European Union Aviation Safety Agency

Notice of Proposed Amendment 2019-04

Additional acceptable means of compliance and guidance material for the safety/safety support assessment of changes to the air traffic management/ air navigation services functional systems

RMT.0719

EXECUTIVE SUMMARY

The objective of this Notice of Proposed Amendment (NPA) is to maintain a high level of safety by providing a set of harmonised measures for the providers of air traffic management (ATM)/air navigation services (ANS) when dealing with the safety/safety support assessment of changes to a functional system. It thus aims to achieve a smooth transition into the new ATM/ANS regulatory framework.

This NPA proposes a set of additional acceptable means of compliance (AMC)/guidance material (GM), which are based on the requirements laid down in the SESAR Safety Reference Material (SRM), as regards the scope of the change, the risk analysis process and the safety criteria determination by the providers of ATM/ANS.

Action area:	Safety management		
Affected rules:	AMC/GM to Commission Implementing Regulation (EU) 2017/373		
Affected stakeholders:	Air navigation service providers (ANSPs); competent authorities		
Driver:	Safety	**Rulemaking group:**	No
Impact assessment:	No	**Rulemaking Procedure:**	Standard

Table of contents

1. About this NPA 3
1.1. How this NPA was developed 3
1.2. How to comment on this NPA 3
1.3. The next steps 3
2. In summary — why and what 4
2.1. Why we need to change the rules — issue/rationale 4
2.2. What we want to achieve — objectives 5
2.3. How we want to achieve it — overview of the proposals 5
2.4. What are the expected benefits and drawbacks of the proposals 7
3. Proposed amendments 8
3.1. Draft acceptable means of compliance and guidance material (Draft EASA decision) 8
4. Proposed actions to support implementation 19
5. References 20
5.1. Related regulations 20
5.2. Affected decisions 20
5.3. Other reference documents 20
6. Appendix 21

1. About this NPA

1.1. How this NPA was developed

The European Union Aviation Safety Agency (EASA) developed this NPA in line with Regulation (EU) 2018/1139[1] (the 'Basic Regulation') and the Rulemaking Procedure[2]. This rulemaking activity is included in the European Plan for Aviation Safety under rulemaking task RMT.0719. The text of this NPA has been developed by EASA with the support of EUROCONTROL. It is hereby submitted to all interested parties[3] for consultation.

1.2. How to comment on this NPA

Please submit your comments using the automated **Comment-Response Tool (CRT)** available at **http://hub.easa.europa.eu/crt/**[4].

The deadline for submission of comments is **11 June 2019**.

1.3. The next steps

Following the closing of the public commenting period, EASA will review all the comments received and will perform a focused consultation, which will consist of one or more thematic review meetings.

Based on the comments received, EASA will develop a decision in order to amend the AMC/GM to Commission Implementing Regulation (EU) 2017/373[5].

The comments received on this NPA and the EASA responses to them will be reflected in a comment-response document (CRD). The CRD will be appended to the decision.

---

1 Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1) (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1535612134845&uri=CELEX:32018R1139).

2 EASA is bound to follow a structured rulemaking process as required by Article 115(1) of Regulation (EU) 2018/1139. Such a process has been adopted by the EASA Management Board (MB) and is referred to as the 'Rulemaking Procedure'. See MB Decision No 18-2015 of 15 December 2015 replacing Decision 01/2012 concerning the procedure to be applied by EASA for the issuing of opinions, certification specifications and guidance material (http://www.easa.europa.eu/the-agency/management-board/decisions/easa-mb-decision-18-2015-rulemaking-procedure).

3 In accordance with Article 115 of Regulation (EU) 2018/1139, and Articles 6(3) and (7) of the Rulemaking Procedure.

4 In case of technical problems, please contact the CRT webmaster (crt@easa.europa.eu).

5 Commission Implementing Regulation (EU) 2017/373 of 1 March 2017 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011, (EU) No 1035/2011 and (EU) 2016/1377 and amending Regulation (EU) No 677/2011 (OJ L 62, 8.3.2017, p. 1) (http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1492589906614&uri=CELEX:32017R0373).

2. In summary — why and what

2.1. Why we need to change the rules — issue/rationale

Commission Implementing Regulation (EU) 2017/373 lays down common requirements for the providers of ATM/ANS and other ATM network functions and their oversight, and sets up a regulatory framework for the safety assessment of changes to functional systems that is performed by the providers of ATM/ANS and other ATM network functions and the oversight of these changes by the competent authorities. In this context, Commission Implementing Regulation (EU) 2017/373 was developed based on EASA Opinions Nos 03/2014 'Requirements for service providers and the oversight thereof'[6] and 02/2015 'Technical requirements and operating procedures for the provision of data to airspace users for the purpose of air navigation'[7] that resulted, among other things, from the consultation of NPA 2014-13 'Assessment of changes to functional systems by service providers in ATM/ANS and the oversight of these changes by competent authorities'[8] (published on 24 June 2014) with the interested parties, including industry, national aviation authorities and social partners.

By enhancing the understanding of the newly introduced concept of 'assessment of changes', it is expected that harmonisation across Europe will also improve.

However, during the preparation period for the implementation of the new Commission Implementing Regulation (EU) 2017/373, EASA was reminded that material already developed by EUROCONTROL (SAM, SAME[9]) or jointly with SESAR JU (SRM) is available for some areas, whereas the AMC/GM material issued with ED Decision 2017/001/R[10] may be amended as regards the scoping of the change, the risk analysis process and the safety criteria determination by the service providers to clarify of the implementing rule requirements and also offer some means of compliance.

The SESAR SRM presents an integrated approach to safety assessment to meet the needs of the SESAR Work Programme. It provides practical guidance on how to perform safety assessments and develop safety assurance for the different life cycle stages up to the pre-industrial stage. In order to properly perform the safety assessments of the SESAR solutions, the SRM details a broader approach to safety assessment in which both the ATM's positive contribution to aviation safety (a success approach) as well as the ATM's negative effect on the risk of an accident (a failure approach) are addressed. The EUROCONTROL SAME, built upon the EUROCONTROL SAM, addresses all the life cycle stages, and in particular the implementation, transfer into operation and operation phases with the same broader approach as defined for the SESAR SRM.

The SESAR SRM and the EUROCONTROL SAM/SAME could complement the existing AMC/GM in the following areas:

— **Scope of the change:** The existing AMC/GM are of generic nature and, in some cases, incomplete (e.g. no reference to degraded modes in the ATS part). Consequently, this NPA propose more detailed guidance for the identification of the scope of changes.

6 https://www.easa.europa.eu/document-library/opinions/opinion-032014

7 https://www.easa.europa.eu/document-library/opinions/opinion-022015

8 https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2014-13

9 See Section 5.3.

10 ED Decision 2017/001/R of 8 March 2017 'AMC/GM to Regulation (EU) 2017/373' (https://www.easa.europa.eu/document-library/agency-decisions/ed-decision-2017001r).

— **Risk analysis process:** Detailed guidance is available in the SRM, with the introduction of the success approach and failure approach. The existing AMC/GM focus on the WHAT (setting up some objectives) but there is no detailed information about the HOW. The current AMC/GM include quite a lot of information about the use of proxies but not about the (classic) risk-based safety assessment.

— **Safety criteria determination:** Detailed guidance is available in the SRM which could complement and detail the existing AMC/GM.

Furthermore, after the closing of the NPA consultation, the aim of EASA is to issue a decision (and the associated CRD) on the additional AMC/GM addressing (at least) the scoping of the change, the risk analysis process and the safety criteria determination by service providers before the applicability date of Commission Implementing Regulation (EU) 2017/373, i.e. 2 January 2020.

In conclusion, it should be highlighted that these additional AMC/GM associated to the safety assessment of changes provide complementary AMC/GM to service providers in order to facilitate their safety/safety support assessment process for any change to the functional system.

2.2. What we want to achieve — objectives

The overall objectives of the EASA system are defined in Article 1 of the Basic Regulation. This proposal will contribute to the achievement of the overall objectives by addressing the issues outlined in Section 2.1.

The specific objective of this proposal is to maintain the level of safety by providing additional AMC/GM for service providers to assess the changes they make to the functional systems. These additional AMC/GM are based on existing safety reference material which has been already applied in particular with the SESAR Work Programme by a variety of stakeholders including several European ANSPs (e.g. DSNA, DFS, NATS, AUSTROCONTROL, ENAIRE, SKYGUIDE) but also ground and airborne industry.

2.3. How we want to achieve it — overview of the proposals

These additional AMC/GM have been developed using the relevant part of the SESAR SRM and the EUROCONTROL SAM/SAME. The proposal for additional AMC/GM is to complement existing AMC/GM for the safety assessment (Part-ATS) for all three areas (i.e. scoping of the change, risk analysis process and safety criteria determination) whereas for the safety support assessment (Part-ATM/ANS.OR) the proposal is to complement existing AMC/GM only for one area which is the scoping of the change.

2.3.1. Proposed amendments to Subpart C 'Specific organisational requirements for service providers other than air traffic services providers' of Annex III 'AMC/GM to Part-ATM/ANS.OR — Common requirements for service providers' to ED Decision 2017/001/R

Two new GM are proposed to ATM/ANS.OR.C.005(a)(1) 'Safety support assessment and assurance of changes to the functional system' in order to address the scope of the change.

— New GM1 ATM/ANS.OR.C.005(a)(1)(i);(ii);(iii);(iv) provides guidance material for non-ATS service providers in order to describe for a change to their functional systems the scoping process to be followed. This GM details what needs to be done at an early stage of the process in order to determine the impact of the change (human, technical and/or procedural) considering the operational environment, and to identify the detailed safety support assessment activities to be undertaken at the different stages of the change's life cycle.

— New GM2 ATM/ANS.OR.C.005(a)(1)(v) provides details for non-ATS service providers about the degraded mode of operation by highlighting the importance to consider any conditions (failure; abnormal conditions, e.g. external event), which could affect compliance with the service requirements.

2.3.2. Proposed amendments to Subpart A 'Additional organisation requirements for providers of air traffic services (ATS.OR)) of Annex IV 'AMC/GM to Part-ATS — Specific requirements for providers of air traffic services (ATS)' to ED Decision 2017/001/R

New AMC/GM are proposed to ATS.OR.205(a)(1) 'Safety assessment and assurance of changes to the functional system' in order to address the scope of the change, the risk analysis process and the safety criteria determination. Provisions similar to the ones mentioned in Section 2.3.1 have been developed for ATS providers for the scope of the change, and additional AMC/GM have been proposed for the risk analysis process and the safety criteria determination.

— New GM1 ATS.OR.205(a)(1)(i);(ii);(iii);(iv) provides guidance material for ATS service providers in order to describe for a change to their functional systems the scoping process to be followed. This GM details what needs to be done at an early stage of the process in order to determine the safety impact of the change (human, technical and/or procedural) considering the operational environment, and to identify the detailed safety assessment activities to be undertaken at the different stages of the change's life cycle.

— New GM1 ATS.OR.205(a)(1)(v) provides details for ATS service providers about the degraded mode of operation by highlighting the importance to consider any conditions (failure; abnormal conditions, e.g. external event), which could affect the safety of the service and potentially lead to a reduced level of operational service.

— New GM1 ATS.OR.205(b)(3) describes the risk analysis process based on the broader safety approach that includes, further to the traditional failure approach, the success approach (effectiveness of the changed functional system when working as intended). In order to support this broader safety approach, integrated risk models per type of accident are introduced as one of the ways to facilitate the determination of the impact of a change, to assess the effects of hazards at operational level, and to determine the potential contribution of these hazards to an accident.

— New AMC3 ATS.OR.205(b)(4) and associated two new GM to that AMC3 are proposed to provide the means of compliance and associated guidance for the risk evaluation and mitigation process to be applied during the different life cycle stage(s) of the change (from the operational specification to the operation) including the degraded mode of operation. The risk evaluation and mitigation process as proposed will provide evidence that risk is sufficiently mitigated by allocating safety requirements to the different elements of the functional system that is affected by the change (equipment, human, and procedures) in order to meet the applicable safety criteria.

— New AMC1 ATS.OR.210(b) is proposed with three associated GM to that AMC1. The purpose is to provide the means of compliance and associated guidance for the safety criteria determination based on the integrated risk model. Safety criteria in such case could be either a quantitative level of safety risk or a proxy. The first GM describes the different steps for the safety criteria determination and the importance of the scope of the change in that process. The second GM provides details on the safety criteria determination based on the integrated risk model, and the third GM gives an example of safety criteria determination supported by the integrated risk model.

2.4. What are the expected benefits and drawbacks of the proposals

When transposing the relevant part of the SESAR SRM and the EUROCONTROL SAM/SAME in order to establish new AMC/GM to be considered by service providers when conducting safety (support) assessments, only the necessary adjustments have been made by associating the requirements with the rules laid down in Commission Implementing Regulation (EU) 2017/373 without detriment to the principles preserved.

In this context, the benefit expected from this proposal is that the service providers can implement these new AMC/GM for the safety assessment of their changes to better scope the change, to assess the safety risk of a change in a broader way, and to determine in a complete and comprehensive manner the safety criteria for the change.

For this reason, no impact assessment (IA) has been developed for this rulemaking task. Moreover, in this context, EASA has already performed an IA for a number of key regulatory developments with the publication of NPA 2014-13 'Assessment of changes to functional systems by service providers in ATM/ANS and the oversight of these changes by competent authorities', addressing, among other things, the changes to the functional system in general, including the scoping of the change, the risk analysis process and the safety criteria determination.

3. Proposed amendments

The text of the amendment is arranged to show deleted text, new or amended text as shown below:

— deleted text is ~~struck through~~;

— new or amended text is highlighted in grey;

— an ellipsis '[…]' indicates that the rest of the text is unchanged.

3.1. Draft acceptable means of compliance and guidance material (Draft EASA decision)

ANNEX III

COMMON REQUIREMENTS FOR SERVICE PROVIDERS

(PART-ATM/ANS.OR)

[…]

SUBPART C — SPECIFIC ORGANISATIONAL REQUIREMENTS FOR SERVICE PROVIDERS OTHER THAN AIR TRAFFIC SERVICES PROVIDERS

[…]

GM1 ATM/ANS.OR.C.005(a)(1)(i);(ii);(iii);(iv) Safety support assessment and assurance of changes to the functional system

SCOPING

(a) Scoping is the initial identification of the scope of the change accompanied by the initial assessment of the service impact resulting from the change in order to specify the detailed safety support assessment activities to be undertaken. This preparatory process identifies the elements that are affected by the change and consequently need to be considered by the safety support assessment and the main service issues associated with the proposed change.

(b) Scoping should address the extent, boundaries and interfaces of the functional system being considered, encompassing affected parts of other service providers and/or aviation undertakings and underlying functional systems, its intended functions as well as the context (operational environment) in which the change is intended to operate.

(c) The scoping is performed considering the following:

(1) The baseline for the change assessment which should be carefully determined in terms of:

(i) the context (operational environment) before the implementation of the change;

(ii) the functional systems and operations before the implementation of the change;

(iii) the applicable regulatory framework and existing industry standards.

(2) The modified context (operational environment) in which the change is intended to operate, if that is a prerequisite to the change. The properties of the context (operational environment) are crucial to a safety support assessment — specifically, a safety support

assessment that is valid for one context may not be valid for a different context. Thus, in order to be correct and complete, a safety support assessment has to be specific to a clearly defined context (operational environment).

(3) The details of the change with respect to the baseline situation (whilst considering GM1 ATS.OR.205(a)(1)(iii) 'Interactions' and GM2 ATS.OR.205(a)(1) 'Scope of the change' regarding interactions within the changed functional system and within the changing functional system, the changed elements and directly or indirectly affected elements), including:

(i) human actors' roles and responsibilities;

(ii) operating methods (procedures), tasks, practices, change in human-performance-related transition factors (staffing, competence, acceptance, and job satisfaction);

(iii) technical systems (architecture, functionalities, and performance);

(iv) human and technical systems: allocation of tasks (man–machine) and new or modified human–machine interface (HMI).

(d) The result of the scoping should determine the detailed set of activities to be undertaken at each stage of the life cycle of the change:

(1) operational specification,

(2) design,

(3) implementation,

(4) transfer into operation,

(5) operation.

(e) The outcome of the initial scoping assessment should be updated and refined if new aspects are revealed as the safety support assessment progresses (e.g. identification of the additional elements' behaviour that are affected by the changed elements or identification of additional new interactions introduced by the changed or directly affected elements).

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

DEGRADED MODE

(a) Degraded mode of operation is a reduced level of operational service invoked by abnormal conditions, equipment outage or malfunction, or staff shortage.

Certain functional system failures might not impact on the normal operations because of the nature of the failure and because the system/service architecture is fault-tolerant to such failures.

Certain functional system failures might result in service delivery malfunction without leading to a degraded mode of operation because they involve only a partial and/or transient operational effect (e.g. the degraded condition is of short duration).

(b) Abnormal conditions are those external changes in the context (operational environment) that the functional system may exceptionally encounter (e.g. severe weather conditions, ionosphere,

interferences, supplier or utility failure, etc.) under which the functional system may be allowed to enter a degraded state provided that it can easily be recovered when the abnormal condition passes and the risk during the period of the degraded state is shown to be tolerable.

ANNEX IV

SPECIFIC REQUIREMENTS FOR PROVIDERS OF AIR TRAFFIC SERVICES (ATS)

(PART-ATS)

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

[…]

Section 2 — Safety of services

[…]

GM1 ATS.OR.205(a)(1)(i);(ii);(iii);(iv) Safety assessment and assurance of changes to the functional system

SCOPING

(a) Scoping is the initial identification of the scope of the change accompanied by the initial assessment of the safety implications of the change which should be conducted to specify the detailed safety assessment activities to be undertaken. This preparatory process identifies the elements that are affected by the change and consequently need to be considered by the safety assessment, the main safety issues associated with the proposed change, the criteria for deciding what is 'safe' and helps to decide the extent to which the safety assessment has to be conducted.

(b) The scoping should address:

(1) the extent, boundaries and interfaces of the functional system being considered, encompassing affected parts of other service providers and/or aviation undertakings and underlying functional systems, its intended functions as well as the context (operational environment) in which the change is intended to operate;

(2) what the change is intended to achieve and with what safety relevance: to either deliver a safety benefit or deliver benefits other than safety (e.g. in capacity, efficiency, business, environmental impact). In the latter case, it should be defined what is expected from the safety perspective (i.e. maintain the current level of safety or accept a capped degradation as a counterpart to the other expected benefits).

(c) The scoping is performed considering the following:

(1) The baseline for the change assessment which should be carefully determined in terms of:

(i) the context (operational environment) before the implementation of the change;

(ii) the ATM/ANS services and underlying functional systems and operations before the implementation of the change;

(iii) the applicable regulatory framework and existing industry standards;

(2) The modified context (operational environment) in which the change is intended to operate, if that is a prerequisite to the change. The properties of the context (operational environment) are crucial to a safety assessment — specifically, a safety assessment that is valid for one context may not be valid for a different context. Thus, in order to be correct and complete, a safety assessment has to be specific to a clearly defined context (operational environment).

(3) The details of the change with respect to the baseline situation (whilst considering GM1 ATS.OR.205(a)(1)(iii) 'Interactions' and GM2 ATS.OR.205(a)(1) 'Scope of the change' regarding interactions within the changed functional system and within the changing functional system, the changed elements and directly or indirectly affected elements), including:

(i) human actors' roles and responsibilities;

(ii) operating methods (procedures), tasks, practices, change in teams and communication (e.g. task redistribution within the planner–executive controllers' team), change in human-performance-related transition factors (staffing, competence, acceptance, and job satisfaction);

(iii) technical systems (architecture, functionalities, and performance);

(iv) human and technical systems: allocation of tasks (man–machine) and new or modified human-machine interface (HMI).

(d) The result of the scoping should determine the detailed set of activities to be undertaken at each stage of the life cycle of the change:

(1) operational specification,

(2) design,

(3) implementation,

(4) transfer into operation,

(5) operation.

(e) The outcome of the initial scoping assessment should be updated and refined if new aspects are revealed as the safety assessment progresses (e.g. identification of the additional elements' behaviour affected by the changed elements or identification of additional new interactions introduced by the changed or directly affected elements).

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

DEGRADED MODE

(a) Degraded mode of operation is a reduced level of operational service invoked by abnormal conditions, equipment outage or malfunction, or staff shortage.

Certain functional system failures might not impact on the normal operations because of the nature of the failure and because the ATS system/service architecture is fault-tolerant to such failures.

Certain functional system failures might result in an operational hazard without leading to a degraded mode of operation because they involve only a partial and/or transient operational effect (e.g. one or few aircraft are affected, or the degraded condition is of short duration).

(b) Abnormal conditions are those external changes in the context (operational environment) that the functional system may exceptionally encounter (e.g. severe weather conditions, airport closure, supplier or utility failure) under which the functional system may be allowed to enter a degraded state provided that it can easily be recovered when the abnormal condition passes and the risk during the period of the degraded state is shown to be tolerable.

GM1 ATS.OR.205(b)(3) Safety assessment and assurance of changes to the functional system

RISK ANALYSIS

(a) The risk analysis (i.e. analysis of the risks posed by the introduction of the change) should be conducted considering safety from two perspectives:

(1) A success approach assessing the effectiveness of the changed functional system when working as intended — i.e. how much the risks inherent to aviation (point (b) of AMC2 ATS.OR.205(b)(1)) will be reduced by the changed functional system. The success approach is concerned with the contribution to aviation safety a functional system makes in the absence of failure.

(2) A failure approach assessing the risks generated by the malfunction of the changed functional system. The failure approach is concerned with the negative contribution to aviation safety a functional system might make in the event of failure(s). Note that applying only the failure approach (i.e. avoiding to conduct the success approach) might result in a changed functional system which is reliable but which might not sufficiently mitigate the aviation risks.

(b) Conducting the risk analysis from a combined success and failure perspective should be supported by integrated risk models. The integrated risk models should:

(1) describe how the risks of aviation accidents are mitigated by service providers and aviation undertakings, providing a structured breakdown of the positive and negative contributions to the risk mitigation (positive contribution to the effectiveness of the mitigation and negative contribution in terms of reducing that effectiveness through failures). These mitigation measures are considered at the service level, i.e. at the level of the operational services provided to airspace users. A dedicated integrated risk model should be defined for each type of aviation accident with the service providers' contribution (mid-air collision, runway collision, controlled flight into terrain (CFIT), etc.);

(2) describe how service providers and aviation undertakings could induce situations that contribute to the risks of aviation accidents (e.g. conflicting situation that might lead to a safety-relevant incident or accident), providing a structured breakdown of the main causes of such induced risks;

(3) model how an aviation accident is prevented from occurring through an inductive logic that considers the next mitigation available for protecting against the propagation of the effects of an induced risk or of another mitigation that has previously failed. In the model, the accident precursors may be represented by the occurrence of induced risks or by the immediate outcome of the failure of the mitigations.

(c) The risk analysis supported by the integrated risk models should:

(1) facilitate the determination of the impact of the change on the safety of aircraft operations and therefore facilitate the risk analysis of the effects related to the change;

(2) assess the effects of hazards, provided the hazards have been previously identified (as per GM1 ATS.OR.205(b)(1)) and further consolidated at the operational level — i.e. at the level

they are perceived by the airspace users (level consistent with the mitigations and induced risks that structure the integrated risk model);

(3) enable the characterisation of hazards consolidated at the operational level in terms of level of the accident probability given that the hazard has occurred, considering the remaining mitigations. Such characterisation of hazards based on an integrated risk model has the advantage of providing clear rules shared by multiple actors.

AMC3 ATS.OR.205(b)(4) Safety assessment and assurance of changes to the functional system

RISK EVALUATION AND MITIGATION

(a) The risk evaluation and mitigation process should provide evidence that the risk is sufficiently mitigated by allocating safety requirements to the different elements of the functional system that is affected by the change (equipment, human, and procedures) in order to meet the applicable safety criteria.

(b) The risk evaluation and mitigation process should be considered to be complete when all the stages of the life cycle of the change have been assessed and safety requirements have been identified to sufficiently mitigate the risk that arises from any hazard introduced by the change or already existing hazards affected by the change as identified in AMC2.ATS.OR.205(b)(1).

(c) The risk evaluation and mitigation process should cover all the life cycle stage(s) of the change:

— operational specification,

— design,

— implementation,

— transfer into operation,

— operation.

GM1 to AMC3 ATS.OR.205(b)(4) Safety assessment and assurance of changes to the functional system

RISK EVALUATION AND MITIGATION

(a) The risk evaluation and mitigation process at operational specification level should:

(1) be limited to the desired safety behaviour of the change at its interface with the context (operational environment) and therefore does not consider the design characteristics/items of the functional system;

(2) cover but not go beyond the scope of the change (to the extent of the scoping information available at this life cycle stage), ensuring that all operational use cases within that scope are considered;

(3) focus on the safety-relevant aspects of the change, aspects which might be identified through the hazard identification (both hazards inherent to aviation and hazards generated by the ATM/ANS functional system malfunction as per GM1 ATS.OR.205(b)(1)) and the initial risk analysis (which might be supported by an integrated risk model at this life cycle stage — see GM1 ATS.OR.205(b)(3));

(4) determine the highest layer of safety requirements that are necessary in order to satisfy the safety criteria, by making use of the initial risk analysis outcomes (GM1 ATS.OR.205(b)(3)) to achieve the following:

(i) capture what has to happen in order for the operational services to operate in the defined context (operational environment) in order to mitigate the hazards inherent to aviation identified in point (3) above. The resulting highest layer of safety requirements will express functional or performance properties of the operational services;

(ii) mitigate the consequences of failure/degradation of the operational services caused by the hazards generated by the changed functional system as per point (3) above. The resulting highest layer of safety requirements will express functional or performance properties of the operational services;

(iii) define the acceptable frequency of occurrence of such failure/degradation of the operational services in order to achieve a tolerable level for the associated system-generated risk derived from the hazards generated by the changed functional system, taking account of the above mitigations.

(iv) mitigate the consequences of failure/degradation of the operational services resulting from the occurrence of abnormal conditions by deriving additional highest layer of safety requirements.

(b) The risk evaluation and mitigation process at design level should:

(1) consider that design safety requirements are the necessary risk-reduction measures identified in the risk assessment to achieve the highest layer of safety requirements defined at operational level. They describe:

(i) the functional, non-functional and performance safety properties (e.g. continuity, integrity, reliability, availability) at the system design level;

(ii) human and procedural aspects (HMI, procedures, training, competence, etc.);

(iii) other organisational or operational requirements;

(2) derive the safety requirements considering all foreseeable conditions (normal, abnormal and failure conditions) that the functional system might encounter;

(3) derive in the success approach the design safety requirements on the functional system elements impacted by the change (equipment, procedures, human elements) for normal and abnormal conditions considering the architecture's structure and behaviour;

(4) derive in the failure approach the design safety requirements by performing the causal analysis of the hazards generated by the changed functional system, with due consideration of all reasonably foreseeable sources of common cause or other dependent failures;

(5) ensure that the design has no negative effect on the operation of related ground-based and airborne safety nets and, more generally, that it does not introduce dependencies leading to new common cause failures — otherwise revisit the risk evaluation and mitigation;

(6) ensure that the design safety requirements are capable of being satisfied in the implementation and that their satisfaction can be demonstrated with the appropriate degree of confidence.

(c) The risk evaluation and mitigation process at implementation level should:

(1) ensure that all the design safety requirements are met by the elements of the implemented change (e.g. check that a specific training-related safety requirement is satisfied by the proposed training manual, courses and simulations);

(2) check the validity of the assumptions on which the safety requirements were based along the risk analysis, evaluation and mitigation processes, and adjust the risk evaluation and mitigation if necessary;

(3) check for any deviation of the implemented functional system from the design safety requirements and for the potential safety effect of any emergent property revealed during implementation. Operational limitations or changes to the elements of the functional system might be used to mitigate the residual risk;

(4) include assurance that any detected safety-relevant deficiencies have been resolved.

(d) The risk evaluation and mitigation process related to transfer into operation should:

(1) determine that the transfer into operation (site installation, shadow operation, switch to operation, etc.) of the functional system ready to be brought into operational use will not affect the continuity and safety of the ongoing service;

(2) identify any specific safety requirements needed to reduce the risk as far as reasonably practicable during the transition to the new functional system, based on the risk analysis of the transfer-into-operation processes (e.g. temporary operational limitation, progressive climb to nominal regime).

(e) The risk evaluation and mitigation process during operation should identify any specific safety-relevant performance indicators to be monitored by the ATM/ANS provider's performance monitoring (ATM/ANS.OR.B.005(d)).

GM2 to AMC3 ATS.OR.205(b)(4) Safety assessment and assurance of changes to the functional system

RISK EVALUATION AND MITIGATION FOR PLANNED DEGRADED MODES

(a) Both the safety risk associated to the immediate operational impact of the event that has triggered the degraded mode (i.e. failure/malfunction of the functional system, and potentially the sudden occurrence of the abnormal condition) and the safety risk associated to the temporary operation in the degraded mode should be sufficiently mitigated. Mitigations of the safety risk associated to the transition to and the operation in the degraded mode encompass the fallback mechanisms, the service continuity strategy, and the recovery back to normal operation.

(b) The risk during the period of the degraded mode should be shown to be acceptable regarding the safety criteria (as per ATS.OR.210) within the given context (operational environment).

(c) ATS contingency measures may be defined in order to cover the degraded modes of operation (encompassing emergency modes) that are new or modified by the change and, ultimately, ensuring service continuity.

[…]

AMC1 ATS.OR.210(b) Safety criteria

QUANTITATIVE LEVEL OF SAFETY RISK

The accident precursors within the integrated risk model should be used to define safety criteria in terms of explicit, quantitative level of the safety risk.

AMC~~1~~2 ATS.OR.210(~~a~~b) Safety criteria
OTHER MEASURES RELATED TO SAFETY RISKS
[…]

AMC~~2~~3 ATS.OR.210(~~a~~b) Safety criteria
OTHER MEASURES RELATED TO SAFETY RISKS — PROXIES
[…]

GM1 ATS.OR.210(~~a~~b) Safety criteria
SAFETY CRITERIA IN TERMS OF PROXIES FOR SAFETY RISKS
[…]

GM1 to AMC1 ATS.OR.210(b) Safety criteria

QUANTITATIVE LEVEL OF SAFETY RISK

(a) The criteria for deciding what is 'safe' in the context of the change should consider the scope of the change as performed in accordance with ATS.OR.205(a)(1).

(b) Safety criteria in terms of explicit, quantitative level of the safety risk might be determined with the support of integrated risk models. Integrated risk models are defined in GM1 ATS.OR.205(b)(3)(b). The integrated risk models to be considered should include all the accident types relevant for the change. The safety criteria should be defined via the following steps:

(1) Determination of those mitigations and induced risks considered at the service level, which are impacted by the change in a positive or negative way.

(2) Identification of the evolution of the accident precursors' occurrence expected with the change, potentially in correlation with the traffic level variation that accompanies the change.

(3) Safety criteria as an explicit, quantitative level of the safety risk will be defined by the accident precursors' occurrence affected by the change combined as necessary with other accident precursors' occurrence modification necessary to ensure the acceptable accident risk.

(4) In those cases where the accident precursors are not easily measurable, proxies defined as contributors to accident precursors can be used as alternative safety criteria.

(5) Update of the safety criteria in case new aspects are revealed as the safety assessment progresses (e.g. new hazards identified).

GM2 to AMC1 ATS.OR.210(b) Safety criteria

QUANTITATIVE LEVEL OF SAFETY RISK

(a) Safety criteria determined from integrated risk models allow to ensure they are justified for the specific change due to the structured identification of the mitigations and induced risks that are impacted by the change.

(b) The use of the integrated risk models allows to specify the acceptable evolution of the safety level for the operations with the functional system after the change (either maintained, increased, or controlled reduction), in relative or absolute terms.

(c) The resulting safety criteria can support the definition of monitoring criteria (see AMC1.ATS.OR.205(b)(6)) as the mitigations and induced risks are considered at the service level

and the occurrences where the mitigations fail or the risks are induced could be observed/measured.

(d) The use of the integrated risk model enables to predict the expected evolution of the accident risk based on the specified or measured occurrence of the mitigation failures and induced risks expected after the change.

(e) When taken collectively across all the integrated risk models for the accident types relevant for the change, and across all the mitigations and induced risks impacted by the change, they enable the complete coverage of the risk acceptability of the change.

GM3 to AMC1 ATS.OR.210(b) Safety criteria

QUANTITATIVE LEVEL OF SAFETY RISK — EXAMPLE

This GM provides an example to illustrate the use of an integrated risk model for the determination of safety criteria.

(a) A runway safety net is to be introduced at an aerodrome where a significant number of runway incursions have occurred. This change is expected to bring a safety improvement which needs to be specified via a safety criterion.

(b) On the ATC side, one contributor to runway incursions is when the air traffic controller momentarily forgets something, e.g. an aircraft on the runway, the closure of a runway, a vehicle on the runway, or a clearance that had been issued. The consequence of forgetting something at the air traffic controller level could lead to clear an aircraft or a vehicle to cross/enter the runway when the runway is occupied. This is called a 'conflicting ATC clearances situation'.

In this simplified example, a safety net is proposed to be introduced in the form of an ATC tool that supports the ATCO at the TWR in detecting conflicting clearances, e.g. 'Clear to Land' versus 'Clear to Line-Up' on the same runway in order to prevent incursions involving aircraft/vehicles on runways. The automatic detection of conflicting ATC clearances will be performed based on the knowledge of the clearances given to aircraft and vehicles (to be input by the air traffic controller via the electronic flight strip).

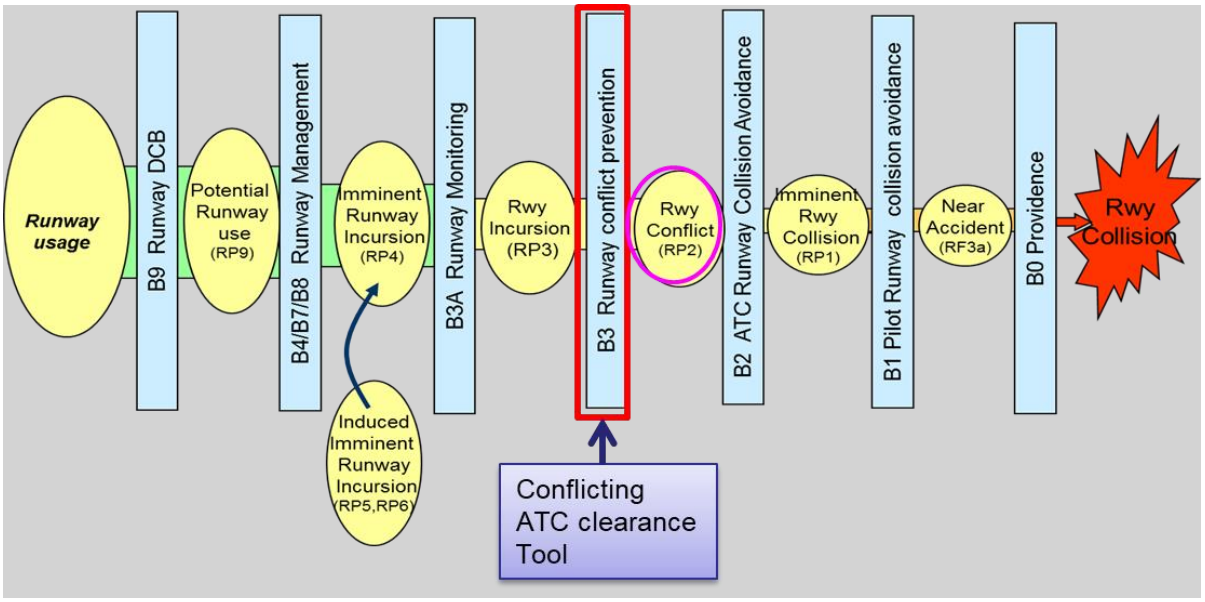
(c) In order to determine the relevant integrated risk model(s) to be used for the safety criteria determination, the risks inherent to aviation that are pre-existing in the context (operational environment) before any form of ATM/ANS planning or deconfliction has taken place shall be identified. Considering the purpose of this safety net, the two following risks inherent to aviation are relevant:

— situation where the intended trajectory of two aircraft is in conflict on the runway;

— situation where the intended trajectory of one aircraft and a vehicle is in conflict on the runway.

The relevant integrated risk model addressing these two above-mentioned risks is the one that addresses the runway collision.

(d) The safety criteria are identified by assessing the impact of this safety net on this integrated risk model. In this example, and as illustrated in the figure below, this safety net provides an early detection of a runway conflict that arises from a conflicting ATC clearance and, therefore, improves the performance of the 'runway conflict prevention' mitigation (safety barrier). The expected effect is a reduction of the frequency of runway conflicts, which represent the accident precursor at the output of this safety barrier, provided the traffic level does not increase.



By analysis it is ensured that this change does not affect other mitigations (safety barriers) or induced risks (e.g. the accident precursor RP5, RP6: induced imminent runway incursion).

The safety criteria are set qualitatively by stating that the number of runway conflicts will be reduced with this tower runway controller safety tool.

In order to derive quantitative safety criteria, additional inputs are necessary like statistics on runway incursions causes. Based on this information, it could be assumed that a reduction of 5 % in the number of runway conflicts could be foreseen.

Indeed, from these statistics it could be determined that 23 % of the runway incursions are due to ATCO operational error (OE), and of this percentage, 22 % corresponds to a situation where a 'controller forgot something', which is a relevant case for the conflicting ATC clearances situation.

From the above analysis, it means that 5 % (23 % × 22 %) of the runway conflicts are potentially due to conflicting ATC clearances.

The quantitative safety criteria for this tower runway controller safety tool should be therefore the following: 'The frequency of runway conflicts (RP 2) shall be reduced by 5 % when ATC is supported by the conflicting ATC clearance tool.'

4. Proposed actions to support implementation

— Dedicated thematic workshop(s)/session(s) with the participation of both industry (including ATM/ANS providers) and competent authorities' representatives.

— Series of thematic events organised on the regional principle with the participation of both industry (including ATM/ANS providers) and competent authorities' representatives.

5. References

5.1. Related regulations

— Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1)

— Commission Implementing Regulation (EU) No 1034/2011 of 17 October 2011 on safety oversight in air traffic management and air navigation services and amending Regulation (EU) No 691/2010 (OJ L 271, 18.10.2011, p. 15)

— Commission Implementing Regulation (EU) No 1035/2011 of 17 October 2011 laying down common requirements for the provision of air navigation services and amending Regulations (EC) No 482/2008 and (EU) No 691/2010 (OJ L 271, 18.10.2011, p. 23)

— Regulation (EC) No 550/2004 of the European Parliament and of the Council of 10 March 2004 on the provision of air navigation services in the single European sky (the service provision Regulation) (OJ L 96, 31.3.2004, p. 10)

— Commission Implementing Regulation (EU) 2017/373 of 1 March 2017 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011, (EU) No 1035/2011 and (EU) 2016/1377 and amending Regulation (EU) No 677/2011 (OJ L 62, 8.3.2017, p. 1)

5.2. Affected decisions

— Executive Director Decision 2017/001/R of 8 March 2017 issuing Acceptable Means of Compliance and Guidance Material to Commission Implementing Regulation (EU) 2017/373 — 'Common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight'

5.3. Other reference documents

— SESAR Safety Reference Material Ed. 4.0 - March 2016 and its associated Guidance Ed. 3.0- May 2016

— EUROCONTROL SAME "Safety Assessment Made Easier" Part 1 Ed. 1.0 – January 2010 and Part 2 Ed. 0.7- July 2010

— EUROCONTROL, 2006, Air Navigation System Safety Assessment Methodology (SAM), SAF.ET1.ST03.1000-MAN-01, Edition 2.1

6. Appendix

Not applicable