EAC
No.19-9

TABLE OF CONTENTS

ATM/ANS Change management procedures

Definitions of terms

Aviation undertaking' means an entity, person or organization, other than the organization regulated by this Regulation that is affected by or affects a service delivered by a service provider;

Functional system' means a combination of procedures, human resources and equipment, including hardware and software, organized to perform a function within the context of ATM/ANS;

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';

Chapter 1
ATM/ANS Change management procedures

1.1 The nature of change.

Changes proposed within the ATM/ANS environment come in two forms:
(1) The service provider e.g. service provider wishes:
(i) To change its functional system; or
(ii) To propose a change to the context in which its own services are delivered
e.g. airspace structure change, increase in traffic.

1.2 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;
(iv) Efficiency.
(2) Environmentally-driven change:
(i) Market share/growth;
(ii) Change in airspace use;
(iii) Introduction of environmental features e.g. winds farms;
(iv) Regulatory-driven changes.
(3) Management System (MS)-driven change:
(i) Reverse a deficiency that affects safety/trustworthiness60;
(ii) Reverse degradation in safety/trustworthiness;
(iii) Improve safety/trustworthiness, i.e. reduce the safety risk as low as is reasonably practicable or improve trustworthiness.
Any resulting changes to the functional system require a safety (support) assessment.
(g) Examples of changes that may or may not need assessment
(h) 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 included in the operations manual. These tactical changes include circumstances associated with day-to-day operations that result in alternatives, 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, change of summer/winter hour.
(i) 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 identicalpart 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 or discontinuity of the service.
(j) Changes described in (h) and (i) need to be covered in an assurance case, e.g. 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. However, it is possible that they have been inexistence for a considerable time and as a result may have been accepted by the ECAAvia another form of oversight. In this case, no assurance Case will exist.

(k) Unplanned/unforeseen changes due to unforeseen urgent circumstances.

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 tomanage the riskintroduced by these unforeseen circumstances, changes will need to bemade to one or more functional systems. In the Case of aservice provider other than an ATS provider, the process needs to decide whether theproposed change will have: no effect; an acceptable effect or an unacceptable effect onthe behavior of the service as currently specified. The process uses many of thetechniques and criteria associated with safety assessment and safety support assessment (And assurance). Moreover, the nature of the change will determine how easy it is tosatisfy those criteria.

(m) 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 completeInsofar as it explains the differences in assessing whether a responsive change isnecessary and the assessment needed if the service provider decides to make a changeto its functional system. The process is very similarfor an ATS provider and a service provider other than an ATS provider, except thatquestions and actions associated with safety risk are replaced by questions and actionsassociated with the specification of the service and the specification of the context overwhich the specification is valid.

(n) 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.

(o) 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.

(p) 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. Clearly, the impact analysis needs to be fit for purpose (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.

(q) 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. In order to do this, there is a need to establish:

(1) What 'hazards' are affected (or whether new ones will be introduced);

(2) What level of 'risk' these changes to the hazards represent; and

(3) whether this level of 'risk' is acceptable without changing the functional system For an ATS provider, 'hazards' and 'risks' are safety hazards and safety risks. For a service provider other than an ATS provider, 'hazards' and 'risks' are not safety hazards or safety risks. Instead, they will be hazards that might Cause the service to behave differently to that which is currently specified and the risks of so doing.

(r) If the level of impact is determined as being acceptable, then the answer to the question: 'Would the proposed change66 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. 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.

(s) What if the answer to the question is: 'yes'. In these circumstances, service provider must propose a change. The minimum change is simply to do the minimum necessary to mitigate the risk — the service provider could do more, if it so desired. In this Case, there is an identified change to the service provider's functional system, so the ECAA must be notified and the requirements for safety assessment or safety support assessment apply.

(t) If a change to the functional system is proposed, then not only does all the analysis have to be performed on that change (which implies taking the service specification and contexts specification from the service provider making the change into account, if this was the source of the original change), but verification of the implementation has to be performed as required.

Once this has been completed (successfully), the safety Case can be stored and, if required, delivered to the ECAA.

(v) In the Case of an ATS provider, it is possible that, initially, the proposed change does not Adequately mitigate the risks, i.e. the answer to the question: '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 change is proposed and is added to the previous proposal. The ECAA 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. 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.

(w) Similarly, it is possible that, for a service provider other than an ATS provider, the proposed change does not mitigate the risks, i.e. the answer to the question: '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 ECAA 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. 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.

(x) 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 ECAA. The planned change is assessed and an assurance Case produced. But what if the change to the ATM/ANS functional system was found to have an acceptable level of impact on the first pass through the assessment process? 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 on the change is an unnecessary and consequently extremely 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 when it is implemented. The verification, therefore, guards against the failure to implement the design as intended.

1.3 Changes to the functional system

(a) A service provider planning a change to its functional system shall:

(1) Notify their competent authority of the change;

(2) Provide the competent authority, if requested, with any additional information that
Allows the competent authority to decide whether or not to review the change; and
(3) Inform service providers and, where feasible, aviation undertakings affected by the planned change.
(b) Having notified a change, the service provider shall inform the competent authority whenever the information provided under (a)(1) and (2) is materially modified, and the relevant service providers and aviation undertakings whenever the information provided under (a)(3) is materially modified.
(c) The service provider shall only allow the parts of the change, for which the activities have been completed, to enter into operational service.
(d) If the change is subject to competent authority review, the service provider shall only allow the parts of the change for which the competent authority has approved the argument to enter into operational service.
(e) When a change affects other service providers and/or aviation undertakings, as identified in (a)(3), the service providers affected shall:
(1) Determine all the dependencies with each other and with the affected aviation undertakings;
(2) include in their notifications to their competent authorities, in accordance with (a)(1),a list of the service providers and other aviation undertakings that are affected;
(3) Plan and conduct a coordinated assessment considering the dependencies as determined in (1); and
(4) Determine the assumptions and risk mitigations that relate to more than one service provider or aviation undertaking.
(f) Those service providers affected by the assumptions and mitigations in (e)(4) shall:
(1) Mutually agree and align these assumptions and risk mitigations; and
(2) Where feasible, mutually agree and align these assumptions and risk mitigations with the aviation undertakings affected by them.

1.4 Management system

A service provider shall implement and maintain a management system that includes:

- a formal process to identify circumstances within the service provider's organization and the environment in which it operates that may affect the provision of ATM/ANS and, where necessary, to plan changes to their functional system to accommodate these circumstances;
- a formal process to consider changing their functional system if it is technically and economically feasible to improve performance by doing so.

The service provider shall monitor the behavior of the functional system and where:

- substandard performance is identified, establish its Causes, determine the implications of such substandard performance, and shall initiate a change to eliminate or mitigate such Causes; and
- It is found that an argument associated with a change to that functional system is unsound; the service provider shall initiate a change or provide a valid argument.

1.5 Change management procedures

(a) Procedures that will be used by a service provider to manage, assess, and, if necessary,
Mitigate the impact of changes to their functional systems
Shall:
(1) Be submitted, for approval, by the service provider to the competent authority; and
(2) Not be used until approved by the competent authority.
(b) When the approved procedures referred to in (a) are not suitable for a particular change,
The service provider shall:
(1) Make a request to the competent authority to deviate from the approved procedures;
(2) Provide the details of the deviation and the justification for its use to the competent
Authority; and
(3) Not use the deviation before being approved by the competent authority.

Chapter 2
SPECIFIC ORGANISATIONAL REQUIREMENTS FOR SERVICEPROVIDERS OTHER THAN ATS PROVIDERS

2.1Scope
Establishing requirements to be met by service providers other than ATS providers with respect to additional responsibilities to those established in Subparts A and B.

2.2 Safety support assessment and assurance of changes to thefunctional system
(a) A service provider other than an ATS provider shall:
(1) Ensure that a safety support assessment is carried out; and
(2) Provide assurance, with sufficient confidence, via a complete, documented and valid argument that the service will behave and will continue to behave only as specified in the specified context, for any change they have notified in accordance with (a)(1).
(b) A service provider other than an ATS provider shall ensure that the safety support assessment referred to in (a) comprises:
(1) The definition of the scope of the change, which consists of:
(i) The equipment, procedural and human elements being changed;
(ii) Interfaces and interactions between the elements being changed and the remainder of the functional system;
(iii) Interfaces and interactions between the elements being changed and the context in which it is intended to operate; and
(iv) The life cycle of the change from definition to operations including transition into service and planned degraded modes;
(2) Verification that:
(i) The change conforms to the scope that was subject to safety support assessment; and
(ii) The service behaves only as specified in the specified context; and
(iii) 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;
(3) The specification of the monitoring requirements necessary to demonstrate that the service delivered by the changed functional system will continue to behave only as specified in the specified context.

Chapter 3
SPECIFIC REQUIREMENTS FOR THE PROVISION OF AIR TRAFFIC SERVICES

3.1 Safety management system

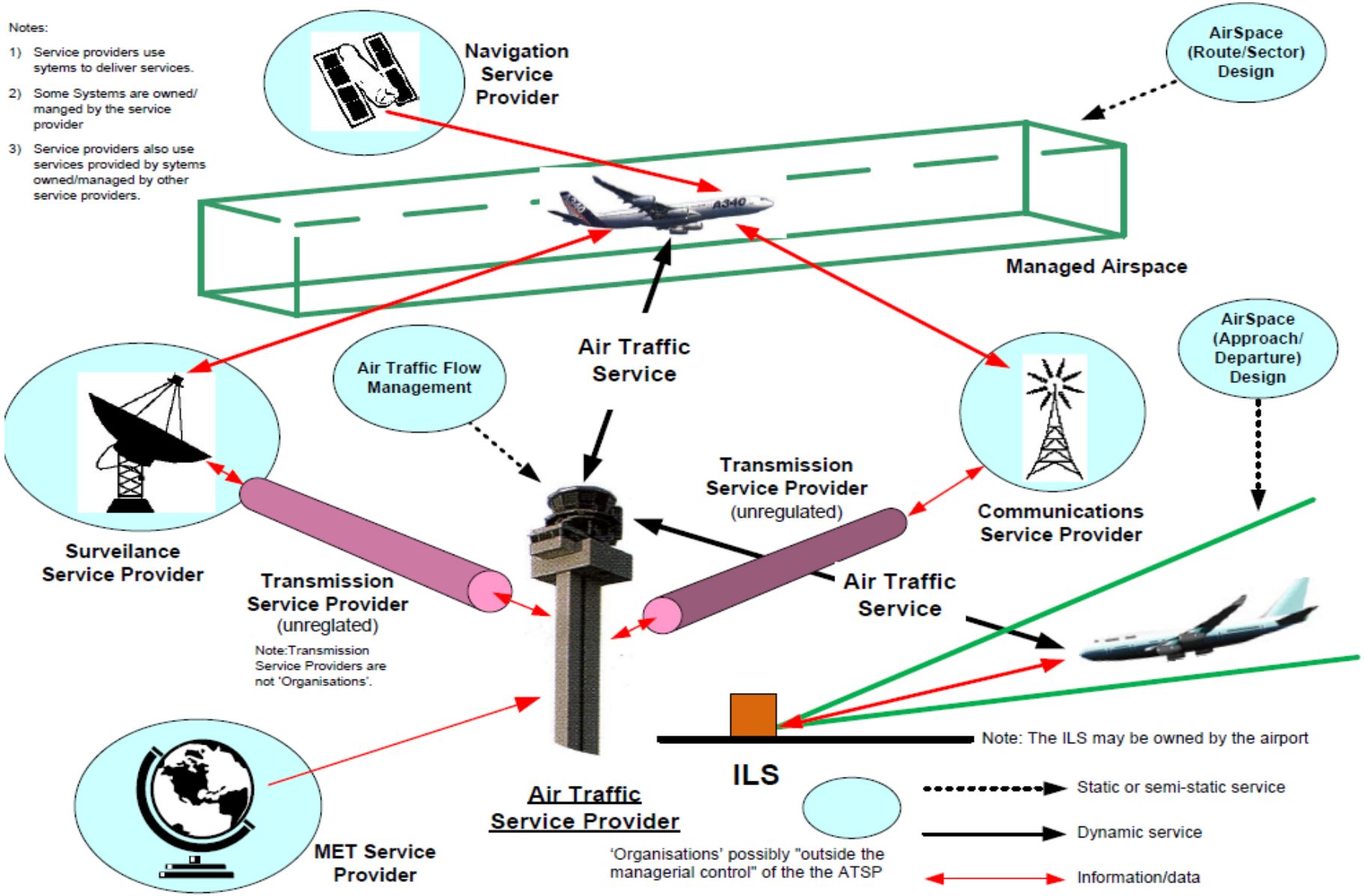
(b) The air traffic service provider shall ensure as part of its SMS that the objective for the safety of a planned change to a functional system that has been notified in accordance with a)(1), shall be that the service will be at least as safe after the change as it was before the change.
(c) Where (b) cannot be achieved, the ATS provider shall reach agreement with the regulatory Authority on a subsequent course of action.

3.2 ATSsafety assessment and assurance of changes to the functional system

(a) An ATS provider providing air traffic services shall:
(1) Ensure that a safety assessment is carried out; and
(2) provide assurance, with sufficient confidence, via a complete, documented and valid argument that the safety criteria are valid, will be satisfied and will remain satisfied for any change they have notified in accordance with (a)(1).
(b) An ATS provider providing air traffic services shall ensure that the safety assessment referred to in (a) comprises:
(1) The definition of the scope of the change, which consists of:
(i) The equipment, procedural and human elements being changed;
(ii) Interfaces and interactions between the elements being changed and the remainder of the functional system;
(iii) Interfaces and interactions between the elements being changed and the context
In which it is intended to operate; and
(iv) The life cycle of the change from definition to operations including transition into service and planned degraded modes;
(2) Identification of hazards;
(3) Determination of the safety criteria applicable to the change;
(4) Risk analysis of the effects related to the change; (5) risk evaluation and, if required, risk mitigation for the change such that it Can meet the applicable safety criteria;
(6) Verification that the change:
(i) Conforms to the scope that was subject to safety assessment; and
(ii) Meets the safety criteria; and
(7) The specification of the monitoring requirements necessary to demonstrate that the service delivered by the changed functional system will continue to meet the safety criteria.

3.3 ATS Safety criteria

(a) The ATS provider shall determine the safety acceptability of a change to a functional system
Using specific and verifiable safety criteria, where each criterion is expressed in terms of safety risk or other measures that relate to safety.
(b) The ATS provider shall specify the safety criteria with reference to one or more of the following:
(1) Explicit quantitative acceptable levels of safety risk or other measures related to safety risk;
(2) Recognized standards and/or codes of practice; and
(3) The safety performance of the existing system or a similar system elsewhere.
(c) The ATS provider shall ensure that the safety criteria:
(1) Are justified for the specific change, taking into account the type of change; and
(2) support the improvement of safety whenever reasonably practicable.


Notes:
1) Service providers use sytems to deliver services.
2) Some Systems are owned/ manged by the service provider
3) Service providers also use services provided by sytems owned/managed by other service providers.
Navigation Service Provider
AirSpace (Route/Sector) Design
Managed Airspace
Air Traffic Service
Air Traffic Flow Management
AirSpace (Approach/ Departure) Design
Surveilance Service Provider
Communications Service Provider
Transmission Service Provider (unregulated)
Transmission Service Provider (unreglated)
Note:Transmission Service Providers are not 'Organisations'.
Air Traffic Service
Note: The ILS may be owned by the airport
ILS
Air Traffic Service Provider
MET Service Provider
'Organisations' possibly "outside the managerial control" of the the ATSP
Static or semi-static service
Dynamic service
Information/data

3.4-Table 1-Examples of changes for ATS providers that may require safety assessment (and perhaps supervision),

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 provider of ATS 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 organizations 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 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.
		Procedures	New or changed procedures to handle new services and increased traffic Changes to the ATM/ANS organization for delivering services	
		Equipment	Possibly improved surveillance, communication and/or other systems, e.g. 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 forthe delivery of an ATS service	
		Architecture	Possibly if the surveillance and communication systems change it may require changes in the interfaces with equipment already present	
		Environment	Increase in traffic	
Changed communication system (Functional system change)	Business-driven: e.g. obsolescence (efficiency), desire	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
		Procedures	Change to maintenance	

Change description	Possible reason for change	Potential changes to		… Remarks
			procedures	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 a/c and ATS, 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.
		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-sitting of aerials	
Introduction of new surveillance facility (Functional system change)	Business-driven: e.g. desire to increase market share SMS-driven: e.g. operational deficiencies	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. 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.
		Procedures	Procedures changed to include the use of new forms of surveillance Change to maintenance procedures	
		Equipment	New equipment and possibly new or changed sensors	
		Architecture	Integration of the new surveillance with rest of the system	
		Environment	Possibly sitting of new sensors or	

Change description	Possible reason for change	Potential changes to		… Remarks
			resiting 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., operational deficiencies	People	Possibly training for new equipment interface Training for technical personnel	This is not intended to include the like-forklike 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 a/c and ATS, 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.
		Procedures	Change to maintenance procedures	
		Equipment	New equipment	
		Architecture	Unlikely	
		Environment	Possibly the re-sitting of aerials/sensors	
Airspace re organization (Class E – A, Mil – Civil, Shape of	Environmentally driven: strategic state initiative	People	Possibly additional operational personnel Training on new procedures and equipment	This change is driven by the State and is probably due to a strategic review of national airspace use. The provider of ATS Cannot ignore it

Change description	Possible reason for change	Potential changes to		… Remarks
sectors) (Environmentally triggered or Functional system change)			Possibly additional technical personnel Training for technical personnel	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 be necessary to improve the surveillance and communication facilities in order to meet the demands of the new classification, in which Casetechnical 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 organization. Both a change in airspace classification and a change in sector shape will have to be promulgated in the AIP.
		Procedures	Change to or the creation of procedures (operational & maintenance)	
		Equipment	Possibly to improve Surveillance/communications if change of airspace classification.	
		Architecture	Likely if procedures call for the use of new/changed information.	
		Environment	Possible change to sector shape	
VFR pilots obliged to transponders below TMA (outside ANSP Controlled airspace)	Environmentally driven: strategic State initiative, European initiative	People	Training to recognize VFR a/c moving towards infringement with controlled airspace	This change has a safety objective and is driven by regulation. The objective is to make VFR a/c more easily seen and, thus, avoid conflict with controlled traffic Caused by their invisibility, primarily to

Change description	Possible reason for change	Potential changes to		… Remarks
(Environmentally triggered change)				providers of ATS. The providers of ATS 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 thenew form of surveillance for VFR a/c. It may also necessitate changes to the SSR to accommodate the increase in responses due to VFR a/c close by.
New missed approach procedure (Functional system change)	Business-driven: e.g. desire to increase efficiency, desire to increase effectiveness SMS-driven: e.g. operational deficiencies	People	Training on new procedure	
		Procedures	New procedure	
		Equipment	Unlikely	
		Architecture	Unlikely	
		Environment	Unlikely	
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
		Procedures	Reduction in operational personnel Training for new role,	

Change description	Possible reason for change	Potential changes to	…	Remarks
			possibly different personnel. Possibly additional technical Personnel Training for technical personnel	presented in a different, more user-friendly, and 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 theequipment at the ATCO's workingposition and very probably implieschanges to the functions providinginformation to those working positions.
		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	
		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/organization to limit ATCO workload	
Integration of automatic meteorological information e.g. METAR, SIGMET (Environmentally triggered Or Functional system change)	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 provider of ATS may simply have to change the way the equipment manipulates and displays thedata. However, it may also be able to reduce the need for human intervention intransforming the data so that it Canbeused directly by the ATCO (or
		Procedures	Possibly change of procedures if MET data Cannot be transformed automatically and displayed in the	

Change description	Possible reason for change	Potential changes to		… Remarks
			current form Change to maintenance procedures	transmitted to the a/c). If it chooses to do the latter, then procedures will have to be changed and, consequently, operational staff retrained.
		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	
Change to cross wind limits (Environmentally-triggered or Functional system change)	Environmentally driven: discovery that the a/c type	People	Possibly additional operational personnel Training on new procedures and equipment Possibly additional technical personnel Training for technical personnel	A reclassification of the a/c type for cross wind maneuvers probably does not necessitate retraining of operational personnel. Notification and awareness may be sufficient. However, a change to the cross wind classification of many a/c, which may be 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. Larger a/c Can usually maneuver safely in higher cross winds than lighter a/c.There fore, this business-driven change is to allow the aerodrome operator to handle larger a/c, presumably because the organization wishes to increase Passenger throughput.
		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 in order to improve surveillance/communications due to increase in traffic Unlikely	
		Environment	Different distribution of a/c in cross winds	

3.5 -Examples of changes that may require safety support assessment

Change description	Possible reason for change	Potential changes to	…	Remarks
Introduction of a new tool for issuing NOTAM	Business-driven: e.g. desire to increase efficiency	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 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 to them. The change then becomes a multi-actor change.
		Procedures	New or changed procedures to handle the new tool Changes to the AIS organization for delivering services	
		Equipment	Likely changes in software and also in hardware	
		Architecture	Unlikely	
		Environment	Unlikely	
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 ATS 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 ATS 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	
		Architecture	Unlikely	
		Environment	Unlikely	

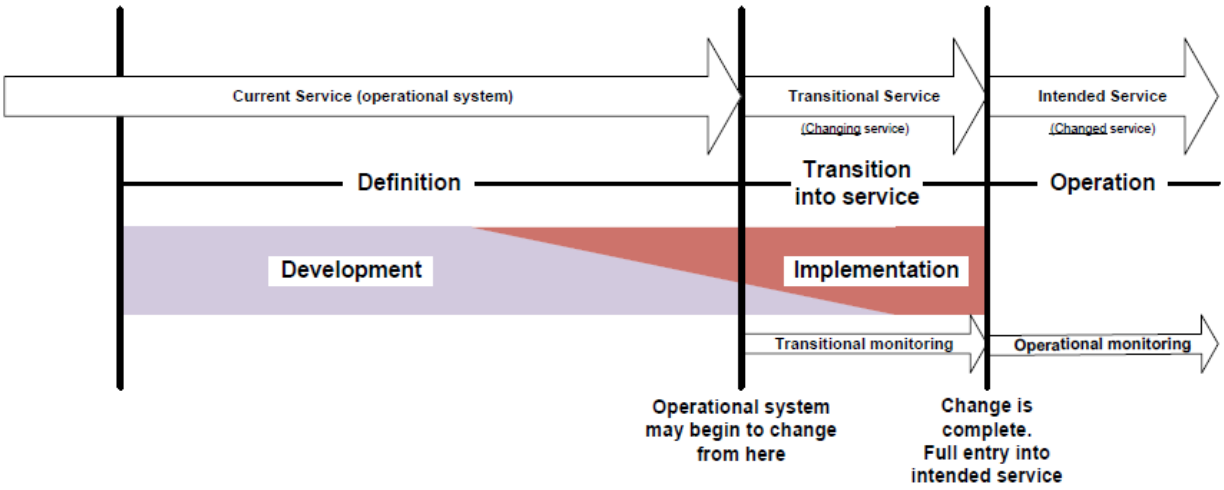
3.6-Table 3 – Examples of changes for service providers that may not require Safety or safety support assessment,i.e. those not in the scope of ATM/ANS/ ATS

Change description	Type of change	Possible reason for change
Organizational Change	Change to organization, not to the functional System.	Political reasons/Desire to increase efficiency
Maintenance change, covered by a procedure, where components are changed on a like-forklike basis	Planned/Regular	Preventive actions on technical components
Day-to-day operations e.g. a change in runway direction, described in operational manuals	Operational tactical change	Change in environment of operations, e.g. wind direction, weather, regular change associated with noise abatement
Use of alternative procedures81 in response to the failure of a system/component	Operational tactical change	Failure of an operational system

Chapter4
Overview of the change process

4.1-Overview of the change process

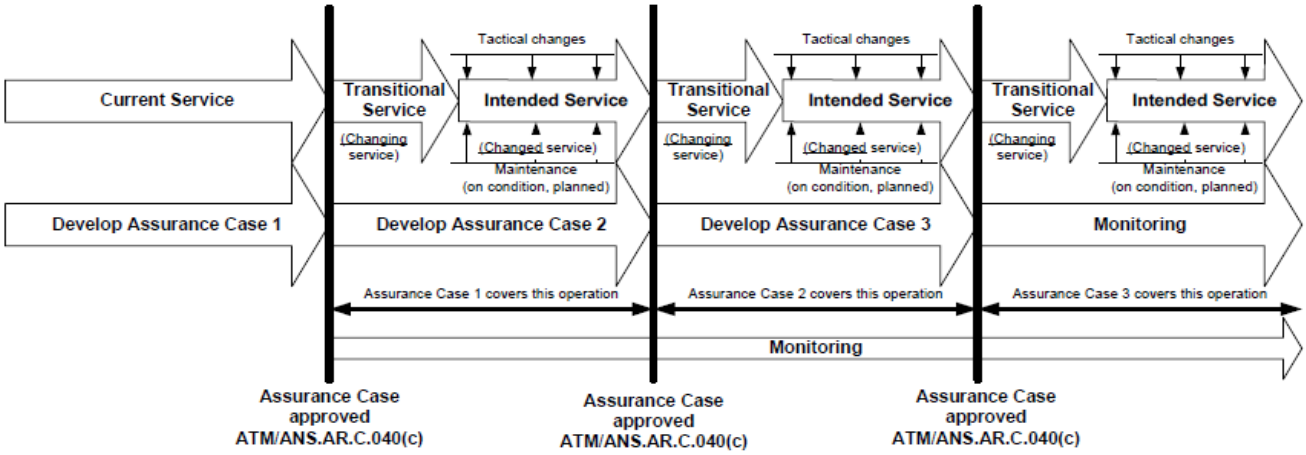
(1) Most changes start by identifying the need for a change and establishing sufficient information about the change, that it can be put to the organization's management board for their agreement.
(2) When a service provider has a real intent to implement a change, it should notify the ECAA of its intent to change the functional system as early as possible bearing in mind that
(i) It has to give the ECAA sufficient time to decide whether to review the assurance ECAA or not; and
(ii) if the ECAA 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 ECAA before making any change to the functional system that could affect the operation.
Note that, as part of general oversight, the competent authority may select such a change to determine if the procedures are applied properly and the change is safe. Apart from general oversight the ECAA will not be involved in the change.
(iii) If the ECAA decides to review the change, the ECAA will be involved in the change process. As a consequence of the ECAA's decision, the implementation of the change is dependent on the approval of the ECAA.
(3) The details of the interaction process will be described in both the ECAA and service provider's procedures. For optimum effectiveness and efficiency, the parts of these procedures dealing with the interaction between the ECAA 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 ECAA about the planning and important steps in respect of safety in the development of the change. If the ECAA decides not to review a change, the exchange of information will be minimal.
(5) All work related to the development of the change ECAA 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 ECAA.



An overview of the change process

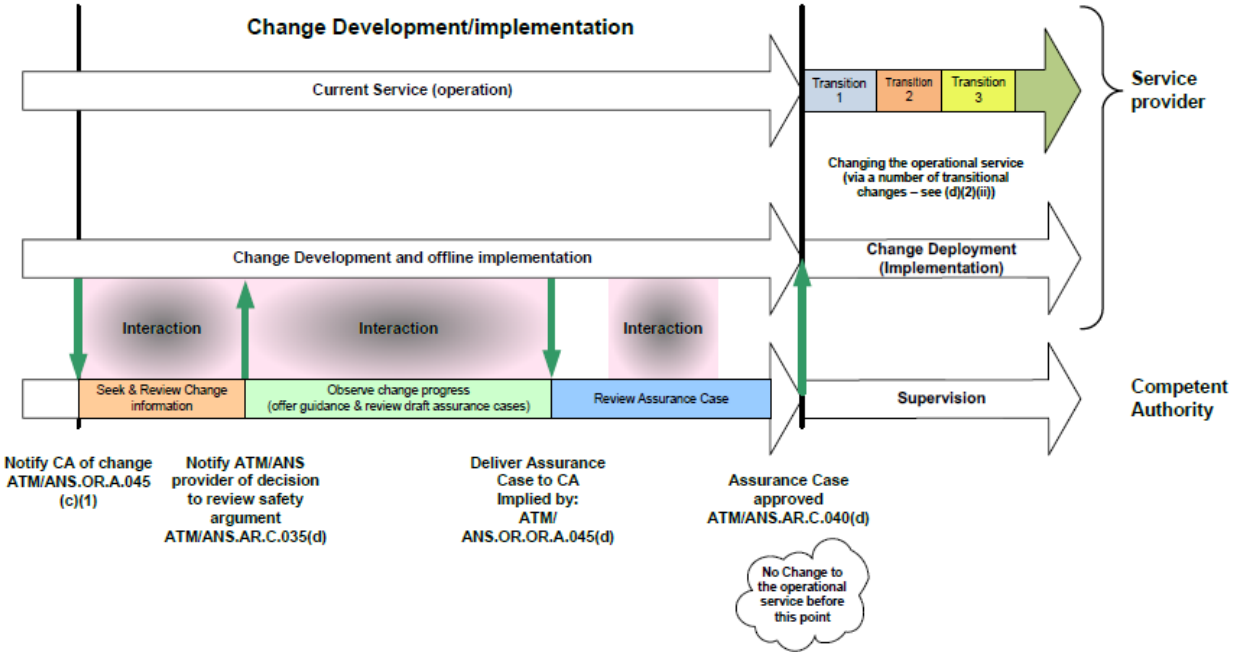
(6) Figure shows that the change process consists of two different processes:
Development and implementation. No timescales are implied in Figure 1 because the definition and transition into service phases may take many years in some cases, e.g.moving an ATC unit to a different location and a few days in others, e.g. simplechange 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 developmentdeals with design84, whereas implementation deals with concrete artefacts i.e. thosebuilt or manufactured component parts that were identified in the design, and alsowith integrating them into the functional system to become a whole. Since, at anystage, some artefacts are beingdeveloped, while others are being implemented e.g.COTS components may be purchased before some other components have beendesigned, and simple changes to software may predate the changes to the hardwareon which it operates, the diagram shows considerable overlap between developmentand implementation.
(8) Note that any part of the implementation that has the potential to affect theoperational service cannot be started until a valid assurance case for the changeexists or, where the CA has decided to review the assurance case, it has beenapproved.
(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 3 shows such a situation. The firstimplementation activities begin before the change has any influence on the operation.Overall development continues during the transitional service and is finalized wellbefore the change reaches the point where the change is completed. Each transitionmay 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 isin line with such an approach.
(11) The 'operation' phase begins when the change has been completed88 and theoperation is as intended. As part of the safety/safety support assessment, it mayhave been decided that, during operation, monitoring activities are required to beestablished. 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 thenecessary interactions.
(12) The assessment of the monitoring activities identified above 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 theassurance case. It may be accompanied by temporary measures such as mitigationsthat reduce the risk of the operation. These measures can be removed once thenecessary level of confidence has been established.
Transition finishes (and 'Operation'90 begins) when all the confidence buildingmeasures (Temporary monitoring and mitigations) have been removed. Consequently,if the transition phase is long, the implementation phase is correspondingly long. Themonitoring that remains is then the permanent monitoring that is required to showthat 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 may depend on the risk involved and also may be conditional on the chance
of an unexpected outcome after implementation of the change.
(d) Different types of transitions in services
4.2-Concatenated changes
(1) Changes, e.g. novel, large or multi-actor changes, may involve several transitionalsteps 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 infollowing figure.
(2) The service provider's decision to implement the change in steps may have variousreasons, such as planning, training of personnel, gaining experience with specificelements of the change before progressing. Independently of the reason for thedecision, it is important to inform the ECAA of the

approach that is chosen and theconsequences for the change process, as it allows the ECAA to prepare, if necessary, fora 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 isnotified separately to the ECAA and will have its own assurance case.
(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 below).



(3) In cases where separate changes are concatenated, as shown in Figure 3, the ECAA 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 socalled‘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 ECAA about
The relationship in order to expose the common information. For such changes, specific arrangements between the service provider and the ECAA may be supportive for proper understanding and communication. Furthermore, the ECAA 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. However, since a transition may not meet the acceptance criteria for the transition in the assurance case, as part of the transition planning, the service provider may need or the ECAA may require a way of returning toan 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 ECAA needs to decide if this is acceptable and may impose specific conditions. The foreseen reduction in safety is to be brought to the ECAA’s attention as soon as it becomes clear. In supporting such a decision, the service provider will explain why such a reduction of safety can’t 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 and the operational service(s) of concern.
(e) Interactions — from notification to approval

A more detailed view93 of the process from notification to approval is shown below:



4.3 Processes prior to initial entry into service

(3) In cases where separate changes are concatenated, as shown in Figure 3, the ECAA 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 socalled‘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 ECAA about The relationship in order to expose the common information. For such changes, specific arrangements between the service provider and the ECAA may be supportive for proper understanding and communication. Furthermore, the ECAA may wish to make suitable internal arrangements in respect of its own phasing of the review of the change.

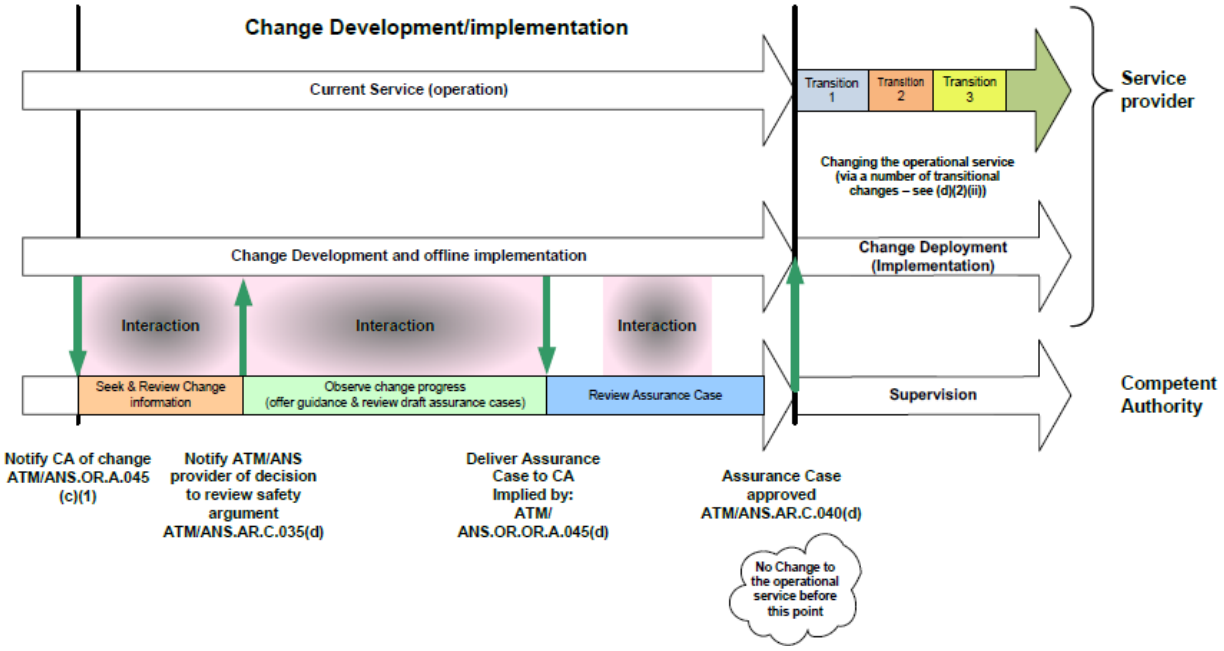
(5) The assurance case must argue and provide evidence that shows that the final operational service is acceptable92. However, since a transition may not meet the acceptance criteria for the transition in the assurance case, as part of the transition planning, the service provider may need or the ECAA may require 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 ECAA 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 serviceprovider will explain why such a reduction of safety can’t beprevented, what measures will be taken to limit the reduction of safety and whatoverall safety gain will be achieved.

(7) As discussed in (d) above, in all cases, the assurance case must cover the transitionservice(s) and the operational service(s) of concern.

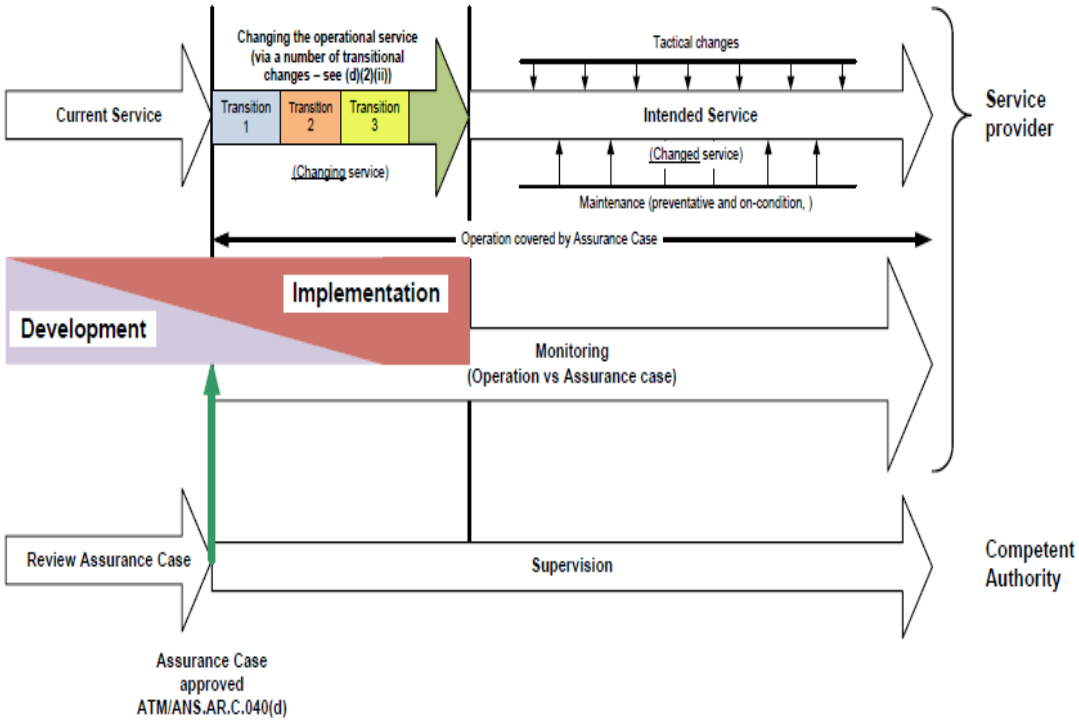
(e) Interactions — from notification to approval

A more detailed view of the process from notification to approval is shown below:



(1) The competent authority's activities in this part of the model are divided in three stages:
(i) Seek and review change information;
(ii) Observe change progress94 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 ECAA of the change.
Immediately after this the ECAA will seek the information needed in order to decide whether to review the assurance case or not .This information will result from interaction between the ECAA and the service provider and it will help the ECAA 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 ECAA does not need or wish to review every assurance case and the service
Provider will minimize the effort of interacting with the ECAA if it provides appropriate and sufficient information about the change.
(ii) Notification is an event. Its intent is to alert the ECAA 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 ECAA and the service provider.
(iii) Having decided whether or not to review the assurance case for the change, the ECAA needs to inform the service provider of the decision. 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 ECAA about the involvement of the ECAA.
(3) Observe change progress
(i) Once the service provider has been advised that the assurance case will be reviewed, the ECAA could wait for the assurance case report 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 novel103, the ECAA would be well advised to engage with the service provider earlier. This will allow the ECAA 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 ECAA to establish that the acceptance criteria are valid
(Relevant, sufficient and necessary).
(ii) Interaction may also be beneficial to the service provider. For instance, the ECAA, may have experience of similar projects for which the service provider does not have (i.e., he change may be larger or more complex than they are used to or may be novel). The ECAA 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 ECAA and the service provider where the ECAA learns about the change in a comfortable way and can offer guidance on the likely acceptability of the assessment and the assurance case.
(4) Review assurance case
(i) The next stage begins once the assurance case has been delivered to the ECAA. Fundamentally, the purpose of the review is threefold, i.e. to determine that: (A) the change is and will remain safe in accordance with the safety criteria(for ATS 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 ATS);
(B) the safety criteria are justified and establish a valid safety level that is a slow as is reasonably practicable and establish the appropriate safety support requirements (for ATS providers) and that the 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 (for service providers other than ATS); and
(C) 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 ATS 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 ATS).
(ii) The assurance case will be discussed by the service provider and the ECAA. 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 ECAA 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. When the change and the argument are considered acceptable to the ECAA, the assurance case will be approved and the change to the functional system can begin.
(iii) The phase ends with the approval or rejection of the change by the ECAA. For purposes of transparency and ultimately resolution of any legal challenge, the ECAA 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.
(f) Interactions — making the change operational an overview of the final part of the process is shown below.



4.4Making the change operational

(1) The operational service may begin to be changed after the:
(i) Receipt of the regulatory approval if the assurance case has been reviewed; or
(ii) Completion of a valid assurance case if the change is not to be reviewed by the ECAA.
(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 ECAA, normally there will be no interaction
Between the service provider and the ECAA in this phase. However, the review will have taken into consideration that the assurance case also covers any foreseen:
(i) Tactical changes, 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, while others may be temporary and/or addressed through the on-going performance monitoring of the functional system. Later changes may make monitoring requirements identified impervious assurance cases 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' of 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 ECAA may perform audits and/or inspections to check that:
(i) Any 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 ECAA will require the service provider to take appropriate corrective actions, which may include an amendment to make the argument valid, the instigation ofa change in order to make the service acceptable or even to revert to the situation before the change.

4.5-Approval of change management procedures for ATM/ANS functional systems

(a) The ECAA should check that the procedures used by a service provider to manage changes
Cover the complete life cycle of a change.
(b) When reviewing the content of the procedures, modifications, and/or deviations, the ECAA should use the compliance matrix provided by the service provider referred to in safety case circulars.
(c) The ECAA should check that the procedures are capable of initiating all the actions and
Producing all the evidence to comply with requirements laid down as means of compliance, if any. As part of this oversight activity, the ECAA should check that the compliance matrix covers all the aforementioned requirements.
(d) The ECAA should check that the procedures identify the roles and responsibilities of the service provider in the change management processes.
(e) The ECAA should agree with the service provider the means and method of submitting the
Procedures, modifications and deviations, until an agreement is reached, the ECAA will prescribe the means and method of submission.
(f) The ECAA 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.
(g) The ECAA 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.
(h) The ECAA should keep a record of all the change management procedures, modifications, and deviations it has approved and those that have been rejected, together with a rationale. The ECAA should be able to cross-reference them to the requirement of the associated Implementing Rule that they intend to comply with.

Chapter 5

Decision to review the notified change

5.1-Decision to review the notified change

Review Criteria — ATS Provider

(a) The review of a safety case.

(1) As the change to the functional system will only start being implemented 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. The table below describes The desired outcome for all possible states of the change and its associated safety case.

Safety case claim: 'The change is Adequately safe.'	**Change**	
Sound: The inferences and supporting evidence Justify the claim.	Adequately safe (Risk is acceptable)	Not adequately safe (Risk is not acceptable)
	The aim of the selection criteria is to minimize the number of reviews here.	Review cannot happen.
	No action needed — the desired state.	Selection criteria are not relevant because the change will be abandoned and the safety case will not be Submitted for review.
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.	State cannot happen. Review is necessary116 if the severity of the A consequence 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	The aim of the selection criteria is to maximize the number of reviews here
	Fix the safety case.	the change and the safety case

The possible states of a change

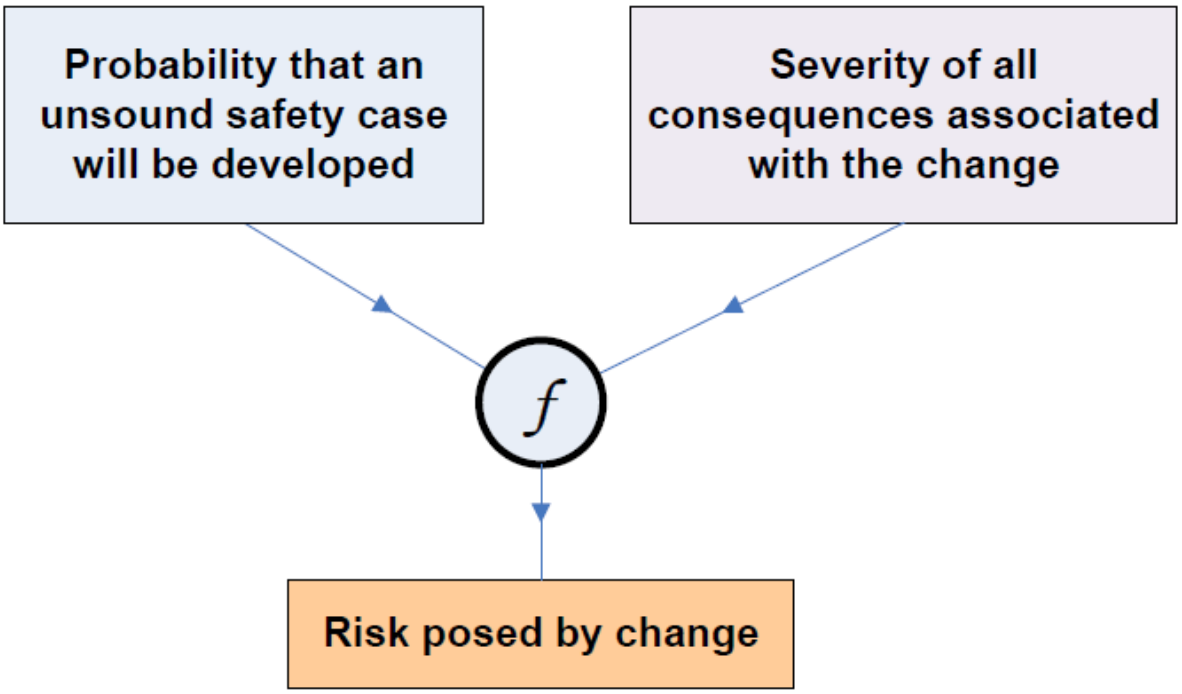
(3) The need for an independent review is based on the notion that two heads are better than one. There is some likelihood (small though it may be) of an unsafe change being developed, but the accompanying safety case claiming that the change is safe. While the ATS provider will use skilled and dedicated staff in the development and review of the change and its associated safety case, mistakes may still be made that remain undiscovered. An ECAA 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 ECAA deals with many ATS providers is likely to have a wider experience of different changes.
(4) The purpose of the review is to establish if the change is 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 safety case will be unsound and the severity of the consequences associated with the change as the selection criterion.
(5) 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) 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;
(ii) Interactions between the ATS provider will take place after the decision has been taken and before the safety case is presented for review;
(iii) 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 ECAA or the ATS provider. Therefore, a significant period should be allocated in the project for this interaction;
(iv) The interactions may change the safety argument (its inferences and the evidence needed) and so time needs to be available for this activity; and
(v) since the activities described above only occur once a decision has been made, itis likely to be more efficient to interact with the ECAA 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. 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
ATS provider will be subjected to the change. In other words, there are always some elements of the ATS provider's operational system that will be completely unaffectedi.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 severities of the consequences associated with the change are small.
(7) Selection for review should, therefore, be based on a combination of the likelihood that the safety case may be unsound 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 below:

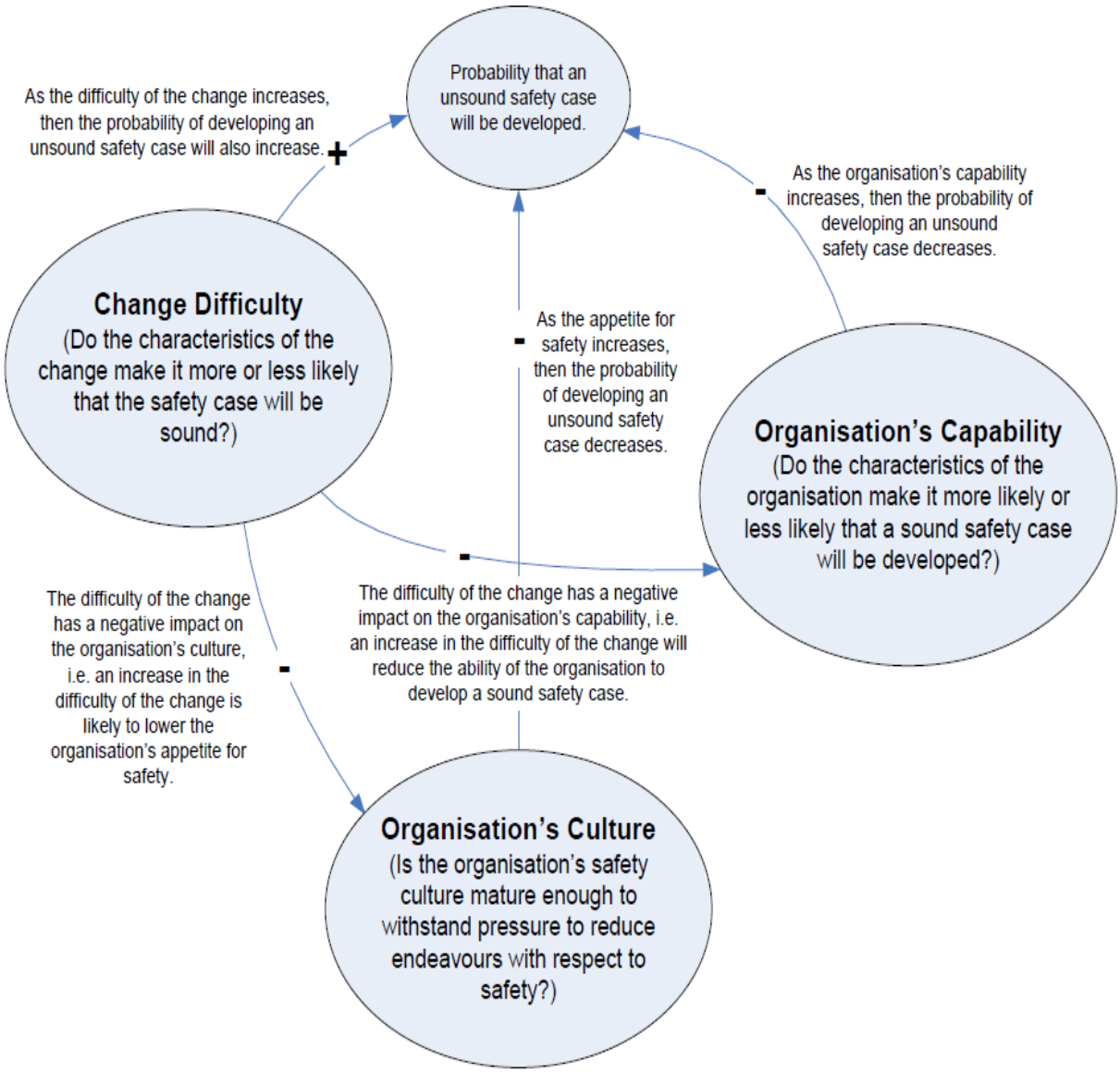


The risk posed by a change

(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 applied, proves to be unacceptable, and/or its safety is queried by the ECAA due to evidence arising after the change has started to be applied, 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 ECAA and/or changes before being approved or rejected or withdrawn by the ATS provider.
(d) The probability that an unsound safety case will be developed
(1) The actual risk, that is to be mitigated by the review of a change, is that associated with an unsound safety case i.e. one that misidentifies or misevaluates the risks associated with the change or provides insufficient evidence to support the inferences used in the arguments. The risks associated with the change stem 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; 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 all cases, 'change' means: addition, removal or a change invalue/nature of some property of the system.
(2) Three different aspects of the change and the organizations performing the change can affect the likelihood that an ATS provider will develop an unsound safety case:
(i) The difficulty of the change
(A) Its size;
(B) Its complexity (technical & managerial);
(C) Its novelty; and
(D) Its span (the range of different services impacted).
(ii) The capability of the ATS provider121
(A) Its technical capability — to manage the complexity, 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 organizations 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 ATS provider safety culture
(A) The stability of the organization; and
(B) The quality of its SMS.
The way these aspects interact is shown in Figure below:

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 system and possibly a projection associated with the future demand rate if it is to be different from the current demand rate.

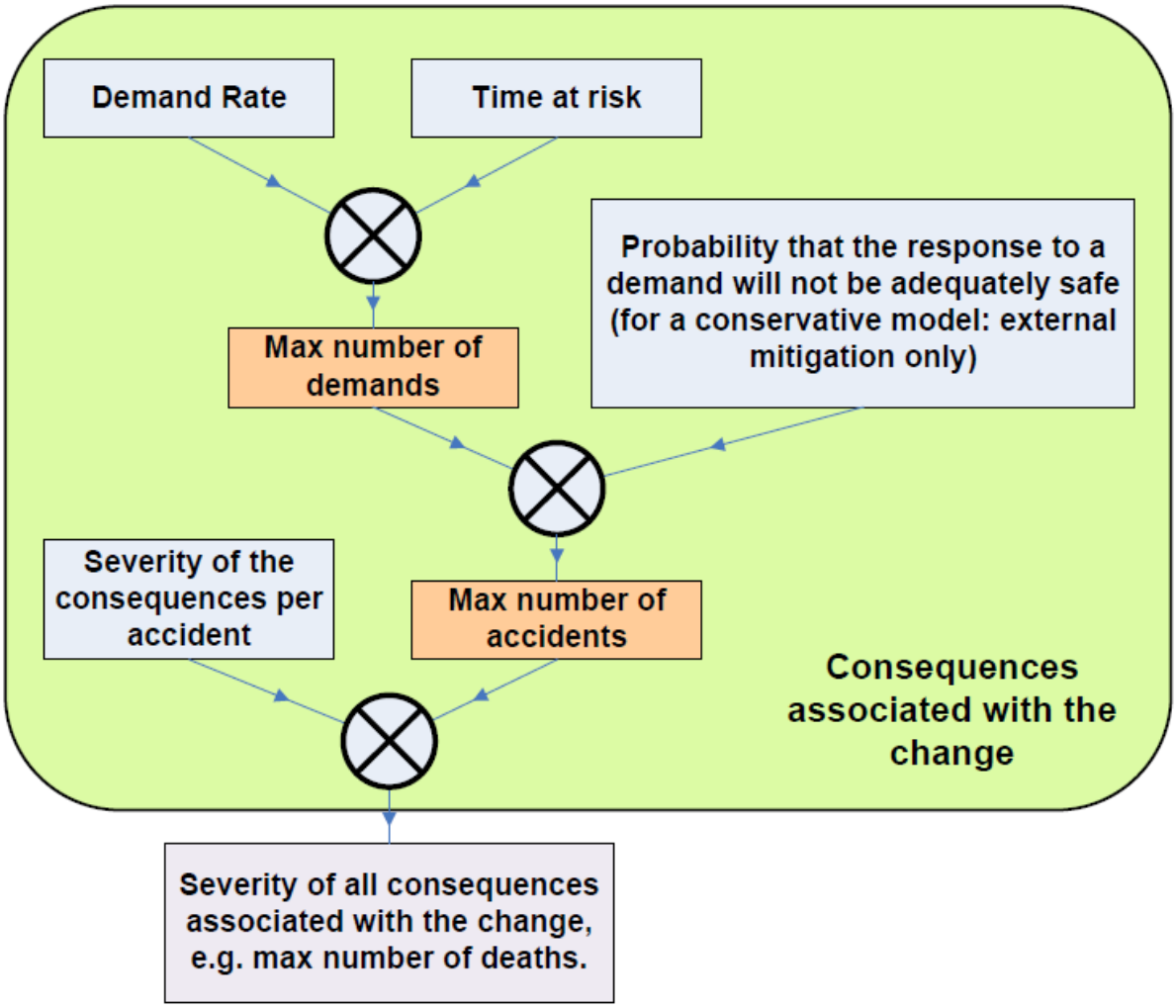


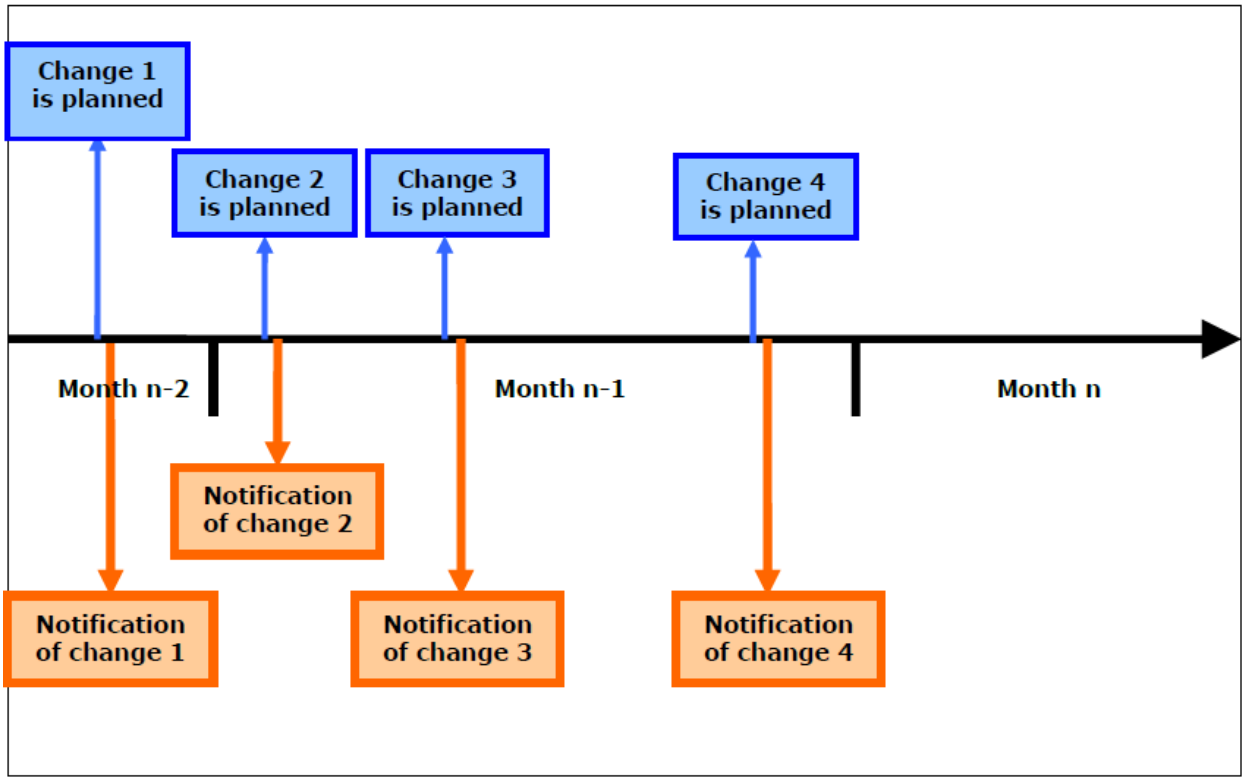
Figure 3: The consequences of a change

(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 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 a scale (which is inevitable when Involving judgment as inputs),
then the result is that the risk posed by a change (the Figure 3: 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 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 a scale (which is inevitable when
Involving judgment as inputs), then the result is that the risk posed by a change.

5.2Changes to the functional system

Means of Notification
(a) There are different means of notifying changes to the ECAA. An appropriate means has to be selected and agreed with the ECAA, 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) organized.
(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’, 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 ECAA 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 ECAA can start the review decision process early.
(2) Periodic notification
The service provider notifies changes to the ECAA 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 ECAA. 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 centralize the notifications for the operational units.
The ECAA 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 ECAA to produce one single answer listing the changes subject to review, facilitating the response process. (3) Short lead time notifications.
When notification occurs close to the scheduled date of entry into service, the service Provider and the ECAA may make the appropriate arrangements to allow individual notifications to be submitted out of the periodic notification period so as to be able todeal with changes on time. This type of short lead time notification is a departure fromthe 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 ECAA should agree on amending the change management process.
The ATS provider may submit an explanation of the impact on safety and other service provider 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 ECAA 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 easily be spotted by the ECAA.

Safety Support Case and Safety Case

(a) The key concepts used in safety and safety support assurance and the terms used to describe them are given in the table below:

Safety Support		**Safety**	
Safety support assurance	Argues that the service behaves only as specified in the Specified context.	**Safety assurance**	Argues that the proposed change to the functional system is acceptably Safe.
Safety support case	A structured documented argument, supported by evidence, that provides a compelling, comprehensible and valid justification that the system behaves only as specified in a given Context. **Safety case** A structured documented argument, supported by a body of evidence that provides a compelling, comprehensible and valid justification that a system is acceptably safe for a given application in a given operating Context.	**Safety case**	structured documented argument, supported by a body of evidence that provides a compelling, comprehensible and valid justification that a system is acceptably safe for a given application in a given operating Context.
Safety support case report	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	**Safety case report**	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

	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 regulator ECAA requires for the evaluation.		bulk of the supporting evidence due to the practicalities of providing it in the report. The ATS provider is obliged to facilitate access to any of this additional information that the regulator ECAA requires for the evaluation.
Safety support assessment	All the activities required to produce a safety support case,	**Safety case report**	All the activities required to produce a safety support case, i.e. all the activities
Assurance case	The collective noun used for either safety cases or safety support Cases.		
Assurance case report	The collective noun used for either safety case reports or safety support case reports.		
Requirement:	A thing that is needed or wanted (it will be or will do); a necessary Condition.		
Specification:	precise and detailed definition of what a thing is claimed to be and To do.		