfy the safety criteria;
- (b) If the frequency of occurrence of the hazards, the severity of occurrence of the harmful effects and the frequency of occurrence of these effects given the occurrences of the hazards have been determined, then risk evaluation takes the form of verifying that the assessed risks satisfy the safety criteria in terms of risks; and
- (c) If the values of all relevant proxies have been determined, then risk evaluation takes the form of verifying that these values satisfy the safety criteria in terms of proxies.

**GM4 ATS.OR.205(b)(5) Safety assessment and assurance of changes to the functional system**

## TYPE OF RISK MITIGATION

Risk mitigation may be achieved in the following ways:

- (a) an improvement of the performance of a functional subsystem;
- (b) an additional change of the ATM/ANS functional system;
- (c) the implementation of a safety net;
- (d) an improvement of the services delivered by third parties;
- (e) a change in the physical environment; or
- (f) any combination of the above-mentioned methods.

**GM1 ATS.OR.205(b)(5)(ii) Safety assessment and assurance of changes to the functional system**

## VERIFICATION OF SAFETY CRITERIA

As the complete behaviour of the change is reflected in satisfying the safety criteria for the change, no safety requirements are set at system or change level. Nevertheless, safety requirements can be placed on the architecture and the components affected by the change.



**AMC1 ATS.OR.205(b)(6) Safety assessment and assurance of changes to the functional system**  
MONITORING OF INTRODUCED CHANGE

The air traffic services provider should ensure that within the safety assessment process for a change, the monitoring criteria, that are to be used to demonstrate that the safety case remains valid during the operation of the changed functional system, are identified and documented. These criteria are specific to the change and should be such that they indicate that:

- (a) the assumptions made in the argument remain valid;
- (b) critical proxies remain as predicted in the safety case and are not more uncertain; and
- (c) other properties that may be affected by the change remain within the bounds predicted by the safety case.

**GM1 ATS.OR.205(b)(6) Safety assessment and assurance of changes to the functional system**  
MONITORING OF INTRODUCED CHANGE

- (a) Monitoring is intended to maintain confidence in the safety case during operation of the changed functional system. At entry into service, the safety criteria become performance criteria rather than design criteria. Monitoring is, therefore, only applicable following entry into service of the change. This is further explained in point (c)(11) of in Section 3.2 of Appendix I to GM1 to Article 5 & Article 6(c).
- (b) Monitoring is likely to be of internal parameters of the functional system that provide a good indication of the performance of the service. These parameters may not be directly observable at the service level, i.e. at the interface of the service with the operational context. For example, where a function is provided by multiple redundant resources, the availability of the function will be so high that monitoring it may not be useful. However, monitoring the availability of individual resources, which fail much more often, may be a useful indicator of the performance of the overall function.

**AMC1 ATS.OR.210(a) Safety criteria**  
OTHER MEASURES RELATED TO SAFETY RISKS

When the air traffic services provider specifies the safety criteria with reference to another measure that relates to safety risk, it should use one or more of the following:

- (a) proxies;
- (b) recognised standards and/or codes of practice; and
- (c) the safety performance of the existing functional system or a similar system elsewhere.

**AMC2 ATS.OR.210(a) Safety criteria**  
PROXIES

Proxies for safety risk, used as safety criteria for those parts of the functional system affected by the change, can only be employed when:

- (a) a justifiable causal relationship exists between the proxy and the harmful effect, e.g. proxy increase/decrease causes risk increase/decrease;
- (b) a proxy is sufficiently isolated from other proxies to be treated independently; and
- (c) the proxy is measurable to an adequate degree of certainty.



**GM1 ATS.OR.210(a) Safety assessment and assurance of changes to the functional system**

## SAFETY CRITERIA IN TERMS OF PROXIES FOR SAFETY RISKS

- (a) In the safety assessment of functional systems, it may not always be possible or desirable to specify safety criteria in terms of quantitative values of risk. Instead, safety criteria may be defined in terms of other measures that are related to risk. These measures are called proxies and they need to meet the requirements for a proxy as stated in AMC2 ATS.OR.210(a). For examples of their use, see GM2 ATS.OR.205(b)(4).
- (b) A proxy is some measurable property that can be used to represent the value of something else. In the safety assessment of functional systems, the value of a proxy may be used as a substitute for a value of risk, providing it meets the requirements for a proxy as stated in AMC2 ATS.OR.210(a). Examples of proxies are the frequency of airspace infringements, runway incursions, false alert rate, head-down time, limited sight, level of situation awareness, fraction of read back errors, reduced vigilance, amount of turbulence, distraction of controller's attention, inappropriate pilot behaviour, system availability, information integrity and service continuity.
- An example of the concept of using a different but specific quantity to assess an actually relevant quantity is the transposition/measure of an aircraft's altitude which is in terms of barometric pressure or the transposition/measure of an aircraft's airspeed which is in terms of dynamic pressure.
- (c) Proxies might be preferred where the extra effort needed to identify, describe and analyse a complete set of sequences of events from the occurrence of a hazard to the occurrence of an accident or incident has no added value in the safety assessment. The intrinsic reasons for the size of the extra effort are the number of significantly different event sequences, the complexity of some accident scenarios, the existence of many barriers preventing the occurrence of a hazard developing into an accident and the lack of evidence on the probability of some events or the frequency of occurrence of some external circumstances and factors. The usage of proxies might then make the safety assessment more tractable and comprehensible and increase the quality of the risk analysis.
- (d) The main advantages of proxies are the easy recognition of safety issues by operational staff involved in the safety assessment, and the direct focus on the analysis and mitigation of the identified hazards and safety issues introduced or affected by the change.
- (e) The main disadvantage of using proxies is that it is not possible to express risk by a uniform measure. However, the value of the proxy should be measurable.
- (f) For further details on the use of proxies, please refer to GM2 ATS.OR.205(b)(4), which contains two examples to assist in the selection and use of proxies in safety analysis.

**GM1 ATS.OR.210(b)(2) Safety criteria**

## SAFETY OF THE CHANGE

- (a) Having decided to make a change, an air traffic services provider needs to set safety criteria, the fulfilment of which will be used to judge the acceptability of the change. The determination of the safety criteria will be based on an overall objective for the safety of the change, which the air traffic services provider has to decide, the structure of the change and the relationship between the overall objective for safety and the various parts of the system being changed. These criteria are such that their fulfilment will necessitate the satisfaction of the overall objective for safety of the change, as stated in ATS.OR.210(b)(2). The safety of the change must be assured to the satisfaction of the service provider



(as per ATS.OR.205(a)(2)) and if it is to be reviewed, then also to the satisfaction of the CA (as per ATM/ANS.AR.C.040).

- (b) This overall objective for safety must be such that the resulting functional system after the change is acceptably safe, which means that:
- (1) the change will leave the delivered services at least as safe as they were before the change. In this case, there is no additional risk introduced by the change. It could even be the case that the safety risk of the system is reduced; or
  - (2) while not leaving the system as safe as before, the change has some societal benefit that compensates for the reduction in safety and this is agreed by the CA; or
  - (3) while not leaving the system as safe as before, the change will leave the system acceptably safe and will be followed by one or more changes that will compensate for the loss of safety<sup>147</sup>. The additional risk, potentially introduced by the change, the time over which it will exist, and any future compensation, must be acceptable to the CA.
- (c) The state diagram is given in Table 5 below. The states in green are acceptable situations and are captured by the provisions of ATS.OR.210(b)(2). Those in red are not acceptable and if they apply to a proposed change, the change must not be implemented. The fact that individual safety criteria must also be valid (as per ATS.OR.210(a) & (b)(1)) is implied in this table.

---

<sup>147</sup> The long-term goal being to restore the system to the level of safety it attained before the original change. However, while it is hoped that this aim can be achieved in the majority of cases, it is not a requirement.





**Table 5** — Acceptable safety criteria and the safety of the change they predict

				Safety Criteria		
				Safety criteria will be satisfied	Safety criteria will not be satisfied	
The safety of the system after the change has been made	1. Safer than before			Implement change and Safety Case approved if reviewed	Change not to be implemented and Safety Case not approved if reviewed	
	2. As safe as before			Implement change and Safety Case approved if reviewed		
	3. Less safe than before	1. There are benefits of the change that counterbalance the loss in safety	1. The justification for the loss of safety is included in the safety case and is accepted by the CA.			Implement change and Safety Case approved if reviewed
			2. The justification for the loss of safety is included in the safety case but is not accepted by the CA.			Change not to be implemented and Safety Case not approved if reviewed
			3. There is no justification for the loss of safety.			Change not to be implemented and Safety Case not approved if reviewed
		2. There are no counterbalancing benefits for the loss of safety	1. A plan exists that shows how the reduction in safety will be offset in the future and is agreed by the CA.			Implement change and Safety Case approved if reviewed. Plan agreed by CA
			2. A plan exists that shows how the reduction in safety will be offset in the future but is not agreed by the CA.			Change not to be implemented and Safety Case not approved if reviewed. Plan not agreed by CA
			3. There is no plan that shows how the reduction in safety will be offset in the future.			Change not to be implemented and SC not approved if reviewed



- (d) In the case represented by (b)(2), the air traffic services provider must provide, within the safety case, the argument<sup>148</sup> that shows, from a societal point of view, how the benefits compensate for the loss in safety.
- (e) In the case represented by (b)(3), the CA may allow an increase in the safety risk of the system to a level that it still judges to be acceptably safe. This GM covers two ways this can be implemented<sup>149</sup>:
- (1) The CA may establish criteria for judging the acceptability of cases where, after a change, the system will not be as safe as it was before the change (i.e. the risk increases) but the risk introduced is small enough that the system remains acceptably safe. The CA will then apply those criteria to each change represented by case 3.2.1 in Table 5. The criteria should be reviewed periodically.
  - (2) The Member State may establish a policy/legislation for the lowest level of safety it will accept for the ATM system, as a whole. This would set a criterion<sup>150</sup> by which the CA would judge the acceptability of changes represented by case 3.2.1 in Table 5. In order for this to be an appropriate strategy, the air traffic services provider must be able to judge the actual safety level of its functional system and compare it against that safety level.
- (f) The air traffic services provider will choose one of the three forms for the overall objective for safety described in (b) to derive the safety criteria from the inception of the change. It may, however, change the objective for safety as the change itself is developed and so change the safety criteria. For example, the change may prove more difficult than envisaged at first and so, while the original aim was to satisfy (b)(1) above, it may only be possible to satisfy (b)(3) above. Consequently, the overall objective for safety should be seen more as a goal (objective) than a requirement.

---

<sup>149</sup> Note: These two ways are not mutually exclusive. For example, some or all of the criteria used in (e)(1) may also be used as the additional criteria for (e)(2) referred to in the footnote below.

<sup>150</sup> There may be other criteria applied as well in order to judge the acceptability of the change, although these are not covered here.

