European Aviation Safety Agency

Notice of Proposed Amendment 2017-10

Software assurance level requirements for safety assessment of changes to air traffic management/air navigation services functional systems

RMT.0469

EXECUTIVE SUMMARY

The objective of this NPA is to maintain a high level of safety by providing a set of harmonised software assurance level (SWAL) measures for providers of air traffic management (ATM)/air navigation services (ANS) and other ATM network functions when dealing with the (safety) assessment of changes to a functional system. It thus aims at achieving a smooth transition into the new ATM/ANS regulatory framework.

This NPA proposes a set of acceptable means of compliance (AMC)/guidance material (GM) for the definition and implementation of a software (safety) assurance system by providers of ATM/ANS and other ATM network functions that is based on the requirements laid down in Regulation (EC) No 482/2008, which is repealed by Regulation (EU) 2017/373.

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

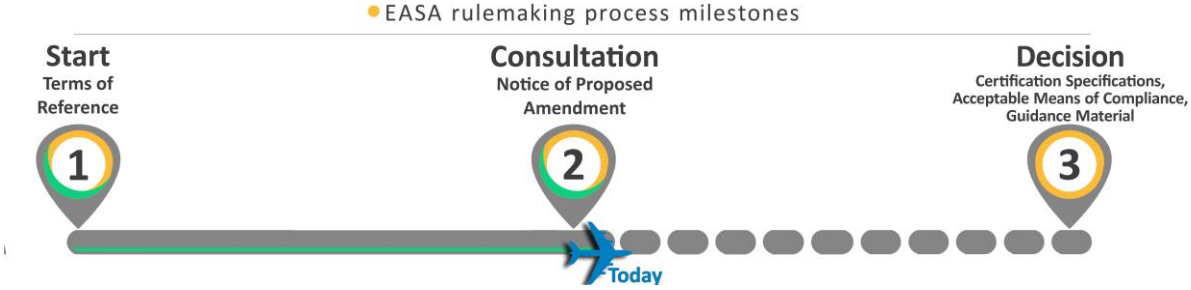

Table of contents

1. About this NPA

1.1. How this NPA was developed

The European Aviation Safety Agency (EASA) developed this NPA in line with Regulation (EC) No 216/2008[1] (hereinafter referred to as the 'Basic Regulation') and the Rulemaking Procedure[2]. This rulemaking activity is included in the EASA Rulemaking and Safety Promotion Programme 2017-2021[3] under rulemaking task (RMT).0469. The text of this NPA has been developed by EASA. It is hereby submitted to all interested parties[4] 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/**[5].

The deadline for submission of comments is **30 November 2017.**

1.3. The next steps

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

Based on the comments received, EASA will develop a decision amending the AMC/GM to Regulation (EU) 2017/373[6].

The comments received and the EASA responses will be reflected in a comment-response document (CRD). The CRD will be annexed to the aforementioned decision.

---

1 Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC (OJ L 79, 19.3.2008, p. 1) (http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1467719701894&uri=CELEX:32008R0216).

2 EASA is bound to follow a structured rulemaking process as required by Article 52(1) of Regulation (EC) No 216/2008. 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 http://easa.europa.eu/rulemaking/annual-programme-and-planning.php

4 In accordance with Article 52 of Regulation (EC) No 216/2008 and Articles 6(3) and (7) of the Rulemaking Procedure.

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

6 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

Regulation (EU) 2017/373 lays down common requirements for providers of ATM/ANS and other ATM network functions and their oversight and repeals amongst others Regulation (EC) No 482/2008[7] that establishes a software safety assurance system to be implemented by ATM/ANS providers. Regulation (EU) 2017/373 was developed based on EASA Opinions Nos 03/2014 and 02/2015.

Opinion No 03/2014 resulted from the consultation of the following NPAs with the interested parties, including industry, national aviation authorities and social partners:

— NPA 2013-08 'Requirements for ATM/ANS providers and the safety oversight thereof' issued on 10 May 2013;

— NPA 2014-07 on 'Technical requirements and operational procedures for the provision of meteorological services' issued on 28 March 2014; and

— NPA 2014-13 on 'Assessment of changes to functional systems by service providers in ATM/ANS and the oversight of these changes by competent authorities' issued on 24 June 2014.

NPA 2014-13 proposed:

— explicit requirements for the oversight of changes to functional systems after their implementation during the continuous oversight by the competent authorities;

— explicit requirements for the approval of the change management procedures from competent authorities;

— enhancement of the requirements for the review decision and the review of the changes to functional systems by competent authorities;

— more explicit requirements to introduce processes into the management system of certified service providers in order to actively monitor the behaviour of the functional system and, where underperformance is identified, to establish and eliminate its causes or mitigate its effects;

— explicit requirements for the change management procedures and for the changes affecting more than one certified service provider and aviation undertakings; and

— requirements for the assessment and the assurance of changes to the functional systems applicable to all certified service providers.

By enhancing the understanding of these concepts, it is expected that harmonisation across Europe will also improve.

However, during the Single Sky Committee (SSC) process as well as other forums, e.g. EASA Advisory Bodies meetings, EASA was warned of a potential safety weakness as regards the software assurance aspects when dealing with the safety (support) assessment of changes to a functional system in ATM/ANS and other ATM network functions. In the current regulatory framework, the software aspects are covered in detail through Regulation (EC) No 482/2008, which applies to any changes to

[7] Commission Regulation (EC) No 482/2008 of 30 May 2008 establishing a software safety assurance system to be implemented by air navigation service providers and amending Annex II to Regulation (EC) No 2096/2005 (OJ L 141, 31.5.2008, p. 5) (http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1492590800640&uri=CELEX:32008R0482).

the software of the systems for air traffic services (ATS), airspace management (ASM), air traffic flow management (ATFM), and communication, navigation, or surveillance (CNS). Additionally, the software aspects for aeronautical information services (AIS) provision are included in Regulation (EU) No 73/2010[8]. On the contrary, Regulation (EU) 2017/373 sets requirements for the assessment and assurance of the changes to functional systems, which is consistent with the concept of the existing requirements laid down in Regulation (EC) No 482/2008 in a more generic manner by providing more flexibility, but also extending the scope of the assurance process to the other parts of the functional system (people, procedures and equipment, i.e. hardware) rather than to software alone. However, this has been seen as a gap compared to the current system.

In this context, following the NPA 2014-13 consultation, the conclusion reached was that Regulation (EC) No 482/2008 can be repealed, thereby simplifying the regulatory framework and avoiding a double set of requirements. Nevertheless, it was identified that the more detailed provisions of Regulation (EC) No 482/2008 should be moved to AMC/GM. Being AMC/GM, they would serve as a means by which the implementing rule requirements, where the software assurance aspects are addressed, can be met, offering, thus, the benefit of presumption of compliance. However, applicants may decide to show compliance with the requirements using other means and may propose an alternative means of compliance (AltMoC), based, or not, on those issued by EASA. These AltMoC can be only used when it is demonstrated that the safety objective set out in the implementing rules is met. In addition, through the present NPA on SWAL AMC/GM would like to gain stakeholders' views as regards the hardware assurance level (HWAL) to ensure that EASA is taking an informed decision on the next steps.

This NPA proposes a transposition of the already known provisions (with some adaptations) in Regulation (EC) No 482/2008 to the AMC material and the introduction into the GM part of the references to some of the existing industrial standards, which may be used by the ANSPs to build their software assurance systems.

Furthermore, after the closure of this NPA consultation, the aim of EASA is to issue the ED Decision (and the associated CRD) on the additional AMC/GM addressing (at least) SWAL well in advance of the applicability date of Regulation (EU) 2017/373, i.e. 2 January 2020.

In conclusion, it should be highlighted that modern ATM/ANS systems include the use of electronic hardware items for performing functions, which were previously allocated to software controlled microprocessor-based systems. Some of these electronic hardware items (e.g. application specific integrated circuits, programmable gate arrays or solid-state logic controllers) are often as complex as software and might require the need of establishing an assurance process to satisfy their functional and safety requirements. The assurance aspects of these items are not within the scope of the current regulatory framework, i.e. Regulation (EC) No 482/2008.

In this context, as regards hardware assurance, the stakeholders are invited to indicate their views on the possibility of an equivalent set of AMC/GM in respect of hardware assurance being developed by EASA and consulted via a separate NPA.

[8] Commission Regulation (EU) No 73/2010 of 26 January 2010 laying down requirements on the quality of aeronautical data and aeronautical information for the single European sky (OJ L 23, 27.1.2010, p. 6) (http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1492593011927&uri=CELEX:32010R0073).

2.2. What we want to achieve — objectives

The overall objectives of the EASA system are defined in Article 2 of the Basic Regulation. This proposal will contribute to the achievement of the overall objectives by addressing the issues outlined in Chapter 2.

The specific objective of this proposal is to maintain the level of safety in the definition and implementation of the software assurance systems.

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

The current applicable regulatory framework for the provision of ANS and oversight in ATM/ANS (i.e. Regulations (EU) Nos 1034/2011[9] and 1035/2011[10]) define the 'functional system' as a combination of systems, procedures and human resources organised to perform a function within the context of ATM/ANS. The software aspects are covered in detail through Regulation (EC) No 482/2008, which applies to any changes to the software of the systems for ATS, ASM, ATFM, and CNS. This was seen as a potential safety weakness; hence, whereas Regulation (EU) 2017/373 is based on the framework of the existing requirements laid down in Regulation (EC) No 482/2008, it sets requirements for the assessment and assurance of the changes to functional systems in a more generic manner by providing more flexibility, but also extending the scope of the assurance process to the other parts of the functional system (people, procedures and equipment[11]) rather than to the software alone.

Consequently, Regulation (EC) No 482/2008 is repealed by Regulation (EU) 2017/373, thereby simplifying the regulatory framework and avoiding a double set of requirements. Nevertheless, it was identified and voiced by ATM/ANS stakeholders that the more detailed provisions of Regulation (EC) No 482/2008 should also be moved to AMC/GM. Therefore, with this NPA, EASA completes the AMC/GM published with ED Decision 2017/001/R by addressing these software (safety) assurance aspects.

The proposal for AMC/GM indicates the characteristics/objectives of the assurance system to be applied to the development and verification of the software components of the functional system. Furthermore, references to the currently available standards (e.g. EUROCAE ED-109A and its supplements, ED-153, ED-76A for AIS, etc.) that could be used by the service providers are included, as part of GM, in order to satisfy the characteristics of the assurance system specified at AMC level.

2.3.1. Proposed amendments to Subpart A 'General requirements' of Annex III 'AMC/GM to Part-ATM/ANS.OR — Common requirements for service providers'

Two new GM are proposed, which stem from Article 3(3) of Regulation (EC) No 482/2008. The service provider is required to produce an assurance argument whether or not it is to be reviewed by the competent authority. In this context, GM2 ATM/ANS.OR.A.045(a) clarifies with regard to the notification that depending on the complexity of the change to the functional system and the criticality of the software, the depth of the evaluation may vary. Therefore, the service provider should

[9] 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) (http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1492673204156&uri=CELEX:32011R1034).

[10] 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) (http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1492673327793&uri=CELEX:32011R1035).

[11] Note: 'equipment' includes both hardware and software.

coordinate as soon as possible with the competent authority in order to define a software oversight strategy as part of the change review activities. On the other hand, GM1 ATM/ANS.OR.A.050 aims to ensure that the service providers make available the required assurances to the competent authority by demonstrating that the software assurance system meets the objectives.

2.3.2. 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'

Two new AMC are proposed to ATM/ANS.OR.C.005(a)(2) 'Safety support assessment and assurance of changes to the functional system'.

AMC5 ATM/ANS.OR.C.005(a)(2) provides the means for compliance on the software assurance when the service provider introduces new software or modifies the existing one.

AMC6 ATM/ANS.OR.C.005(a)(2) addresses the software assurance processes. It provides the minimum evidence and arguments that need to be considered/addressed by the software assurance processes, their definition and also specifies what they should ensure and cover.

These AMC originate mainly from Articles 3(2), 4 and 5 and Annex II to Regulation (EC) No 482/2008.

Moreover, three GM are introduced to AMC6 ATM/ANS.OR.C.005(a)(2) that respectively address:

— the SWALs;

— the SWALs allocation; and

— examples of existing industrial standards.

2.3.3. Proposed amendments to Subpart A 'Additional organisation requirements for providers of air traffic services) of Annex IV 'AMC/GM to Part-ATS — Specific requirements for providers of air traffic services'

Similar provisions to the ones mentioned in Section 2.3.2. have also been developed for ATS providers, i.e. two new AMC are proposed to ATS.OR.205(a)(2) 'Safety assessment and assurance of changes to the functional system' supplemented by three GM to AMC4 ATS.OR.205(a)(2).

The only new GM compared to the GM on software assurance for providers other than ATS provider, is the one that addresses the allocation of the SWALs by the ATS providers.

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

When 'transposing' Regulation (EC) No 482/2008 that establishes a software safety assurance system to be implemented by ANSPs, only the necessary adjustments have been made by associating the provisions with the rules laid down in Regulation (EU) 2017/373 without detriment to the principles preserved. Therefore, EASA simply transposed the remaining provisions of Regulation (EC) 482/2008 with no major changes to the principles.

In this context, the benefit expected from this proposal is that the service providers can continue with their existing SWAL systems as part of the safety (support) assessments and hence, there are no drawbacks identified. Therefore, the possibility for choosing the options on how to proceed with the development of rules on the software changes to the functional system in ATM/ANS was very limited.

For this reason, no RIA has been developed for this task. Moreover, in this context, EASA has already performed a regulatory impact assessment (RIA) for a number of key regulatory developments with the publication of NPA 2014-13, addressing, amongst other issues, the changes affecting software and Regulation (EC) No 482/2008.

Furthermore, in order to assist the reader in identifying the changes that have been made to Regulation (EC) No 482/2008, a cross reference table has been developed with the aim of facilitating traceability of the provisions proposed. The cross reference table shows how Regulation (EC) No 482/2008 has been transposed, what the changes are and their justification. Said table is contained in the Appendix to this NPA (Chapter 6).

In addition, the implementation feedback of Regulation (EC) No 482/2008 from EASA standardisation inspections has not shown relevant issues with the implementation across the EU Member States.

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

GM2 ATM/ANS.OR.A.045(a) Changes to a functional system
NOTIFICATION — SOFTWARE CRITICALITY

Depending on the complexity of the change to the functional system and the criticality of the software, the depth of the evaluation may vary. The service provider should coordinate as soon as possible with the competent authority in order to define a software oversight strategy as part of the change review activities.

(…)

GM1 ATM/ANS.OR.A.050 Facilitation and cooperation
AUDITS — SOFTWARE ASSURANCE PROCESSES BY THE COMPETENT AUTHORITY

(a) The assessment of an effective application of the documented software assurance processes may necessitate a technical evaluation of the evidence and arguments produced for the software assurance by the competent authority when reviewing a notified change. In this context, the service provider should ensure access to the development environment and to the configuration management system to the competent authority that needs to verify:

(1) the consistency of all the evidence; and

(2) the fact that all the evidence derived from a known version of the software (i.e. all evidence and arguments are actually available and can be traced without ambiguity to the executable version).

(b) The service provider should:

(1) anticipate the possibility for on-site audits or inspections by the competent authority; and

(2) when evidence and arguments are developed by contracted organisations, include the corresponding rights to audit into the contractual provisions.

(…)

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

(…)

AMC5 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system
ASSURANCE — SOFTWARE

(a) When a change to a functional system includes the introduction of new software or modifications to existing software, the service provider should ensure the existence of documented software assurance processes necessary to produce evidence and arguments that demonstrate that the software behaves as intended (software requirements), with a level of confidence consistent with the criticality of the required application.

(b) The service provider should use feedback of software experience to confirm that the software assurance processes are effective and, when applicable, the allocated software assurance level (SWAL) and the rigour of each assurance level are appropriate. For that purpose, the effects from a software malfunction or failure reported according to the relevant requirements on reporting and assessment of service occurrences should be assessed in comparison with the effects identified for the system concerned as per the service specification.

AMC6 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system
ASSURANCE — SOFTWARE ASSURANCE PROCESSES

(a) The software assurance processes should provide evidence and arguments that they, as a minimum, demonstrate the following:

(1) The software requirements correctly state what is required by the software, in order to meet the service and safety support requirements, as identified by the safety support assessment (AMC2.ATM/ANS.OR.C005(a)(2)). For that purpose, the software requirements:

(i) are correct, complete and compliant with the upper level requirements; and

(ii) specify the functional behaviour, in nominal and downgraded modes, timing performances, capacity, accuracy, software resource usage on the target hardware, robustness to abnormal operating conditions and overload tolerance, as appropriate, of the software.

(2) The traceability is addressed in respect of all software requirements as follows:

(i) Each software requirement introduced at each level in the design should be traced to the same level of design at which its satisfaction is demonstrated.

(ii) Each software requirement, at each level in the design, at which its satisfaction is demonstrated, should be traced to an upper level requirement. If a requirement cannot be traced to any upper level requirement, its need should be justified and

assessed that it does not affect the satisfaction of the safety requirements allocated to the component.

(3) The software implementation contains no functions which adversely affect safety.

(4) The functional behaviour, timing performances, capacity, accuracy, software resource usage on the target hardware, robustness to abnormal operating conditions and overload tolerance, of the implemented software comply with the software requirements.

(5) The verification of the software is correct and complete, following verification methods (analysis, testing and/or equivalent means) agreed with the competent authority.

(c) The evidence and arguments should be derived from:

(1) a known executable version of the software;

(2) a known range of configuration data; and

(3) a known set of software products and descriptions, including specifications, that have been used in the production of that version.

(d) The software assurance processes should determine the rigour, to which the evidence and arguments are produced.

(e) The software assurance processes should include the necessary activities to ensure that the software life cycle data can be shown to be under configuration control throughout the software life cycle, including the possible evolutions due to changes or problems corrections. They should include, as a minimum:

(1) configuration identification, traceability and status accounting activities, including archiving procedures;

(2) problem reporting, tracking and corrective actions management; and

(3) retrieval and release procedures.

(f) The software assurance processes should also cover the particularities of specific types of software such as commercial-off-the-shelf (COTS), non-developmental software and previously developed software where generic assurance processes cannot be applied. The software assurance processes should include other means to give sufficient confidence that the software meets the service and safety support requirements, as identified by the safety risk assessment and mitigation processes. If no sufficient assurance can be provided, complementary mitigation means aiming at decreasing the impact of specific failure modes of this type of software, should be applied. This may include but is not limited to:

(4) software and/or system architectural considerations;

(5) existing service level experience; and

(6) monitoring**.**

GM1 to AMC6 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system

ASSURANCE — SOFTWARE ASSURANCE LEVELS

(a) The assurance required by AMC6 ATM/ANS.OR.C.005(a)(2) can be provided with different levels of confidence depending on the rigour of the evidence and arguments that are produced. Whereas, for air traffic services (ATS) providers, the use of the SWAL concept can be helpful to provide an explicit link between the criticality of the software and the rigour of the assurance, for service providers other than ATS providers, the use of SWAL concept may not be relevant considering that non-ATS providers may not be aware of the safety aspects of the ATS provider using their services.

(b) However, considering that the safety support assessment will be based on the evidence and arguments generated by the software assurance processes and that the safety support assessment will support a safety assessment, it is foreseen that, in many changes, the software assurance evidence and arguments will have to demonstrate a certain level of confidence and therefore will have to show compliance with the SWAL allocated by the ATS provider.

(c) The use of multiple SWALs would also allow the possibility of managing several criticalities of the different software components within the system by the same set of software assurance processes. When the software assurance processes are intended to rely on several Software Assurance Levels, they should define for each SWAL the rigour to which the assurances are established to achieve compliance with the objectives set out in AMC6 ATM/ANS.OR.C.005(a)(2). As a minimum:

(1) the rigour should increase as the software increases in criticality; and

(2) the variation in rigour of the evidence and arguments per SWAL should include a classification of the activities and objectives according to the following criteria:

(i) required to be achieved with independence;

(ii) required to be achieved; and

(iii) not required.

(d) When dealing with specific types of software, such as COTS, non-developmental software and previously developed software, where evidence and arguments cannot be provided with generic assurance processes, the software assurance processes should define, for each SWAL, the alternative means that may be applied in order to demonstrate an equivalent level of confidence as with generic assurance processes.

GM2 to AMC6 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system

ASSURANCE — SOFTWARE ASSURANCE LEVELS ALLOCATION

The process to allocate a SWAL to a software consistently with its foreseen criticality as identified by the safety support assessment and requirements should consider the following elements:

(a) The allocated SWALs should relate the rigour of the software assurances to the foreseen criticality of the software.

(b) The allocated SWAL should be commensurate with the most severe effect that software malfunctions or failures may cause, according to the safety support assessment.

(c) The software components that cannot be shown to be independent of one another should be allocated to the SWAL of the most critical of the dependent components.

(d) The allocated SWALs should be consistent with the levels defined in the software assurance processes.

GM3 to AMC6 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system

ASSURANCE — EXAMPLES OF EXISTING INDUSTRIAL STANDARDS

(a) The service provider is responsible for the definition of the software assurance processes. In this definition of processes, the service provider may consider the guidance material contained in existing industrial standards for the production of safety-critical software. It should be considered that not all standards address all aspects required and the service provider may need to define additional software assurance processes. The guidance material typically includes:

(1) objectives of the software life cycle processes;

(2) activities for satisfaction of those objectives;

(3) descriptions of the evidence, in the form of software life cycle data, that indicates that the objectives have been satisfied;

(4) variations according to the SWAL, to accommodate the different levels of rigour; and

(5) particular aspects (e.g. previously developed software) that may be applicable to certain applications.

(b) The following table presents some of the existing industrial standards (at the latest available issue) used by the stakeholders:

Document title	Reference	Date
Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems	EUROCAE ED-109A/ RTCA DO-278B	January 2012
Software Considerations in Airborne Systems and Equipment Certification	EUROCAE ED-12C/ RTCA DO-178C	January 2012
Guidelines for ANS Software Safety Assurance	EUROCAE ED-153	August 2009
Standards for Processing Aeronautical Data (only for AIS providers)	EUROCAE ED-76A/ RTCA DO-200B	June 2015

ED-109A/DO-278B and ED-12C/DO-178C make reference to some external documents (supplements), which are integral part of the standard for the use of some particular technologies and development techniques. The supplements are the following:

(1) Formal Methods Supplement to ED-12C and ED-109A (EUROCAE ED-216/RTCA DO-333)

(2) Object-Oriented Technology and related Techniques Supplement to ED-12C and ED-109A (EUROCAE ED-217/RTCA DO-332)

(3) Model-Based Development and Verification Supplement to ED-12C and ED-109A (EUROCAE ED-218/RTCA DO-331)

When tools are used during the software development lifecycle, EUROCAE ED-215/RTCA DO-330 'Software Tool Qualification Considerations' may be considered in addition to ED-12C RTCA/DO-178C and ED-109A/RTCA DO-278B.

(c) The definition of the software assurance processes may be based on one of these industrial standards, without combining provisions for different standards as far as the consistency and validation of each of the industrial standards have only been performed at individual level by each specific standardisation group.

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

(…)

AMC3 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system
ASSURANCE — SOFTWARE

(a) When a change to a functional system includes the introduction of new software or modifications to existing software, the ATS provider should ensure the existence of documented software assurance processes necessary to produce evidence and arguments that demonstrate that the software behaves as intended (software requirements), with a level of confidence consistent with the criticality of the required application.

(b) The ATS provider should use feedback of software experience to confirm that the software assurance processes are effective and, when applicable, the allocated assurance levels and the rigour of each assurance level are appropriate. For that purpose, the effects from a software malfunction or failure reported according to the relevant requirements on reporting and assessment of safety occurrences should be assessed in comparison with the effects identified for the system concerned as per the severity classification scheme.

AMC4 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system
ASSURANCE — SOFTWARE ASSURANCE PROCESSES

(a) The software assurance processes should provide evidence and arguments that they, as a minimum, demonstrate the following:

(1) The software requirements correctly state what is required by the software, in order to meet the upper level requirements, including the allocated system safety requirements, as identified by the safety assessment of changes to the functional system (AMC2.ATS.OR.205(a)(2)). For that purpose, the software requirements:

(i) are correct, complete and compliant with the upper level requirements; and

(ii) specify the functional behaviour, in nominal and downgraded modes, timing performances, capacity, accuracy, software resource usage on the target hardware, robustness to abnormal operating conditions and overload tolerance, as appropriate, of the software.

(2) The traceability is addressed in respect of all software requirements as follows:

(i) Each software requirement introduced at each level in the design should be traced to the same level of design, at which its satisfaction is demonstrated.

(ii) Each software requirement, at each level in the design, at which its satisfaction is demonstrated, is traced to an upper level requirement. If a requirement cannot be traced to any upper level requirement, its need should be justified and assessed that it does not affect the satisfaction of the safety requirements allocated to the component.

(3) The software implementation contains no functions which adversely affect safety.

(4) The functional behaviour, timing performances, capacity, accuracy, software resource usage on the target hardware, robustness to abnormal operating conditions and overload tolerance, of the implemented software comply with the software requirements;

(5) The verification of the software is correct and complete, following verification methods (analysis, testing and/or equivalent means) agreed with the competent authority.

(b) The evidence and arguments should be derived from:

(1) a known executable version of the software;

(2) a known range of configuration data; and

(3) a known set of software products and descriptions, including specifications, that have been used in the production of that version.

(c) The software assurance processes should determine the rigour to which the evidence and arguments are produced.

(d) The software assurance processes should include the necessary activities to ensure that the software life cycle data can be shown to be under configuration control throughout the software life cycle, including the possible evolutions due to changes or problems corrections. They should include, as a minimum:

(1) configuration identification, traceability and status accounting activities, including archiving procedures;

(2) problem reporting, tracking and corrective actions management; and

(3) retrieval and release procedures.

(e) The software assurance processes should also cover the particularities of specific types of software such as COTS, non-development software and previously developed software where generic assurance processes cannot be applied. The software assurance processes should include other means to give sufficient confidence that the software meets the safety objectives and requirements, as identified by the safety risk assessment and mitigation processes. If no sufficient assurance may be provided, complementary mitigation means aiming at decreasing the impact of specific failure modes of this type of software, should be applied. This may include but is not limited to:

(1) software and/or system architectural considerations;

(2) existing service level experience; and

(3) monitoring.

GM1 to AMC4 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system

ASSURANCE — SOFTWARE ASSURANCE LEVELS

(a) The assurance required by AMC4 ATS.OR.205(a)(2) should be provided with a level of confidence consistent with the criticality of the software in order to generate an appropriate and sufficient body of evidence to help establish the required confidence in the argument.

(b) The use of the SWAL concept can be helpful to provide an explicit link between the criticality of the software and the rigour of the assurance.

(c) The use of multiple SWALs would also allow the possibility of managing several criticalities of the different software components within the system by the same set of software assurance processes. When the software assurance processes are intended to rely on several SWALs, they should define for each SWAL, the rigour to which the assurances are established to achieve compliance with the objectives set out in AMC4 ATS.OR.205(a)(2). As a minimum:

(1) the rigour should increase as the software increases in criticality; and

(2) the variation in rigour of the assurances per SWAL should include a classification of the activities and objectives according to the following criteria:

(i) required to be achieved with independence;

(ii) required to be achieved; and

(iii) not required.

(d) When dealing with specific types of software, such as COTS, non-developmental software or previously developed software, where evidence and arguments cannot be provided with generic assurance processes, the software assurance processes should define, for each SWAL, the

alternative means that may be applied in order to demonstrate an equivalent level of confidence as with generic assurance processes.

GM2 to AMC4 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system

ASSURANCE — SOFTWARE ASSURANCE LEVELS ALLOCATION

The process to allocate a SWAL to a software consistently with its criticality as identified by the risk assessment and mitigation process should consider the following elements:

(a) The allocated SWALs should relate the rigour of the software assurances to the criticality of the software by using the combination of the used severity classification scheme with the likelihood of occurrence of a certain adverse effect.

(b) The allocated SWALs should be commensurate with the most severe effect that software malfunctions or failures may cause, according to the used severity classification scheme. It should, in particular, take into account the risks associated with software malfunctions or failures and the architecture and/or procedural defences identified.

(c) The software components that cannot be shown to be independent of one another should be allocated to the SWAL of the most critical of the dependent components.

(d) The allocated SWALs should be consistent with the SWALs defined in the software assurance processes of the ATS provider and of the non-ATS provider(s), when the safety case is based on the evidence presented in the corresponding safety support case(s).

GM3 to AMC4 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system

ASSURANCE — EXAMPLES OF EXISTING INDUSTRIAL STANDARDS

(a) The service provider is responsible for the definition of the software assurance processes. In this definition of processes, the service provider may consider the guidance contained in existing industrial standards for the production of safety-critical software. It should be considered that not all standards address all aspects required and the service provider may need to define additional software assurance process. The guidance material typically includes:

(1) objectives of the software life cycle processes;

(2) activities for satisfaction of those objectives;

(3) descriptions of the evidence, in the form of software life cycle data, that indicates that the objectives have been satisfied;

(4) variations according to the SWAL, to accommodate the different levels of rigour; and

(5) particular aspects (e.g. previously developed software) that may be applicable to certain applications.

(b) The following table presents some of the existing industrial standards (at the latest available issue) used by the stakeholders:

Document title	Reference	Date
Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems.	EUROCAE ED-109A/ RTCA DO-278B	January 2012
Software Considerations in Airborne Systems and Equipment Certification	EUROCAE ED-12C/ RTCA DO-178C	January 2012
Guidelines for ANS Software Safety Assurance	EUROCAE ED-153	August 2009

ED-109A/DO-278B and ED-12C/DO-178C make reference to some external documents (supplements), which are integral part of the standard for the use of some particular technologies and development techniques. The supplements are the following:

(1) Formal Methods Supplement to ED-12C and ED-109A (EUROCAE ED-216/RTCA DO-333)

(2) Object-Oriented Technology and related Techniques Supplement to ED-12C and ED-109A (EUROCAE ED-217/RTCA DO-332)

(3) Model-Based Development and Verification Supplement to ED-12C and ED-109A (EUROCAE ED-218/RTCA DO-331)

When tools are used during the software development lifecycle, EUROCAE ED-215/RTCA DO-330 'Software Tool Qualification Considerations' may be considered in addition to ED-12C/DO-178C and ED-109A/DO-278B.

(c) The definition of the software assurance processes may be based on one of these industrial standards, without combining provisions for different standards as far as the consistency and validation of each of the industrial standards have only been performed at individual level by each specific standardisation group.

GM4 to AMC4 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system

ASSURANCE — SWAL COORDINATION

(a) Within the scope of this Regulation, only the ATS provider can identify hazards, assess the associated risks and mitigate or propose mitigating measures where necessary. This requirement applies also to software assurances as they may be identified as mitigation means against software design failures.

(b) ATS and non-ATS providers may rely on different set of software assurance processes and, when applicable, different set of SWALs.

(c) For a particular change to the functional system, the safety assessment performed by the ATS provider, and documented in the safety case, may rely on evidence associated with the services provided by a non-ATS provider, as documented in its corresponding safety support case. It should as a minimum demonstrate that the rigour of the assurances produced by the non-ATS provider within the safety support case provides the adequate level of confidence for the purpose of the ATS safety demonstration in the safety case.

(d) When SWALs are used, the ATS provider should evaluate the adequacy of the SWALs defined in the software assurance processes of the non-ATS providers and the consistency of the allocated SWALs for the parts of the functional system affected by the change at the non-ATS provider.

4. Proposed actions to support implementation

— Dedicated thematic workshop(s)/session(s) with the participation of both industry and competent authorities representatives

— Series of thematic events organised on the regional principle with the participation of both industry and competent authorities representatives

5. References

5.1. Related regulations

— Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC (OJ L 79, 19.3.2008, p. 1).

— Commission Regulation (EC) No 482/2008 of 30 May 2008 establishing a software safety assurance system to be implemented by air navigation service providers and amending Annex II to Regulation (EC) No 2096/2005 (OJ L 141, 31.5.2008, p. 5).

— 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

5.3. Other reference documents

— EUROCAE ED-109A/RTCA DO-278B — Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems, dated January 2012

— EUROCAE ED-12C/ RTCA DO-178C — Software Considerations in Airborne Systems and Equipment Certification, dated January 2012

— EUROCAE ED-153 — Guidelines for ANS Software Safety Assurance, dated August 2009

— EUROCAE ED-76A/RTCA DO-200B — Standards for Processing Aeronautical Data (only for AIS providers), dated June 2015

6. Appendix

Cross reference table — Regulation (EC) No 482/2008 of 30 May 2008 establishing a software safety assurance system to be implemented by air navigation service providers as transposed through the proposed requirements in this NPA

Regulation (EC) No 482/2008	**Subject**	**NPA reference**
Article 1	Subject matter and scope	n/a
Article 2	Definitions	n/a
Article 3	General safety requirements	
Article 3(2)(a)		AMC6 ATM/ANS.OR.C.005(a)(2), point (1)(a) AMC4 ATS.OR.205(a)(2), point (1)(a)
Article 3(2)(b)		AMC6 ATM/ANS.OR.C.005(a)(2), point (1)(b) AMC4 ATS.OR.205(a)(2), point (1)(b)
Article 3(2)(c)		AMC6 ATM/ANS.OR.C.005(a)(2), point (1)(c) AMC4 ATS.OR.205(a)(2), point (1)(c)
Article 3(2)(d)		AMC5 ATM/ANS.OR.C.005(a)(2), point (1) AMC3 ATS.OR.205(a)(2), point (1)
Article 3(2)(e)		AMC6 ATM/ANS.OR.C.005(a)(2), point (2) AMC4 ATS.OR.205(a)(2), point (2)
Article 3(3)		GM2 ATM/ANS.OR.A.045(a) GM1 ATM/ANS.OR.A.050
Article 4	Requirements applying to the software safety assurance system	ATM/ANS.OR.B.010(a)(1)
Article 4(1)		regarding the need of having documented software assurance processes: AMC5 ATM/ANS.OR.C.005(a)(2), point (1) AMC3 ATS.OR.205(a)(2), point (1)
Article 4(2)		Same reference as Annex I
Article 4(3)(a)		Same reference as Annex II Part A
Article 4(3)(b)		Same reference as Annex II Part B
Article 4(3)(c)		Same reference as Annex II Part C
Article 4(3)(d)		Same reference as Annex II Part D
Article 4(4)		Mainly addressed in NPA 2014-13; In this NPA, the software elements are dealt with in: AMC6 ATM/ANS.OR.C.005(a)(2), point (3) AMC4 ATS.OR.205(a)(2), point (3) *Note: with the exception of the element pertaining to*

Regulation (EC) No 482/2008	**Subject**	**NPA reference**
		how to consider the independent execution of activities, which is moved to GM.
Article 4(5)		AMC5 ATM/ANS.OR.C.005(a)(2), point (2) AMC3 ATS.OR.205(a)(2), point (2)
Article 5	Requirements applying to changes to software and to specific software	Mainly addressed in NPA 2014-13; In this NPA the software elements are: AMC6 ATM/ANS.OR.C.005(a)(2), point (5) AMC4 ATS.OR.205(a)(2), point (5)
Article 6	Amendment to Regulation EC (No) 2096/2005	N/A
Article 7	Entry into force	N/A
Annex I	Requirements applying to the software assurance level referred to in Article 4(2)	Mainly addressed in NPA 2014-13; In this NPA the software elements are dealt with in: AMC3 ATS.OR.205(a)(2)
Annex II — Part A		AMC6 ATM/ANS.OR.C.005(a)(2), points (1)(a)(i) and (ii) AMC4 ATS.OR.205(a)(2), points (1)(a)(i) and (ii)
Annex II — Part B		AMC6 ATM/ANS.OR.C.005(a)(2), points (1)(d) and (e) AMC4 ATS.OR.205(a)(2), points (1)(d) and (e)
Annex II — Part C		AMC6 ATM/ANS.OR.C.005(a)(2), point (4) AMC4 ATS.OR.205(a)(2), point (4)
Annex II — Part D		AMC6 ATM/ANS.OR.C.005(a)(2), points (1)(b)(i) and (ii) AMC4 ATS.OR.205(a)(2), points (1)(b)(i) and (ii) *Note: with some specific development regarding the derived requirements*