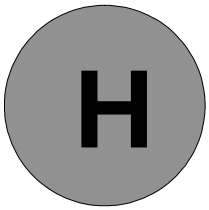

ANNEX:

CHANGE DETERMINATION PROCESS

(“WHAT IS A CHANGE?”)

TABLE OF CONTENT

1 INTRODUCTION

This annex proposes means to assess whether an event in the Air Navigation System can be considered as a change as per ESARR4 and EC Common Requirements 2096/2005 and to determine which type of safety assessment should be conducted depending on the nature of the event.

2 PURPOSE

The purpose of this Guidance Material is two fold:

- Firstly propose guidelines (based on a process) to determine when an event can be considered as a change as per ESARR4 & SES CR 2096/2005.
- Secondly, propose guidelines (based on a process) to determine which type of safety assessment should be conducted for events considered as change as per ESARR4 & SES CR 2096/2005.

It is also important to recognise that the application of this guidance will be strongly linked to and reliant upon the ANSP safety management system, particularly for the following:

- Existing risk assessments and procedures – for reference and to generate new risk assessments;
- Safety Management System – procedures, document and records control;
- Competence management system – to ensure the competence of the ATM operational and maintenance staff;
- Change management system – to ensure all change proposals are formally assessed and approved/rejected and that suitable records are maintained;
- Quality Assurance system – procedures, document and records control;
- Project management procedures – to control the change lifecycle;
- Safety occurrence reporting system – to ensure that urgent unanticipated changes are followed up with the necessary risk assessments, etc. when time permits;
- The survey & review process – to identify any necessary changes to the safety management system which are required;

- The argument developed to demonstrate that existing operations (so-called “legacy”) are acceptably safe;

- Contingency planning and procedures – to ensure that all credible contingency requirements are addressed.

3 TERMINOLOGY

In this document, the word “change” will be restricted to the meaning of a “change” as per ESARR4 & SES CR 2096/2005.

Anything happening that is subject to a determination whether it is or not a change as per ESARR4 & SES CR 2096/2005 will be so called “event”.

An event could be due to an ATM or no ATM event.

In this document each time ESARR4 is mentioned, in fact both ESARR4 and SES regulation CR 2096/2005 are meant. However, for readability reason, only ESARR4 will be mentioned.

4 APPROACH

The provision of an air navigation service is inherently risky operation providing the primary means of avoiding accidents (e.g. aircraft collisions). The existing systems in use across the ECAC states have been developed over an extended period of time, much of which pre-dates formal safety management practices. In many cases the only evidence that legacy systems are ‘tolerably safe’ is that they have been considered so over years of operation and that the provision of the service has been certified by NSA in the framework of the compliance to the Single European Sky Common Requirements 2096/2005.

Safety management practices rightly demand that before acting or intervening onto a safety related system, appropriate steps are taken to ensure that such action or intervention does not introduce an unacceptable risk into the system.

The aim of this study is to identify when a safety assessment should, or should not be applied and which type of safety assessment. This includes to identifying what events can be implemented in the ATM system without the need for a safety assessment procedure. It is recognised that there are many events made to the system on a day-to-day basis for which a formalised and recorded safety assessment is not undertaken, indeed were necessary the whole operation would be unable to continue (possibly presenting a greater risk than implementing the event without assessment). In many cases such events are already covered by an existing safety assessment – they are merely “configuration changes” within a safe ‘**operational or design envelope’**.

5 CRITERIA TO DEFINE THE OPERATIONAL ENVELOPE AND THE ATM SYSTEM FOR THIS PROCESS

The operational envelope for strategic event should be defined as:

- Operations manuals as per the EC reg. Common Req 2096/2005 Annex I cpt. 3.3 including all technical procedure related to the ATM system.(check for completeness)
- National, international legislation, standards(operational actions themselves but excluding methods to be used to derive the local operational actions);
- supported with :
    - local previous experiences in managing the event
    - safety assurance of previous usage.
    - Production of evidence of correct application (this evidence is the one produced as per the operational procedure application, it is not a additional specific safety assessment evidence. See step3)

  N.B. The objective is to describe procedures that are not formally in the Operational Manual Document but which are used and applied and delivered a safe service.

The operational envelope for anticipated tactical event should be defined as:

- Operations manuals as per the EC reg. Common Requirements 2096/2005 Annex I cpt. 3.3 plus all technical procedure related to the ATM system.
- National, international legislation, standards;
- supported with :
    - And previous experiences in managing the event.
    - And safety assurance of previous usage.

NB: The baseline of the operational envelope is the one that was defined at the time of the SES CR certification. Any change (as defined in this document) of the operational envelope baseline is subject to risk assessment and mitigation as per ESARR4 or SES CR 2096/2005 Annex II.

NB: the definition of Operational envelope has to be validated, maintained approved and included in the ANSP safety management system.

NB :Air Traffic Management (ATM) System definition: An ATM system is part of ANS system composed of a ground based ATM component and an airborne ATM component. (cfr. EUROCONTROL SRC RTF , http://www.eurocontrol.int/src/public/standard_page/other_srcsru.html)

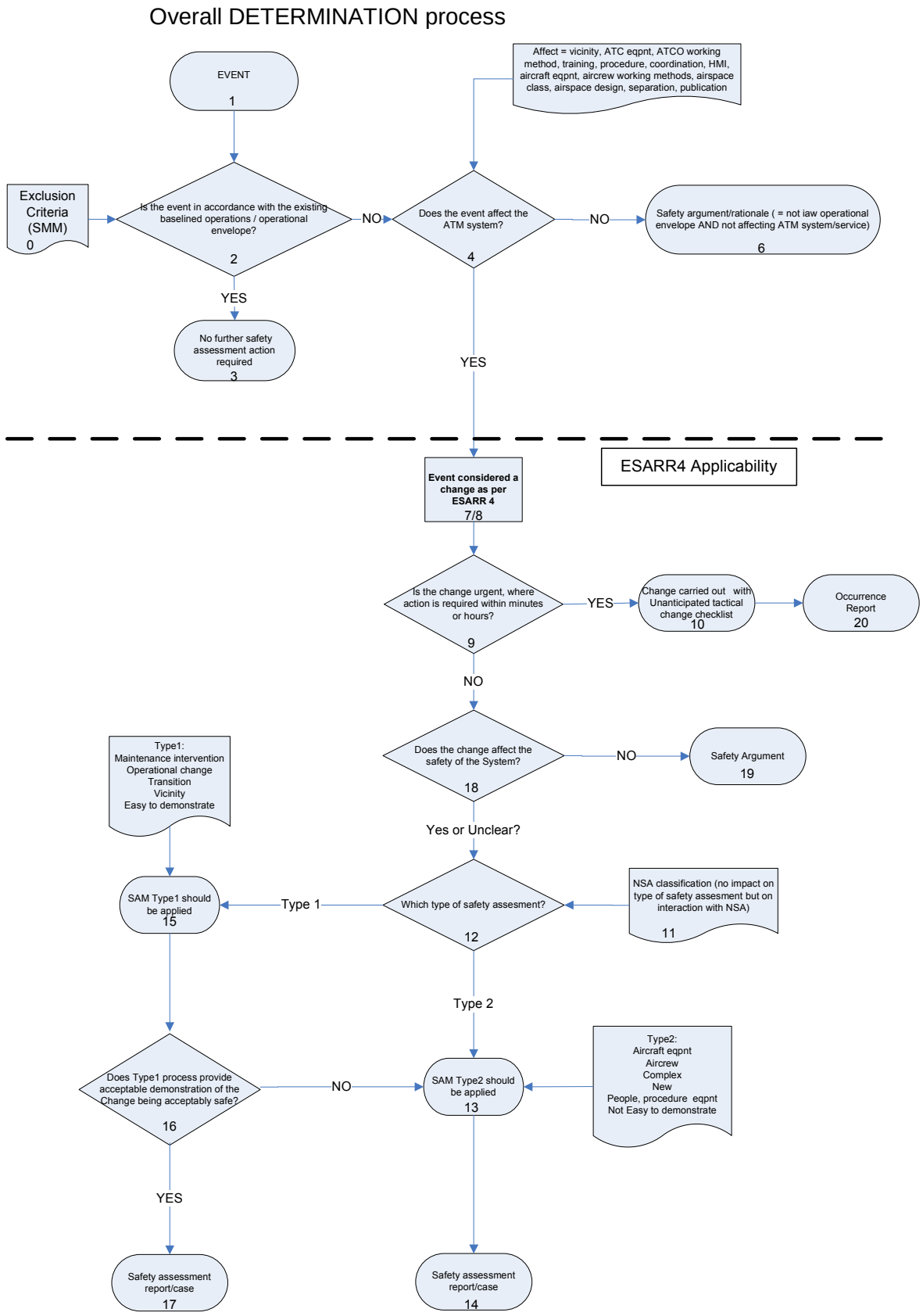

Figure 1: Determination process

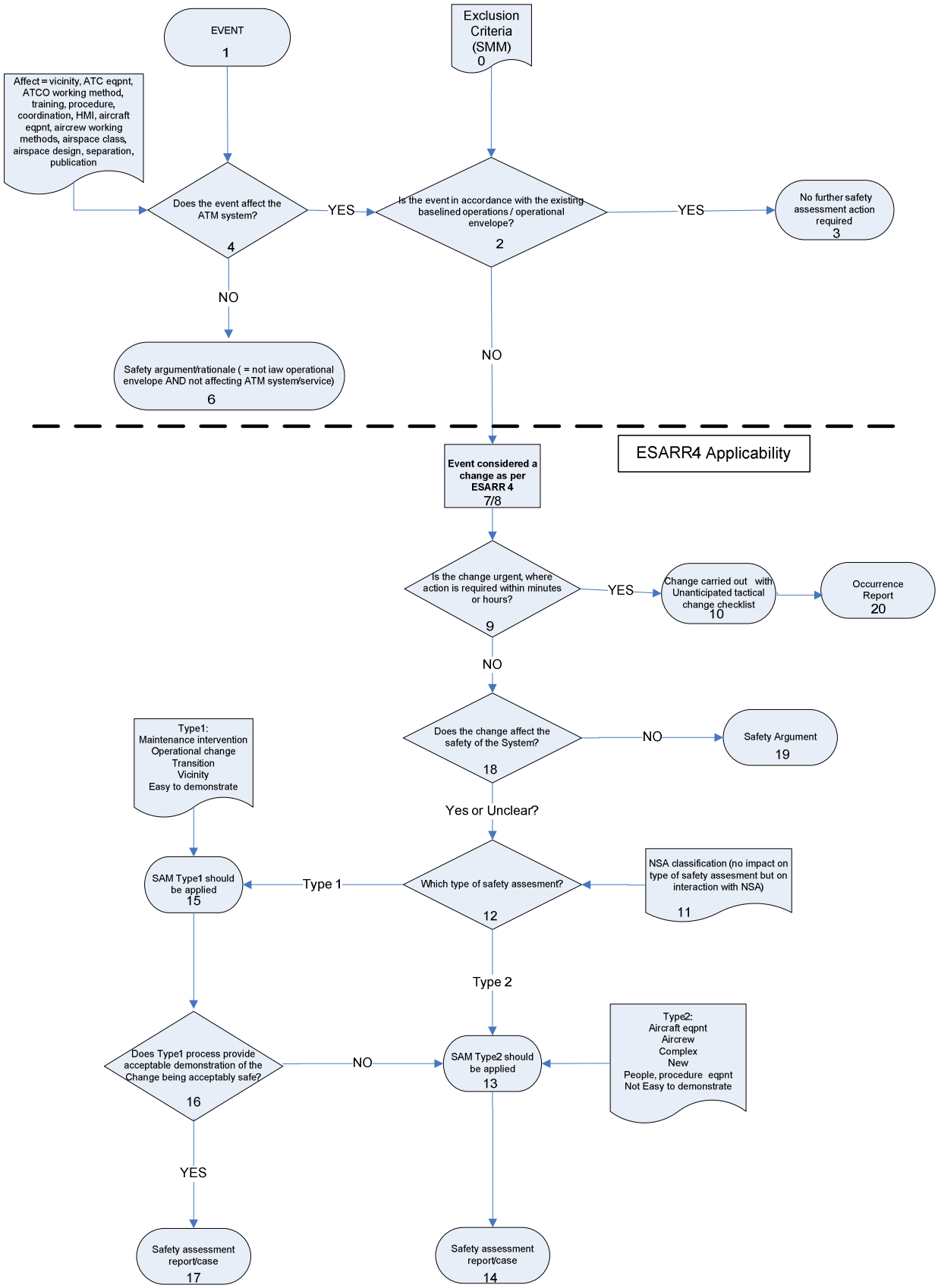

Figure 2: Determination process

Both flow charts can be used.

Depending on the highest number of events:

either being part of the operational envelope (See figure 1)

or of “administrative” nature (event not affecting the ATM system/service, See figure 2),

ANSPs will select one of the two flow charts or will propose different flow charts to different parts of their organisation (e.g. figure1 applicable by the Operational Division and figure2 applicable by the Procurement Division).

6 DETERMINATION PROCESS STEPS

6.0 Step0: Exclusion Criteria (SMM)

The Exclusion Criteria allow determining whether an event is in accordance with (iaw) the baselined operational envelope.

The Exclusion Criteria are part of the Safety Management Manual. Therefore it has been endorsed by the ANSP Safety Manager, accepted by the ANSP Senior Manager and approved by the National Supervisory Authority (NSA).

For more information on the Exclusion Criteria content, criteria and management, please refer to Appendix 1 §3

For more information on the baselined operational envelope, please refer to §5.

6.1 Step1: Definition of Event

Any modification of operational or technical aspects of the Air Navigation Service Provision, upgrade, degradation, removal/decommissioning is considered as an event.

6.2 Step2: Operational Envelope

Step2 decides whether an event can be considered as part of the normal operations as defined in the baselined operational envelope.

This step consists in assessing the event using assessor competence.

Such competence includes the knowledge and usage of the Exclusion Criteria.

As the assessor has to rely on his/her competence, such responsibility should be part of his/her job description and more specifically part of his/her safety responsibilities/accountabilities. Consequently, he/she should be trained, assessed and maintained competent for such task.

The assessor can be:

- Operational staff :
    - ATCO for any operational event under his/her responsibility (e.g. allocation of direct to a point as per Operational Manual; management of policy flights, management of emergency, …);
    - Supervisor (e.g. splitting/combining sectors, activation/deactivation of TSA as per Operational Manual);
    - Flight Data assistant (e.g.change of flight plan as per Operational Manual);
    - Simulator Instructor (e.g. initiating a training session scenario);

- Technical staff:
    - Technical Supervision staff (e.g. main/stand-by switch as per Technical Manual);
    - Simulator technician (e.g. loading an existing simulation scenario);
    - Urgent corrective maintenance intervention.
- Management:
    - Senior management (e.g. Reorganisation);
    - Line management (e.g. Procurement/Finance manager when purchasing non-operational related parts or services or when purchasing specific items as identified in the Quality Management Manual (e.g. ink, paper, fuel));
    - Air Traffic Management Unit Manager (e.g. next month shift roster planning as per the rules).

This step should not generate any safety assessment evidence if the answer is “YES” (going to Step3).

Competence may also be relied upon for any event that requires an immediate action (0 to few minutes) for which no knowledge or training exists. Such event has to be immediately operationally managed even though no safety assessment was conducted before (See §7.3.3). Such event should lead to fill an ESARR2-type occurrence report. Such report should be assessed as per the determination process to decide which type of safety assessment should be performed in order to ensure that future occurrences of such event will not be anymore unknown.

Safety surveys (e.g. Normal Operation Safety Survey (NOSS)) could be used as means to ensure that Step2 is conducted in accordance with the Safety Management Manual procedure describing the Determination Process which should specify that staff competence.

6.3 Step3: No further safety argument

Step2 conclusion is that such event has been classified as being part of the Operational envelope (part of the baselined mode of operation) as specified in the Exclusion Criteria. No further safety assessment action is needed.

No specific safety assessment evidence of such decision exists. However, the operational procedure applied to manage such event may require filling some form that can be used as evidence. The determination process as such does not require any additional evidence production in addition to the operational procedure output.

Examples of events would not require additional safety assessment are:

- Planned Declared Sector capacity change within the sector type maximum declared capacity
- ATFCM Service change (no change to mode of operation)
- Unexpected weather change (unforeseen but known)

(For a more extensive list of events refer to the Appendix 1 § 3.1)

6.4 Step4: Identification of event affecting ATM System

Step2 has concluded that this event was not part of the Exclusion Criteria. The event owner submits this event to a Change Assessment Process (CAP) in order to determine whether the event may affect the Air Navigation System/Service.

The following **non-exhaustive** types have been considered to define the verb "affect":

- non ATM events affecting the ATM: System / services
    - Vicinity: if the event occurs in the geographical proximity of the Air Navigation System even though it is not part of it, then it can be considered as a change (e.g. building nearby the ILS, works in the ATCC that can generated noise, dust, vibration impacting the Air Navigation System/Service),
    - Installation of non-ATC equipment in ATC environment
    - Environmental restrictions (noise abatement), New security systems,
- ATM events affecting the ATM System / services :
    - ANS equipment: if the event modifies an ANS equipment;
    - Staff working method (ATCO, flight data assistant, operational &, technical supervisors, technical maintenance): if the event modifies staff workings method beyond their definition as stated in the baselined operational envelope;
    - Staff training (ATCO, flight data assistant, operational &, technical supervisors, technical maintenance): if the event modifies staff training beyond its definition in accordance with the baselined operational envelope;
    - ATM Procedure: if the event modifies ATM Procedures beyond their definition as stated in the baselined operational envelope;
    - Coordination (Inter/intra centre/sector, technical/operational): if the event modifies coordination beyond its definition as stated in the baselined operational envelope;
    - HMI (Human Machine Interface) (operational and technical): if the event modifies operational HMI beyond their configurability range as stated in the baselined operational handbooks/users manual;
    - Aircraft equipment or aircraft equipment standard: if the event modifies aircraft equipment (number and type) or aircraft equipment standard (specification) beyond their definition as stated in AIP/AIC (Aeronautical Information Publication/Circular);
    - Aircrew working methods/ATM&Navigation procedure: if the event modifies aircrew working methods or aircrew ATM&navigation procedures beyond their definition as stated in AIP/AIC (Aeronautical Information Publication/Circular),

- Airspace class (See ICAO Annex 11 §2.26): if the event modifies the airspace class assignment beyond its definition as stated in the baselined operational envelope;
- Airspace design (See ICAO Annex 11 §2.26): if the event modifies the airspace design beyond its definition as stated in the baselined operational envelope;
- Separation standard (See ICAO Annex 11 §2.26): if the event modifies the separation standard beyond its definition as stated in the baselined operational envelope;
- Publications: if the event modifies the publications (AIP, AIC, LoA) beyond their definition as stated in the baselined operational envelope.

If the decision whether the event affects or not the Air Navigation System/service cannot be sustained with a rationale, an argument, then it has to be processed as a change.

6.5 Step5: N/A

6.6 Step6: Safety argument / rational

As Change Assessment Process concluded during Step4 that the event does not affect the Air Navigation System/Service, no safety assessment of any type is needed.

Change Assessment Process should produce a rationale, a safety argument sustaining such decision.

6.7 Step7

Combined with Step8.

6.8 Step8: Identification of a change

As Change Assessment Process concluded during Step4 that the event does affect the Air Navigation System/Service, then the event is from now on considered as a change.

For a extensive list of example please refer to Appendix 1 §3.3

Examples of changes deserving a safety assessment are:

- New building on airport
- Introduction of a new services
- Change of the system architecture
- Change of a procedure
- Introduction of new separation standards
- Temporary airspace change out of the mode of operation (exceptional/big airshow, …)

6.9 Step9: Identification of urgent changes

Change Assessment Process should assess whether the change is considered in an urgent tactical timeframe (few hours).

See §7.3.2 for more explanation on “unanticipated tactical change”.

6.10 Step10: Check List for urgent changes

As Step9 decided that this change was an unanticipated tactical change, the Type1 safety assessment as described in Appendix 1 §1.13 should be applied.

As part of applying such Type1 safety assessment, an “occurrence report” should be filled to record such occurrence and trigger a safety assessment to anticipate any future similar event.

See Appendix 1 §1.13 for guidance to conduct Type1 safety assessment of unanticipated tactical change.

6.11 Step11: NSA Classification

The classification of changes as stated by the NSA and as identified in the SMM (Safety Management Manual) requires the ASNP to submit the safety assessment of given categories of changes to the NSA for review and approval. Consequently, such requirement impacts the interaction with the NSA with regards safety assessment/case.

The NSA classification should not impact the type of safety assessment to be conducted for a given change as any type of safety assessment should generate the appropriate argument and evidence that the change can be safely introduced into operation and operated.

6.12 Step12: Identification of type of assessment

This step decides which type of safety assessment fits more the nature of the change.

Step12 assesses whether a change deserves a Type1 or a Type2 safety assessment.

By default a Type2 safety assessment should be conducted.

The criteria for such decision are the following:

Type1 safety assessment has to be conducted for the following non-exhaustive type of changes (the reference is provided to the Appendix1 of this document describing the tailored way of conducting safety assessment):

1. Maintenance Intervention (excluding. Urgent Corrective maintenance) (Appendix 1 § 1.1)
2. Changes triggered by external providers (Appendix 1 § 1.2)
3. Sharing information on Cross Border Changes (Appendix 1 §1.3)

4. Notification of cross-border technical interventions (multi-sites ...) (Appendix 1 § 1.4)
5. Transition phases (Appendix 1 §1.5)
6. Replacement of HW by equivalent HW.(Appendix 1 §1.6)
7. ATC Procedural/Operational Changes (Appendix 1 §1.7)
8. Connection of Non Operational Sub-Systems onto the Operational System. (Appendix 1 §1.8)
9. Changing roster scheme (Appendix 1 §1.9)
10. Modification of Configuration Data (Appendix 1 §1.10)
11. Modification of HMI Lay-out (subset) (Appendix 1 §1.11)
12. Unanticipated Tactical Change (Appendix 1 §1.12)
13. Easy to demonstrate (Appendix 1 §1.13)
14. Vicinity (Appendix 1 §1.14)
15. Software correction (Appendix 1 §1.15)

Change Assessment Process should produce rationale and evidence of decision for applying Type1 Safety Assessment. The decision rationale should be included into the records. (See §9 for such Change Assessment Process decision record template).

Type2 safety assessment has to be conducted for the following non-exhaustive type of changes:

- Aircraft equipment or aircraft standard: when the change impacts aircraft CNS/ATM equipment or aircraft CNS/ATM standard.

- CNS/ATM Aircrew working methods or procedure: when the change impacts aircrew CNS/ATM working methods or procedure.

- Complex - People & procedure & equipment: When the change impacts the three ATM elements (people & procedure & equipment) and/or has a high level of complexity that implies a complex safety assessment.

- New system or service or application: When the system or service or application is new from the definition point of view or new for the local implementation point of view (already implemented by other ANSPs but for the first time for the ANSP in charge).

- Not Easy to demonstrate: When the change implies a complex safety assessment.

However, some changes may not be submitted to Change Assessment Process for assessment due to lack of safety culture dissemination through the organisation. Consequently, some means should be put in place as part of the SMS to improve this aspect of SMS implementation such as an updated list of changes and their associated type of safety assessment or safety survey.

6.13 Step13: Application of the Type 2 safety assessment

Step13 consists in conducting the Type2 safety assessment of the change.

It can be decided to conduct a Type2 safety assessment on a wider scope than the scope of the change itself (the scope can be only wider, not narrower).

The rationale for such decision of an extended scope of safety assessment can be justified by an organisation policy to benefit from a change to conduct safety assessment at level which will

avoid duplication of effort or reduce potential inconsistencies with near to come safety assessments on related topics.

Note that conducting a Type2 safety assessment does not imply that all steps of the SAM namely FHA, PSSA and SSA have to be all conducted again. If previous Type2 safety assessments were done on changes having equivalent scope, then maybe some SAM steps have only to be reviewed (e.g. review the existing FHA for system definition, operational environment and assumptions confirmation, however, the PSSA and SSA have to be partially updated). Consequently, the safety argument and safety plan will justify the appropriateness of the way to conduct the Type2 safety assessment.

Even if Step11 does not impose to submit the safety assessment to the NSA for review, then the safety assessment (type1 & type2) should always be applied as described in the ANSP Safety Management Manual.

6.14 Step14: Safety assessment report as type2 safety assessment output

As a result of Step14, a safety assessment and its associated safety argument are produced that should be put under configuration management and maintained up-to-date with regards system evolution.

6.15 Step15: Application of the type1 safety assessment

Step15 consists in conducting an appropriate Type1 safety assessment of the change.

Type1 safety assessments are NOT conducted on a wider scope than the scope of the change itself.

Even if Step11 imposed to submit the safety assessment to the NSA, then the Type1 safety assessment should always be applied as described in the ANSP Safety Management Manual.

If a previous Type1 safety assessment was done on a change having an equivalent scope, then maybe it has only to be reviewed or updated.

6.16 Step16: Acceptability check of Type1 output

Step16 decides about the acceptability of the demonstration that the change is acceptably safe, based on Type1 safety assessment outcome.

If the demonstration is not adequate then a Type2 Safety Assessment should be conducted (See Step13).

If the demonstration is adequate then the Type1 Safety Assessment results are captured through Step17.

The definition of “adequate” is that the demonstration satisfy safety acceptability claim

6.17 Step17: Safety assessment report as Type1 safety assessment output

As a result of Step17, the Type1 safety assessment should produce some argument and evidence that should be part of a safety assessment/case that should be put under configuration management and maintained up-to-date with regards system evolution.

6.18 Step18: Safety impact of the change

Step18 decides about the safety impact of the change. More precisely, Step18 decides about the absence of safety impact of the change (supported with evidence, see Step19).

If the safety impact is obvious or the absence of safety impact cannot be demonstrated, then Step12 should be conducted.

6.19 Step19: Safety Argument of absence of safety impact

Step19 collects the argument and evidence that the change has no safety impact as stated by Step18.

6.20 Step20: Occurrence Report for unanticipated tactical change

Step20 raises a technical occurrence to capture the occurrence of an unanticipated tactical change that was assessed only via a checklist (See Step10).

Such technical occurrence report will ensure that an appropriate *a posteriori* safety assessment (Type1 or Type2) is performed for such change and that the next occurrence of such event will be addressed by the new release of the operational envelope baseline.

7 TYPES OF CHANGES

7.1 Introduction

Changes applied to the Air Navigation System/Service can be classified as follows and further explained below:

- **Strategic changes**
- **Tactical changes**
    - Anticipated Tactical Changes;
    - Unanticipated Tactical Changes;
    - Immediate Unanticipated Tactical Changes.

Only changes are considered in this section, it means those changes are event that are assessed by the determination process as changes (beyond the step7/8)

7.2 Strategic Changes

Strategic changes are those changes that are anticipated and planned and as such, a thorough risk assessment can be undertaken in advance of implementation and transfer into operation. Typically this will include engineered changes to the system, such as new equipment or procedures or airspace, routes, SIDs and STARs or resectorisation (additional sector or change of the existing sectorisation) or ….

Strategic change is what might be considered the normal process of change in Air Navigation. A strategic change will involve changes to one or more parts of the Air Navigation System/Service (people, procedures & equipment) which are applied with prior consideration and planning. Strategic changes would include, amongst others, new services, changes to hardware or software in the Air Navigation System/Service, airspace redesign or changes to operational procedures or staffing arrangements.

An appropriate type of safety assessment (type1 or type2) will be applied depending on the nature of the change.

7.3 Tactical changes

Tactical changes (not tactical event) are those changes that are necessary as a result of circumstances and situations that arise during operation of the system

Ideally, all these changes should have been assessed from the safety point of view before being introduced into operation..

7.3.1 Anticipated Tactical Change

An anticipated tactical change may be defined as “an operational change to the Air Navigation System/Service that has previously been planned for” and “for which normally associated risks have been assessed” before to introduce the change in to operation.

Type 1 safety assessment will be conducted for those anticipated tactical changes; if a type 2 safety assessment is found necessary (cf step16) then this change became a strategic change and the introduction into operation should be re-scheduled in accordance with the safety assessment conclusion.

Examples of Anticipated Tactical Change are:

- Unknown or unusual tactical activation of TSA (Temporary Segregated Area);
- Unknown or unusual tactical aircraft operations, parachuting exercise, ...

7.3.2 Unanticipated Tactical Change

An **unanticipated** tactical change may be defined as a change to the established normal, degraded, or emergency Air Navigation operations which is not identified in the baselined Operational envelope and to be managed under time constraints.

This change should be subject to a formal risk assessment, but the **time will only permit assessing some subjective consideration of the risks** and identifying the best way to mitigate them.

In this situation heavy reliance is placed upon the Air Navigation staff’s competence and experience.

Filling a subsequent occurrence report will trigger an *a* posteriori review and a risk assessment of the change .

For such change, there is no more time to carry out a risk assessment and mitigation in accordance with ESARR4 & SES CR 2096/2005 and the change cannot be postponed.

Typically, “time constraint could range from a **few minutes to a few hours**, and it is important to make the best use of this time to minimise risk.

Examples of unanticipated tactical changes are:

- Lebanon war in summer 2006;

- Contingency occurrence to happen in few minutes or hours for which no contingency plan exists;
- Extreme weather conditions forecast in few minutes or hours but never experienced by OPS staff in the considered operational environment;
- Operational circumstances to happen in few minutes or hours for which no procedure or experience exist;
- …

7.3.3 Immediate Unanticipated Tactical Change

An **immediate** unanticipated tactical change may be defined as a change to the established normal, degraded, or emergency Air Navigation operations which is not identified in the baselined Operational envelope and to be managed immediately (no time at all for any form of formal safety assessment).

This change should be subject to a formal risk assessment, but the **time will not permit any type of safety assessment**.

In this situation full reliance is placed upon the Air Navigation staff's competence and experience.

Filling a subsequent occurrence report will trigger an *a posteriori* review and a risk assessment of the change.

In order to help defining "immediate": its value should be expressed in number of seconds or very few minutes.

Examples of immediate unanticipated tactical changes are:

- 9/11 at the time it happened;
- Actual immediate contingency occurrence for which no contingency plan exists;
- Actual immediate operational circumstances for which no procedure or experience exist;
- …

8 LISTS

8.1 Exclusion Criteria (Step0 & 2)

The Exclusion Criteria aim to identifying those events that are “not subject to further safety assessment” and are used by the initial step in the determination process (Step2).

Such events are defined as being part of the baselined operational envelope.

The Exclusion Criteria should include references to any baselined document or manual (e.g. Operation Manual) against which events will be assessed.

The maintenance and update of the operational envelope baseline (set of documents which specify what is considered as the on-going operational Air Navigation System/Service) has to be specified as part of the ANSP Safety Management Manual.

Examples of such events are proposed here after.

Events not subject to any further safety assessment (proposed list to be validated, maintained, approved and included in the ANSP Safety Management Manual):

- Identical HW spare (exact same specifications -incl. dissimilarity req.-)
- Operational action in accordance with the baselined Operational envelope:
  - Planned Declared Sector capacity change within the sector type maximum declared capacity;
  - Temporary airspace change part of the mode of operation (military, parachuting, small airshow, …);
  - Phraseology change (inside ICAO and inside mode of operation);
  - Restricted area activation (known area);
  - Special flights (e.g.: State/Head of State) (dynamic restricted area);
  - Police flights;
  - Combining/splitting sectors (existing);
  - Change of ATIS message content (e.g. every 20 minutes);
  - Frequency change (normal operation);
  - Summer programme;
  - Change of hour (summer/winter);
  - Sharing airspace with Military;
  - Temporary closing an airport for several hours;
  - Newly qualified staff in ops room;
  - Tactical request for closure of area due to SAR, police, intruders…
  - Manual coordination of Entry/Exist FL;
  - ATCO to ATCO dialog;
- Furniture managed via the Quality Management System (QMS):
  - Change of Furniture (pen, ink, fuel);
  - Change of Battery vendor for Voice comms.
- Training:
  - Changing trainer (licensed trainer);
  - Conducting a training session;
  - First OJTI for ATCO on new sector;
  - Delivery of a training session (operational training: ESARR5-related + competency in ESARR3-related) (at the time of delivering a session of the

training, but it assumes that the training plan and material have been assessed & accepted);
- Usual weather conditions;
- …

8.2 Examples of Events NOT part of the operational envelope and NOT affecting the ATM system/service (Step4)

This paragraph proposes examples of events which are NOT part of the operational envelope and that do NOT affect the ATM system/service:

- Replacement of or new material for administration offices (not on operational/simulation network and not in areas adjacent to operational system);
- Replacement of or new test equipment (for those equipment which do not impact operational equipment or not adjacent to them);
- Periodic actions on administrative rooms (cleaning, ...) (excluding those that can be noisy, generate dust or vibrations nearby operational areas: see Step4);
- Decommissioning of administrative (non-operational) equipment not in a area adjacent to operational systems;
- Visitors in Operation-related areas of the Centre (in accordance with the approved Security rules);
- …

8.3 Examples of changes (Step7/8)

This paragraph proposes examples of changes:

- New system (people, procedure, equipment);
- New service;
- AIRAC Change (except non-ATM operations-related, correction of previous erroneous data, already published in NOTAM);
- Reduced separation minimum to be applied within an airspace or an aerodrome;
- Reorganisation of the ATS route structure;
- Resectorisation of an airspace;
- Airspace class change;
- Physical changes to the layout of the runways and/or taxiways at an aerodrome;
- New type of aircraft (new performance characteristics including aircraft navigation capabilities and navigation performance);
- Inclusion of a new waypoint;
- Suppression of an existing waypoint;
- Return to service of a previously suppressed waypoint;
- Decommissioning of operational equipment;
- Testing in ATC environment;
- Installation of non-ATC equipment in ATC environment;
- …

8.4 Examples of changes deserving a Type1 safety assessment (Step15)

This section proposes examples of changes subject to Type1 safety assessment (See Annex):

1. Maintenance Intervention (excl. Corrective maintenance as being considered as part of the operational envelope);
2. External Supplier Intervention (infringing the Service Level Agreement (SLA));
3. Notification of cross-border technical interventions (multi-sites ...);
4. Transition phases;
5. Replacement of HW by equivalent (non-regression);
6. ATC Operational/Procedural Changes;
7. Connection of Non Operational Sub-Systems onto the Operational System (to demonstrate non-interference)
8. Changing roster scheme;
9. Modification of Configuration Data;
10. Modification of HMI Lay-out (subset);
11. Unanticipated Tactical Change;
12. Easy to demonstrate;
13. Vicinity.

8.5 Examples of changes deserving a Type2 safety assessment (Step13)

This section proposes examples of changes subject to Type2 safety assessment:

- New system (people, procedure, equipment);
- New service;
- Reduced separation minimum to be applied within an airspace or an aerodrome;
- Reorganisation of the ATS route structure;
- Resectorisation of an airspace;
- Airspace class change;
- Physical changes to the layout of the runways and/or taxiways at an aerodrome;
- New type of aircraft (new performance characteristics including aircraft navigation capabilities and navigation performance);
- Inclusion of a new waypoint;
- Suppression of an existing waypoint;
- Return to service of a previously suppressed waypoint;
- Decommissioning of operational equipment;
- …

9 CHANGE ASSESSMENT PROCESS (CAP)

9.1 Change Assessment Process aim

The aim of the Change Assessment Process is to:

- determine if the event that has been considered as a change is affecting the safety of the Air Navigation System /Service (step4 section 6.4, step18 section6.18)

- determine the type of safety assessment to perform (step9 section 6.9 ,step12 section 6.12),

- and to ensure provision of related assurance and evidence (step6 section 6.6 , step10 section 6.10, step13 section 6.13 ,step15 section 6.15, step16 section 6.16, step17 section 6.17, step19 section 6.19, step20 section 6.20)

9.2 Change Assessment Process roles and responsibilities

The following roles and responsibilities should be addressed in the Change Assessment Process:

- Event owner responsible for submitting the event for Change Assessment Process.

- Safety assessor responsible for assessing the safety aspect of the change.

- The management level and organizational area responsible for accepting the event after assessment.

- Operational expert where the operational level is effected, involving engineering expert where the engineering level is effected

Change Assessment Process should describe the circumstances when these roles can be combined or must be independent. Generally the circumstances depend on the safety impact of the change.

As Change Assessment Process participants have to rely on their competence, such responsibility should be part of their job description and more specifically part of their safety responsibilities/accountabilities. Consequently, they should be trained, assessed and maintained competent for such task.

As any other organizational process Change Assessment Process should be surveyed and audited to ensure its application.

9.3 CHANGE ASSESSMENT PROCESS DECISION RECORD TEMPLATE

The following fields should be included in any Change Assessment Process decision record template:

- Change ID;
- Change owner;
- Change description;
- Change Assessment Process decision approved by Ops department
- Safety endorsement of Change Assessment Process decision by;
- Change Assessment Process decision approved / accepted by;
- Occurrence report reference (for unanticipated tactical changes) ;
- Change Assessment Process decision:
    - o “not affecting the ATM system” sustained with rationale (see step6)
    - o Unanticipated tactical change criteria applicability (see step9) see note;

- "not affecting the safety of the ATM system" sustained with rationale(see step19);
- Type of safety assessment supported with rationale (see step12);

- Safety case/assessment reference;

Note: the decision of applying the unanticipated tactical change criteria can be made either by the Change Assessment Process itself (if time allows) or by the OPS staff but anyhow such decision has to be recorded afterwards by Change Assessment Process.

10 TYPES OF SAFETY ASSESSMENT

The Determination Process has described in section 6 identifies the need to conduct either a Type1 or a Type2 safety assessment.

Type1 safety assessment: This safety assessment consists in applying either partially or with some interpretations or restrictions SAM Guidance Material for the whole SAM set of recommendations: safety consideration, safety argument, SAM steps (FHA, PSSA, SSA).

It means that compliance with ESARR4 needs:

- some interpretation of some requirement(s) and an argument for such interpretation or restriction exists;

- or that certain requirements are not complied with and such non-compliance is sustained with a rationale.

The following needs for interpretation or restriction of ESARR4 requirements can be:

- Interpretation of Safety Objective (SO) definition: Only qualitative Safety Objective will be identified (Cf: SES CR 2096/2005 Article 2.k) : Safety Objective: 'safety objective' shall mean a qualitative or quantitative statement that defines the maximum frequency or probability at which a hazard can be expected to occur) because:

  - The effort of trying to quantify SO is not commensurate with the safety benefit that can be expected (e.g. transition phase of few hours: quantifying hazards that can happen during this transition phase will not add any value to the safety assessment as they can occur once or not occur at all. The safety assessment should aim at avoiding them appearing.).

  - The effort of trying to quantify SO is not commensurate with the safety assessment effort as a whole (safety assessment can be easy and quick except if we quantify) (e.g.).

- Top-Down approach including the identification of hazards/SO: The nature of the change is such that failures have to be identified and a bottom-up approach (Cause-Consequence Analysis or Failure Mode and Effects Analysis (FMEA)) is applied to assess the consequences of such failures. The nature of the change is such that it is preferred to wait for the definition, design and implementation completion to initiate the safety assessment (perform the SSA part of SAM). Acceptable failure occurrence rates

are defined but without defining hazard occurrence rate. For such Type1 safety assessment, the notion of hazards will be interpreted as failures. Consequently, Safety Requirements will be allocated to the failures and no hazards and their associated Safety Objective will be specified.

- Risk level acceptability: The nature of the change can lead to a qualitative bottom-up assessment of the contribution of the change to the overall level of ATM risk. It means that the interpretation of ESARR4 5.2.b.iii consists in demonstrating that the final level of risk generated by the hazards associated to this change is acceptable without qualifying via quantitative values. This can be applicable to some specific changes for which it has been agreed between the ANSP and the NSA that such Type1 safety assessment including such restriction/interpretation is accepted (e.g. ATC operational procedural change).

- Comparative assessment: The interpretation of ESARR4 consists in only demonstrating that the change to a legacy system is assessed as having only more stringent Safety Requirements than those of the legacy system before the change and that a demonstration shows that no additional risk is introduced. It assumes that the legacy system was contributing to achieve, at least, a tolerable level of risk.

Type2 Safety assessment: This safety assessment consists in applying SAM Guidance Material for the whole SAM set of recommendations: safety consideration, safety argument, SAM steps (FHA, PSSA, SSA). “Applying” can mean either “apply for the first” or “review and update its previous application”. It means that full compliance with ESARR4 can be achieved without interpretation or restriction of the applicability of certain requirements.

11 HOW TO USE OF THIS GUIDANCE MATERIAL

A customisation of this Guidance Material and its process has to be done to match the organisational aspects of the Air Navigation Service Provider (ANSP).

This customisation has to be included in the ANSP Safety Management Manual.

In particular, the following aspects need the endorsement of the ANSP Senior Management and the National Supervision Authority (NSA):

- Exclusion Criteria (type of changes straight forward not subject to further safety assessment);
- Criteria for unanticipated tactical change or immediate unanticipated tactical change;
- Type1 safety assessment criteria and processes.

This page is intentionally left blank.