EU 2017/373 NPA

CANSO workshop in Brussels

18th January 2019

Bruno RABILLER, Nicolas FOTA, Marta LLOBET
EUROCONTROL

Notice of Proposed Amendment

The proposed GM/AMC are based on safety methodology Safety Reference Material (SRM) and the use of Integrated Risk Models supporting this methodology

They complement the existing GM/AMC in the following areas:

1. **Scope of the Change**
2. **Risk analysis process**
   - introduction of the success approach and failure approach.
   - includes information about risk-based safety assessment.
3. **Safety Criteria determination**

Proposal done in Q3 of 2018. Consultation will take place in 2019 (Q1)

Notice of Proposed Amendment

ANNEX III

COMMON REQUIREMENTS FOR SERVICE PROVIDERS

(Part-ATM/ANS.OR)

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

SUBPART B — MANAGEMENT (ATM/ANS.OR.B)

SUBPART C — SPECIFIC ORGANISATION REQUIREMENTS FOR SERVICE PROVIDERS OTHER THAN ATS PROVIDERS (ATM/ANS.OR.C)

SUBPART D — SPECIFIC ORGANISATIONAL REQUIREMENTS FOR ANS AND ATFM PROVIDERS AND THE NETWORK MANAGER (ATM/ANS.OR.D)

1. Scope of the Change

ANNEX IV

SPECIFIC REQUIREMENTS FOR PROVIDERS OF AIR TRAFFIC SERVICES

(Part-ATS)

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

SECTION 2 — SAFETY OF SERVICES

2. Risk Analysis Process

3. Safety Criteria determination

NPA : 1.Scope of the Change

ANNEX III

SUBPART C — SPECIFIC ORGANISATION REQUIREMENTS FOR SERVICE PROVIDERS OTHER THAN ATS PROVIDERS (ATM/ANS.OR.C)

ATM/ANS.OR.C.005 Safety support assessment and assurance of changes to the functional system

(a) For any change notified in accordance with point ATM/ANS.OR.A.045(a)(1), the service provider other than the air traffic services provider shall:

(1) ensure that a safety support assessment is carried out covering the scope of the change which is:

(i) the equipment, procedural and human elements being changed;

(ii) interfaces and interactions between the elements being changed and the remainder of the functional system;

(iii) interfaces and interactions between the elements being changed and the context in which it is intended to operate;

(iv) the life cycle of the change from definition to operations including transition into service;

(v) planned degraded modes;

GM1 – Scoping: 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 **current and future operational environment and functional system,** the '**multi-actors'** concerned and to identify the **detailed safety activities** to be conducted at the different stages of the change lifecycle..

GM1 – Degraded Mode: Provides details to non-ATS service provider about the **degraded mode** of operation by highlighting the importance to consider any conditions (**equipment malfunction**, **staff shortfall**, **abnormal conditions** e.g. external event,…) which could affect the performance of the functional system and lead therefore to a reduced level of operational service

NPA : 1.Scope of the Change

ANNEX IV

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

SECTION 2 — SAFETY OF SERVICES

ATS.OR.205 Safety assessment and assurance of changes to the functional system

(a) For any change notified in accordance with point ATM/ANS.OR.A.045(a)(1), the air traffic services provider shall:

(1) ensure that a safety assessment is carried out covering the scope of the change, which is:

(i) the equipment, procedural and human elements being changed;

(ii) interfaces and interactions between the elements being changed and the remainder of the functional system;

(iii) interfaces and interactions between the elements being changed and the context in which it is intended to operate;

(iv) the life cycle of the change from definition to operations including transition into service;

(v) planned degraded modes of operation of the functional system; and

GM1 – Scoping: 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 **current and future operational environment and functional system,** the '**multi-actors'** concerned and to identify the **detailed safety activities** to be conducted at the different stages of the change lifecycle.

GM1 – Degraded Mode: Provides details to ATS service provider about the **degraded mode** of operation by highlighting the importance to consider any conditions (**equipment malfunction**, **staff shortfall**, **abnormal conditions** e.g. external event,…) which could affect the performance of the functional system and lead therefore to a reduced level of operational service

NPA : 2.Risk Analysis Process

ANNEX IV

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

SECTION 2 — SAFETY OF SERVICES

ATS.OR.205 Safety assessment and assurance of changes to the functional system

(b) An air traffic services provider shall ensure that the safety assessment referred to in point (a) comprises:

(3) the risk analysis of the effects related to the change;

GM1 – Risk Analysis: describes the risk analysis process based on the safety broader approach which includes in addition to the traditional **failure approach** the **success approach**. In order to support this broader approach, **integrated risk models per type of accident** are introduced to facilitate the **determination of the impact of a change**, to **assess the effects of hazards** at operational level and to **determine the distance** of these hazards **to an accident**.

NPA : 2.Risk Analysis Process

ANNEX IV

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

SECTION 2 — SAFETY OF SERVICES

ATS.OR.205 Safety assessment and assurance of changes to the functional system

(b) An air traffic services provider shall ensure that the safety assessment referred to in point (a) comprises:

(4) the risk evaluation and, if required, risk mitigation for the change such that it can meet the applicable safety criteria;

AMC3 – Risk Evaluation and Mitigation: It provides the means of compliance for the risk evaluation and mitigation process to be applied during the **different lifecycle phases** 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 (induced by the change or already existing) by **allocating safety requirements** to the different elements of the functional system affected by the change (**equipment, human and procedure**) in order to **meet the applicable safety criteria**.

GM1 – Risk Evaluation and Mitigation: provides guidances for the risk evaluation and mitigation process in terms of **scope** and guidance for the process at different lifecycle phases: the **initial risk analysis** - which might be supported by an **integrated risk model** (to determine **highest layer of safety requirements**), the process at **design** level (to determine **design safety requirements**), at **implementation** level, related to **transfer into operations**, and related to **operations and maintenance.**

GM2 – Risk Evaluation and Mitigation for planned degraded modes: provides guidance on how to address **degraded modes** in the risk evaluation and mitigation process

NPA : 3.Safety Criteria determination

ANNEX IV

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

SECTION 2 — SAFETY OF SERVICES

ATS.OR.210 Safety criteria

(b) The safety acceptability of a change shall be assessed by using specific and verifiable safety criteria, where each criterion is expressed in terms of an explicit, quantitative level of safety risk or another measure that relates to safety risk.

AMC1 – General: provides the means of compliance for the safety criteria determination based on the **integrated risk model** (at **accident precursor** level). Safety criteria in such case could be either a quantitative level of safety risk or a proxy.

GM1 – General: describes the different steps for the safety criteria determination, with the support of **integrated risk models** (considering **all type** of relevant accidents, taking into account **traffic variations**, using **contributors** to accident precursors for proxies as alternative, …), and the importance of the **scope** of the change in that process.

GM2 – Safety Criteria Based on integrated risk models: provides **details** on the safety criteria determination based on the **integrated risk model** (suitability, relative or absolute approach, being measurable, centralized management of SACs)

GM3 – Safety Criteria Based on integrated risk models - Example: provides an **example** of safety criteria determination supported by the **integrated risk model** (airport safety nets concept).

« Terminology »

« NPA proposal » terminology		« SRM » terminology
“determine the distance to an accident”	➡	Relates to ‘Severity’ as per the SRM
“highest layer of safety requirements”	➡	Relates to ‘Safety Objectives’ as per the SRM
“integrated risk models”	➡	Barriers models as AIM/IRiS
“risk mitigation in integrated risk models”	➡	Related to Barriers in AIM / IRiS models
“induced risk in integrated risk models”	➡	Related to Induced Events precursors in AIM / IRiS models
“accident precursors in integrated risk models”	➡	Related to Precursors in AIM / IRiS models