European Union Aviation Safety Agency

Comment-Response Document 2017-10

RELATED NPA 2017-10 — RMT.0469 — 29.10.2019

Table of contents

1. Summary of the outcome of the consultation

The public consultation period was prolonged, following the request of stakeholders, and ended on 8 December 2017. As a result of the public consultation, EASA received 315 comments, whose distribution is shown in Figure 1 below.

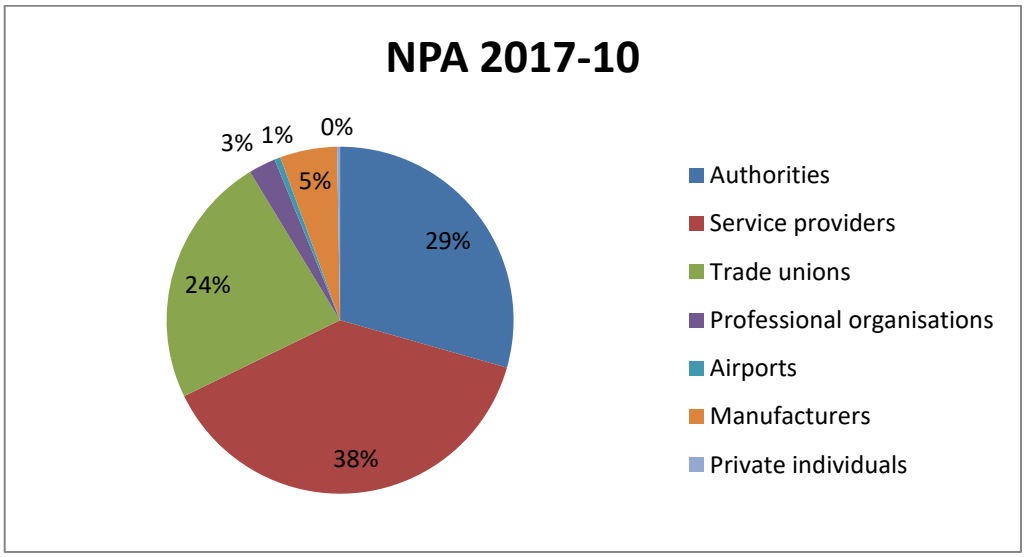

Figure 1: Percentage of comments per type of stakeholder

The nature of the comments received varies from comments regarding the applicability of the software assurance AMC & GM to certain service providers (e.g. MET providers) until proposals for stricter implementing measures.

Furthermore, after the closure of the public consultation, EASA carried out a focused consultation and held a thematic meeting in October 2017 purposed to review the main topics commented on the proposed acceptable means of compliance (AMC) and guidance material (GM). The thematic meeting involved experts who contributed actively to the NPA consultation. The purpose of the meeting was to gather advice on specific subjects that would facilitate EASA in taking informed decisions for the CRD publication and the final ED Decision.

The thematic meeting covered the following subjects:

— Legal responsibility for suppliers of EATMN systems and components;

— Extension and transition period for service providers not currently regulated by Regulation (EC) No 482/2008;

— Terminology;

— Software aspects in the context of safety (support) assessment;

— Coordination between the competent authority and the service provider(s);

— The use of industry standards as AMC & GM, including cyber security standards;

— (Possible) extension of the AMC & GM to hardware, people and procedures; and

— Reporting and assessment of service occurrences.

As regards the applicability of this set of AMC & GM, EASA considers that some of the service providers other than the ones that apply today Regulation (EC) No 482/2008 (e.g. MET, FPD, DAT providers) are more and more influenced by the software. Therefore, it was concluded that the features of these providers' systems are affected by the current regulatory requirements, which also supports the approach that the proposed set of AMC & GM should apply to all service providers of ATM/ANS, incl. AIS and MET providers towards software assurance level standardisation.

Following the NPA 2017-10 consultation, as regards hardware assurance, it is concluded that a further consideration is required and this element should be further discussed via a separate rulemaking activity.

EASA reviewed all the comments and, based on them, adjusted the AMC & GM that are annexed to Decision 2019/022/R.

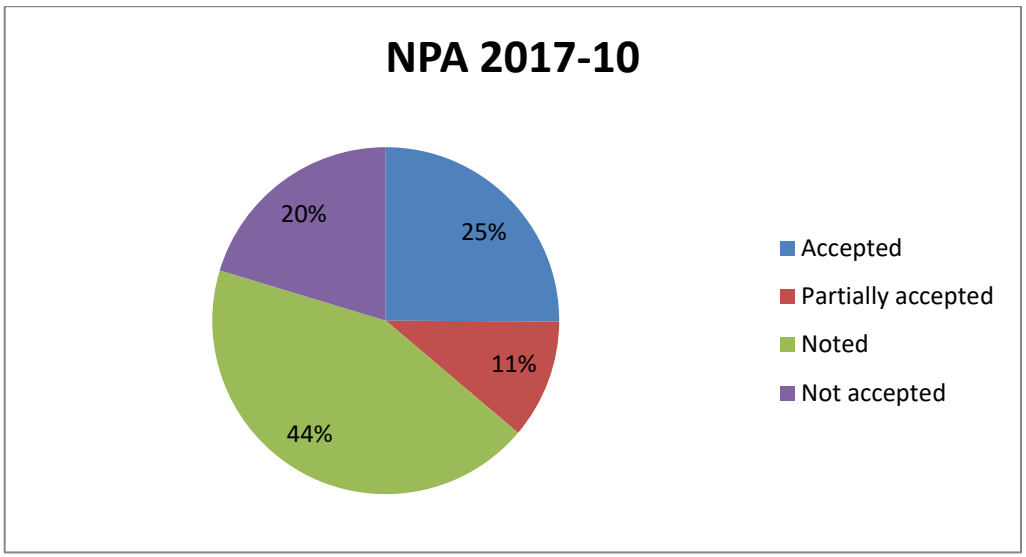

Figure 2: Percentage of comments that have been accepted, partially accepted, noted, or not accepted

2. Individual comments and responses

In responding to comments, a standard terminology has been applied to attest EASA's position. This terminology is as follows:

(a) **Accepted** — EASA agrees with the comment and any proposed amendment is wholly transferred to the revised text.

(b) **Partially accepted** — EASA either partially agrees with the comment, or agrees with it but the proposed amendment is only partially transferred to the revised text.

(c) **Noted** — EASA acknowledges the comment, but no change to the existing text is considered to be necessary.

(d) **Not accepted** — The comment or proposed amendment is not agreed by EASA.

(General Comments)	-

comment	*1* comment by: *DFS Deutsche Flugsicherung GmbH* There is high probability that the felt "potential safety weakness as regards the software assurance aspects" is a result of the complexity of the Common Requirements in this particular context. Adding more AMC, which do rather serve as new IR requirements than as means for implementation of existing ones, is not the right way to solve the complexity. These AMC represent a hurdle too high for the creation of any AltMoC. Instead, the provisions on safety management for ATM/ANS providers including changes to their functional systems should be revisited in applying the principles for Better Regulation, finding the right balance between IR and AMC and ensuring a level playing field.
response	*Noted* The comment is duly noted. The aim of the proposed set of AMC is not to trigger a development/management of AltMoC, but rather to provide AMC for the software assurance when introducing changes to the functional system. The need for this additional material regarding software assurance was expressed by several stakeholders, especially authorities during the Comitology process that resulted in Regulation (EU) 2017/373.

comment	*39* comment by: *CANSO* There is high probability that the felt "potential safety weakness as regards the software assurance aspects" is a result of the complexity of the Common Requirements in this particular context. Adding more AMC, which do rather serve as

new IR requirements than as means for implementation of existing ones, is not the right way to solve the complexity.

These AMC represent a hurdle too high for the creation of any AltMoC.

Instead, the provisions on safety management for ATM/ANS providers including changes to their functional systems should be revisited in applying the principles for Better Regulation, finding the right balance between IR and AMC and ensuring a level playing field.

response *Noted*

The comment is duly noted.

The aim of the proposed set of AMC is not to trigger a development/management of AltMoC, but rather to provide AMC for the software assurance when introducing changes to the functional system. The need for this additional material regarding software assurance was expressed by several stakeholders, especially authorities during the Comitology process that resulted in Regulation (EU) 2017/373.

comment *80* comment by: *EUROCONTROL*

The EUROCONTROL Agency welcomes the publication of EASA Notice of Proposed Amendment 2017-10. It also thanks EASA for the opportunity that has been given to submit comments. In addition, the EUROCONTROL Agency would like to confirm that it will read with interest the other comments on the NPA which will be received from the stakeholders and the responses given to them by EASA in its future comment-response document (CRD). It is hoped that the CRD will be published before it is annexed to the decision amending the AMC/GM to Regulation (EU) 2017/373 in order to give stakeholders some time for analysing the responses to comments and, if need be, further reflection.

In general, the EUROCONTROL Agency feels that the amendments proposed under NPA 2017-10 are almost the same as the requirements under EC482/2008, which will be repealed once EU 2017/373 comes in force. The EUROCONTROL Agency therefore does not make any comments on NPA content, with the exception of those made concerning ATS.OR.205(a)(2) and ATM/ANS.OR.C.005(a)(2). In addition, since the requirements proposed in the NPA are almost exclusively found at the level of Guidance Material only, and not at the level of Acceptable Means of Compliance, it seems that the NPA content could weaken the case for software assurance.

response *Noted*

EASA duly noted the comment.

On the other hand, the commentator is invited to note that Article 9 of MB Decision No 18-2015 (‘Rulemaking procedure’) applies. It regulates that the Executive Director shall issue his or her decision in respect of the rule in question together with the CRD.

comment *84* comment by: *EASA Focal Point for AustroControl ANSP-issues*

AUSTRO CONTROL, General Comment:
Observation:
AUSTRO CONTROL is highly concerned about the general direction of this NPA, to put the burden of legal responsibility for EATM-system's liability only on the ANSP's shoulders.

Proposal:
Even though it is clear responsibility of the ANSP to deliver safe services – including software - there should be a legal responsibility also for suppliers of EATMN systems and components, **to develop their components according the aeronautical standards.**

response *Noted*

This proposal follows the same principles as the ones laid down in Regulation (EU) 2017/373, where the responsibility lies with the ANSP for the provision of safe services. Consequently, no change is introduced by this set of AMC & GM on this particular aspect. It is considered that the ANSPs should have the appropriate interface with the developers of the EATM-systems in order to ensure the provision of safe services when using them.

comment *88* comment by: *CANSO*

Remark:
Rigour is used in EC 482/2008 as general sense, but in the present document it could also be understood in a stringent way where several rigour classes should be identified, depending of the SWAL, for the same process.
The term rigour should be clarified in this document in the way that it means the same as used in EC 482/2008.

response *Partially accepted*

A review of the rule text has been performed. Some of the AMC & GM have been updated in order to avoid the potential misunderstanding identified by the commentator.

comment *106* comment by: *ENAV*

There is high probability that the felt “potential safety weakness as regards the software assurance aspects” is a result of the complexity of the Common Requirements in this particular context. Adding more AMC, which do rather serve as new IR requirements than as means for implementation of existing ones, is not the right way to solve the complexity.

These AMC represent a hurdle too high for the creation of any AltMoC.

Instead, the provisions on safety management for ATM/ANS providers including changes to their functional systems should be revisited in applying the principles for Better Regulation, finding the right balance between IR and AMC and ensuring a level playing field.

response *Noted*

The comment is duly noted.

The aim of the proposed set of AMC is not to trigger a development/management of AltMoC, but rather to provide AMC for the software assurance when introducing changes to the functional system. The need for this additional material regarding software assurance was expressed by several stakeholders, especially authorities during the Comitology process that resulted in Regulation (EU) 2017/373.

comment *107* comment by: *ENAV*

Rigour is used in EC 482/2008 as general sense, but in the present document it could also be understood in a stringent way where several rigour classes should be identified, depending of the SWAL, for the same process.
The term rigour should be clarified in this document in the way that it means the same as used in EC 482/2008.

response *Partially accepted*

A review of the rule text has been performed. Some of the AMC & GM has been updated in order to avoid the potential misunderstanding identified by the commentator.

comment *126* comment by: *ENAV*

ENAV is highly concerned about the general direction of this NPA, to put the burden of legal responsibility for EATM-system's liability only on the ANSP's shoulders.

Proposal:
Even though it is clear responsibility of the ANSP to deliver safe services – including software - there should be a legal responsibility also for suppliers of EATMN systems and components, **to develop their components according the aeronautical standards**.

response *Noted*

This proposal follows the same principles as the ones laid down in Regulation (EU) 2017/373, where the responsibility lies with the ANSP for the provision of safe services. Consequently, no change is introduced by this set of AMC & GM on this particular aspect. It is considered that the ANSPs should have the appropriate interface with the developers of the EATM-systems in order to ensure the provision of safe services when using them.

comment	*129* comment by: *Avinor Air Navigation Services (Avinor Flysikring AS)* **Comment:** We think there is too little focus on exactly how to provide software assurance for COTS or already developed software, which leads everyone to develop a new strategy for this every time. **Justification:** Our opinion is that the ANSPs tend to buy and use more of COTS or already developed software, instead of going through an entire development process (which is also more costly).
response	*Accepted* An amendment to the text was introduced to include the definition for commercial off-the-shelf (COTS). At this moment, the proposed approach follows Regulation (EC) No 482/2008, where this is subject to agreement between the ANSP and the competent authority.

comment	*135* comment by: *LFV* Since NPA 2017-10 covers all ATM/ANS services, while current requirements for software assurance only covers ATS, ATFM, ASM and CNS services, a transition period is needed for these services, similar to those in EU 482/2008 article 7.
response	*Not accepted* It should be noted that Regulation (EC) No 482/2008 entered into force in 2010 and, hence, after several years of application, it is understood that the concept of software legacy does not require a particular treatment. Consequently, any new software or modifications to existing software should follow the software assurance processes.

comment	*138* comment by: *CANSO* CANSO is concerned about the general direction of this NPA, to put the burden of legal responsibility for EATM-system's liability only on the ANSP's shoulders. Proposal: Even though it is clear responsibility of the ANSP to deliver safe services – including software - there should be a legal responsibility also for suppliers of EATMN systems and components, to develop their components according the software development standards.
response	*Noted* This proposal follows the same principles as the ones laid down in Regulation (EU) 2017/373, where the responsibility lies with the ANSP for the provision of safe services. Consequently, no change is introduced by this set of AMC & GM on this particular aspect. It is considered that the ANSPs should have the appropriate

interface with the developers of the EATM-systems in order to ensure the provision of safe services when using them.

comment *142* comment by: *Federal Office of Civil Aviation (FOCA), Switzerland*

The Federal Office of Civil Aviation (FOCA) would like to thank the Agency for the opportunity to comment on the NPA 2017-10 Software assurance level requirements.
Please by advise that FOCA fully supports the content of this NPA.

response *Noted*

EASA appreciates the comment.

comment *173* comment by: *DSNA*

Rigour is used in EC 482/2008 as general sense, but in the present document it could also be understood in a stringent way where several rigour classes should be identified, depending of the SWAL, for the same process.
The term rigour should be clarified in this document in the way that it means the same as used in EC 482/2008.

response *Partially accepted*

A review of the rule text has been performed. Some of the AMC & GM have been updated in order to avoid the potential misunderstanding identified by the commentator.

comment *183* comment by: *AESA/DSANA*

What is considered a functional system in ATM and ANS? Does this NPA apply to all SW or only to operational SW?
This NPA includes more service providers in the SW assurance processes than EC 482/2008. For example, ASD providers were not taken into account in EC 482/2008.
Some doubts can arise such as:
Are Flight Procedures Design SW solution considered as a functional system?

response *Noted*

The AMC & GM presented in this NPA corresponds to the software part of the ANSP functional system, which is subject to safety or safety support assessments.

On the other hand, the applicability of Subpart C of Part-ATM/ANS.OR (safety support assessment requirements) and the associated AMC & GM to the Flight Procedure Design (FPD) provider is regulated in Article 6 of the subject Regulation.

comment *209* comment by: *European Transport Workers Federation - ETF*

definitions in EU Reg. 482/2008	Those definitions are not proposed for transposition here, can you confirm those have all been transposed in EU Reg. 2017/373 and if not explain why some are not transposed.

response *Accepted*

Considering the comment, the text has been updated to ensure that either all the definitions from Regulation (EC) No 482/2008 are included in Regulation (EU) 2017/373 or specifically mentioned in this set of AMC & GM.

comment *212* comment by: *DSAC - FR NSA*

Frenh NSA fully supports this NPA which explicitely develops software assurance concept as a necessary argument for safety (suppport) cases. This NPA will highly facilitate the oversight and the management of software aspects.

In the philosophy of this NPA, first discussions about 2017/373 have shown few understanding and considerations to system engineering concepts that have been propagated from software to the overall functional system in the scope of changes. Moreover the application of SWAL or any concept of assurance level is difficult to apply without an overal system development assurance level. Therefore, French NSA would also highly support the development of a complete set of development assurance levels addressing first system development aspects including equipment, people and procedures and then addressing all components of the functional system (people, procedure, swal, hwal).

response *Noted*

EASA appreciates the comment.

comment *213* comment by: *DSAC - FR NSA*

As stated in rmq#1, French NSA is in favour of any kind of assurance level concept. However, to the question of developing a HWAL AMC/GM, it should be considered 2 categories of hardware devices.
Most of complex electronic devices involved in ATM systems are COTS and consist of General Purpose Processors, Graphical Processor Units or microcontrollers. No or few assurance could be obtained from manufacturers. However regarding this kind of electronic hardware, software assurance considerations could be deemed sufficient considering that software verifications would cover hw functionalities. No HWAL would be required.
Some other ATM systems requiring specific functions and performances (radars, navigation systems (ILS, DME,...), radios) may require dedicated hardware devices which will definitely have to meet some safety performances. For these specific

hardware devices which are not verified through a software assurance process, it should be considered to develop a hardware assurance concept at least allowing to establish their functional requirements (including functions needed for safety considerations) and to demonstrate their achievement.

response *Noted*

Acknowledging the stakeholders' feedback from the NPA 2017-10 consultation, EASA will consider a separate rulemaking activity dedicated on the hardware assurance level requirements related to the assessment of changes to functional systems, where the comment will be taken into account.

comment *218* comment by: *NATS*

The structure of the guidance material leads to significant duplication of text that applies equally to service providers and ANSP sections, which could be presented more concisely.
Impact: Duplication of text could lead to subtle unintended variations in compliance against similar requirements
Suggested Resolution: Consider presenting guidance as applicable to both service providers and ANSPs in one section, and identifying differences at that level (rather than duplicating as currently)

response *Noted*

EASA acknowledges the existing duplications of provisions, but this approach was preferred to keep the segregated set of requirements separately, depending on the type of service provider.

A recast of the order of the requirements at IR level and the associated AMC & GM could be considered at a later stage via a separate rulemaking activity.

comment *219* comment by: *NATS*

Neither the NPA nor (EU)2017/373 appear to retain a definition of 'software', to set out what falls into scope. (EC) No 482/2008 states:
'software' means computer programmes and corresponding configuration data, including non-developmental software, but excluding electronic items, namely application specific integrated circuits, programmable gate arrays or solid-state logic controllers;
Impact: Assurance activity may/may not be required, dependent on scope.
Suggestion: Include a definition of software, either as stated for (EC) No 482/2008 or amended as appropriate to reflect the scope of (EU) No 2017/373.

response *Accepted*

The text has been updated in order to include the definition for 'software' in the set of AMC & GM, in line with Regulation (EC) No 482/2008.

comment	*220* comment by: *NATS* Neither the NPA nor (EU)2017/373 identifies a harmonised severity classification scheme for use when setting assurance levels. Is this covered by the more general references to the (unspecified) "severity classification scheme"? **Impact:** The use of an unspecified 'severity' classification scheme potentially leads to different assurance requirements from different ANSPs, for the same software product being used in the same way. **Suggestion**: Provide guidance/requirements for the severity classification scheme to facilitate common software assurance requirements.
response	*Noted* The comment is duly noted. It should be highlighted that the proposed set of AMC & GM corresponds to the safety objectives laid down in Regulation (EU) 2017/373. On the other hand, the same product can be used in different ways by different ANSPs and could lead to hazardous effects of different severities. This is an element to be considered by each of the ANSPs when performing the assurance level allocation.

comment	*221* comment by: *NATS* The term SWAL is used extensively in the NPA but no formal definition of it is provided. (EC) No 482/2008 mandated "a minimum of four software assurance levels shall be identified, with software assurance level 1 indicating the most critical level". Has this requirement been dropped intentionally? **Impact:** The lack of a definition for software assurance levels potentially leads to inconsistency of approach by ANSPs complying with the guidance material and therefore requiring different assurance evidence from system suppliers for the same product. **Suggestion:** Either: Add definition of SWAL to Annex I of (EU) 2017/373 or provide guidance/requirements regarding software assurance levels to facilitate common software assurance requirements.
response	*Accepted* Considering the comment, the text has been amended (please refer to ATM/ANS.OR.C.005(a)(2)).

comment	*222* comment by: *NATS* (EC) No 482/2008 had a clear requirement (Article 3, 1.) for an organisation to define and implement a software safety assurance system. A stated objective of this NPA (2.2) is to maintain the level of safety in the definition and implementation of the

	software assurance systems, yet there is no requirement, or even mention, in either (EU) 2017/373 or this NPA of a software (safety) assurance system. **Issue:** The migration from (EC) No 482/2008 to (EU) 2017/373 + NPA has lost the requirement for implementation of a software (safety) assurance system. **Suggestion:** Include a requirement equivalent to (EC) No 482/2008 Article 3, 1 and other associated requirements.
response	*Partially accepted* The commented element is duly considered. It is addressed by the combination of the new AMC & GM (for software aspects) with the existing AMC & GM, where all the software information is planned to be used as part of the safety (support) case(s) demonstration. It is noted that AMC3 ATS.OR.205(a)(2) requests that 'the ATS provider should ensure the existence of documented software assurance process necessary to produce evidence and arguments that demonstrate that the software behaves as intended (software requirements), which level is consistent with the criticality of the required application'. The main change in the concept is that the software safety assurance system is intended to provide inputs to the safety (support) assessments.

comment	*223* comment by: *NATS* In the transposition from (EC) No 482/2008 to the NPA, the requirements relating to "software safety requirements" (Article 3, 2.) have been broadened to "software requirements" (AMC6 ATM/ANS.OR.C.005(a)(2). NATS supports this change and believes it should improve the rigour applied to the software as a whole. No change required; this is a positive observation in support of the changes made from (EC) No 482/2008
response	*Noted* EASA appreciates the comment.

comment	*224* comment by: *NATS* The concept of hardware assurance level would be of potential benefit for bespoke hardware developed to support ATM applications. Such hardware procured at the direct request of an ANSP is rare, with most hardware procured being COTS hardware. Assurance of such equipment is well understood and therefore introducing a HWAL concept would provide little benefit at increased cost and is covered as part of the safety argument. **Impact:** Increased difficulty and cost of assurance for minimal assurance benefit over current practice. There is no requirement for the introduction of hardware assurance level.
response	*Noted*

Acknowledging the stakeholders' feedback from the NPA 2017-10 consultation, EASA will consider a separate rulemaking activity dedicated on the hardware assurance level requirements related to the assessment of changes to functional systems, where the comment will be taken into account.

comment *225* comment by: *NATS*

The suggested need for guidance for the assurance of complex hardware would be of limited use, albeit this type of hardware is more likely to be developed for ATM use.
Impact: Increased difficulty and cost of assurance for minimal assurance benefit over current practice.
Suggestion: There is no requirement for guidance regarding complex hardware.

response *Noted*

Acknowledging the stakeholders' feedback from the NPA 2017-10 consultation, EASA will consider a separate rulemaking activity dedicated on the hardware assurance level requirements related to the assessment of changes to functional systems, where the comment will be taken into account.

comment *270* comment by: *German NSA (BAF)*

Whereas Regulation (EC) No 482/2008 is applicable to providers of ATS and CNS services as well as entities providing ATFM and ASM for general air traffic this NPA proposes to expand software safety assurance through the back-door to encompass all providers of ATM/ANS including those currently not subject to 482 requirements. The extra effort for those service providers newly affected as of 2020 has not been evaluated at all.
In particular, it is not clear why this expansion is necessary.

response *Noted*

It should be noted that Regulation (EU) 2017/373 will be applicable from 2 January 2020. Considering also the feedback from this consultation, it was concluded that this extension to other service providers not addressed in Regulation (EC) No 482/2010 to use these means to demonstrate compliance would not affect significantly these other providers. On the other hand, the 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 must only be used when it is demonstrated that the safety objective set out in the Implementing Rules is met.

Additionally, the presented AMC & GM includes high-level principles for the software assurance process that should be achievable for any organisation where the software failure might have an impact on the service specification.

comment	*271* comment by: *German NSA (BAF)* Since none of the industry standards has been officially accepted as an AMC to Regulation (EC) No 482/2008 and since the NPA doesn't propose to do so either, the burden of negotiating / accepting approaches proposed by ATM/ANS providers to overcome the known deficiencies, gaps and weaknesses in each of the existing industry standards still lies with the CAs. It would have been helpful to propose standards which fully comply with the requirements set out in Regulation (EC) No 482/2008 and this NPA, respectively along with this NPA, to trigger harmonisation across Europe in that respect.
response	*Noted* The comment is duly considered. Currently, the software safety assurance systems of the ANSPs are compliant with Regulation (EC) No 482/2008 and under the oversight of the competent authorities. They are based on different software assurance standards (e.g. ED153, ED109A), already identified in the AMC & GM. Rather than defining a particular software assurance standard to be applied by all the EU ANSPs, the conclusion reached was that it would be better to keep today's flexibility that allows ANSPs to select the best suitable option and to ensure compliance with the provisions.

comment	*272* comment by: *German NSA (BAF)* Related to complex electronical hardware items BAF supports measures to develop AMC/GM in respect of hardware assurance.
response	*Noted* Acknowledging the stakeholders' feedback from the NPA 2017-10 consultation, EASA will consider a separate rulemaking activity dedicated on the hardware assurance level requirements related to the assessment of changes to functional systems, where the comment will be taken into account.

comment	*275* comment by: *CANSO* The structure of the guidance material leads to significant duplication of text that applies equally to service providers and ANSP sections, which could be presented more concisely. Impact: Duplication of text could lead to subtle unintended variations in compliance against similar requirements. Suggestion: Consider presenting guidance as applicable to both service providers and ANSPs in one section, and identifying differences at that level (rather than duplicating as currently)

response | *Noted*

EASA acknowledges the existing duplications, but this approach was preferred to keep the segregated set of requirements separately, depending on the type of service provider.

A recast of the order of the requirements at IR level and the associated AMC & GM could be considered at a later stage via a separate rulemaking activity.

comment | *276* comment by: *CANSO*

The term SWAL is used extensively in the NPA but no formal definition of it is provided. (EC) No 482/2008 mandated "a minimum of four software assurance levels shall be identified, with software assurance level 1 indicating the most critical level". Has this requirement been dropped intentionally?

Impact: The lack of a definition for software assurance levels potentially leads to inconsistency of approach by ANSPs complying with the guidance material and therefore requiring different assurance evidence from system suppliers for the same product.

Suggestion: Either:
Add definition of SWAL to Annex I of (EU) 2017/373
or provide guidance/requirements regarding software assurance levels to facilitate common software assurance requirements.

response | *Accepted*

Considering the comment, the text has been amended (please refer to ATM/ANS.OR.C.005(a)(2)).

comment | *277* comment by: *CANSO*

(EC) No 482/2008 had a clear requirement (Article 3, 1.) for an organisation to define and implement a software safety assurance system. A stated objective of this NPA (2.2) is to maintain the level of safety in the definition and implementation of the software assurance systems, yet there is no requirement, or even mention, in either (EU) 2017/373 or this NPA of a software (safety) assurance system.

Impact: The migration from (EC) No 482/2008 to (EU) 2017/373 + NPA has lost the requirement for implementation of a software (safety) assurance system.

Suggestion: Include a requirement equivalent to (EC) No 482/2008 Article 3, 1 and other associated requirements.

response | *Partially accepted*

The commented element is duly considered.

It is addressed by the combination of the new AMC & GM (for software aspects) with the existing AMC & GM, where all the software information is planned to be used as part of the safety (support) case(s) demonstration. It is noted that the AMC3 ATS.OR.205(a)(2) requests that 'the ATS provider should ensure the existence of documented software assurance process necessary to produce evidence and arguments that demonstrate that the software behaves as intended (software requirements), which level is consistent with the criticality of the required application'. The main change in the concept is that the software safety assurance system is intended to provide inputs to the safety (support) assessments.

comment *282* comment by: *Copenhagen Airport*

The most critical part of the NPA is based on the fact that ANSP providers apart from ATS no longer is supposed to produce a full safety case, thus the software assurance process
no longer is related to the full scope of what a malfunction related to software potential can cause in terms of safety occurrences since the process is cut into two. The ATS and CNS are related to two different safety management systems, thus the full picture is left for the NSA to combine!

Mostly all the engineering in regards to ATM/ANS functional system/services are defined as the specified functionality and the required safety specifications to it. These functional and safety specifications are defined and put in the specifications in the contract given to the manufacture when ordering software.
These specifications are based upon experience and result of a safety study in regards what a fault in a particular part of software can cause, thus the development, test and robustness verifications to the functionality should increase accordingly. A complicated verification and validation process provide by two the different observers ANSPs are foreseen - and will cause both the Providers and NSA a troublesome future.

The safety study should be developed by the combined effort from the involved providers (ATS,CNS) – neither the ATS provider nor the CNS provider is by themselves capable of fully to demonstrate the SWAL levels has been met, since the manufactures development process in regards to the assigned SWALL levels are not a simple figure but a combination of many arguments that combined forms the statement – "the system (software) is safe to put into operation"- and again relating to two different risc class specifications schemes.

response *Noted*

It should be highlighted that the already adopted IR as well as the already issued associated AMC & GM rely on the role of the ATS provider in order to set up the software requirements (and the associated assurance level) to be met by the system/equipment used by the ATS and non-ATS activities. Taking the example of the CNS provider mentioned in the comment, it is up to the ATS provider to establish those requirements for the CNS systems, which might be different from the use of

the same systems by another ATS provider, depending on the particular installation aspects.

The comment will be duly considered for further rulemaking developments.

comment *287* comment by: *ASD/Thales Air Systems*

A section with definitions of terms is missing:
What is:
- software criticality
- a safety support assessement
- safety support requirements
- previously developed software

response *Not accepted*

It should be highlighted that the NPA proposal relates to changes at the level of AMC/GM, while the proposal in the comment relates to an amendment at IR level, which is outside the scope of this consultation.

On the other hand, it was acknowledged that the term 'software criticality' was already used in Regulation (EC) No 482/2008 with no particular definition and no major concern was reported by stakeholders when showing compliance. The other referenced terms are considered either already described in the set of AMC & GM or of a general nature, so it is found that there is no need of a particular definition in the frame of this proposal.

comment *350* comment by: *UK CAA*

Attachments #1 #2

response *Noted*

All the comments were duly noted, evaluated and addressed.

Please refer to the specific comments in the CRD.

Furthermore, EASA appreciated the work performed by the commentator as it was recognised by EASA as a benefit to the subject rulemaking activity, which facilitated the review of the proposed set of AMC & GM.

comment *351* comment by: *Yves Rodenas*

ATC requirements as defined in ED73 are complex requirements with multiple options based on the aircraft characteristics and the development team targeted design.

Experience shows that it is not always evident for the development team and/or the certification authority to select the requirements associated with a specific transponder option.
This is a source of inefficiency during the development and certification process that may increase costs, development time and is a non-value added activity (each project development/certification team repeating the same process).

It would be beneficial to include an addendum to the requirements standard, linking each transponder option with its associated set of requirements. This could be done once for all development/certification teams. It would save valuable validation time on the requirements and would prevent possible implementation error (what requirements to implement based on the multiple options).

AIRplus Maintenance GmbH

response *Noted*

It is perceived that the comment refers to another document subject to consultation.

comment *354* comment by: *DWD*

General comment
The proposed new AMC/GM in order to include SWAL in Reg (EU) No 2017/373 introduces SWAL for MET SPs where previously the regulations did not specify this requirement. Thus, MET SPs cannot "continue with their existing SWAL systems as part of the safety (support) assessments" as written in Section 2.4 of NPA 2017-10. In order to allow MET SPs to fulfill this obligation in a meaningful manner, the AMC/GM should more clearly specify that SWAL is needed for safety critical software that is part of EATMN-software (in the sense of Reg (EU) 482/2008) or for software of an ANSP that provides direct input into EATMN-software.

Best regards,
Dorothea Banse

response *Noted*

The comment is duly considered.

It should be highlighted that in the current regulatory framework, 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 air traffic services (ATS), airspace management (ASM), air traffic flow management (ATFM), i.e. air traffic management (ATM) and communication, navigation, or surveillance (CNS). Additionally, the software aspects for aeronautical information services (AIS) provision are included in Regulation (EU) No 73/2010. On the other hand, it is acknowledged that the MET providers will be affected as regards the software assurance AMC & GM.

EASA considers that some of the service providers other than the ones that are subject to Regulation (EC) No 482/2008 today have a contribution to software (e.g. MET providers, FPD) and in order EASA to take an informed decision, a specific

meeting with other stakeholders was organised to address this issue (among others). The discussion clearly concluded that some features of the MET systems are affected by the current regulatory requirements, which also supports the approach taken for the proposed set of AMC & GM; that is, to apply for all service providers of ATM/ANS, including AIS and MET providers, towards software assurance level standardisation.

Procedural information p. 1

comment *266* comment by: *ASD/Thales Air Systems*

Please add Manufacturers as Affected stakeholders since they provide software and have to comply with the sw assurance level requirements.

response *Accepted*

2. In summary — why and what | 2.1. Why we need to change the rules — issue/rat p. 4-5

comment *2* comment by: *DFS Deutsche Flugsicherung GmbH*

We agree that hardware can be as complex as software, but just complexity is not the issue. The question is what can happen in case of a failure. In this matter software seems to be more critical as a malfunction can lead to wrong conclusions of the air traffic controller whereas hardware problems will most likely cause an outage, which is in most cases less critical.

Secondly, the introduction of HWALs (together with a “Hardware Assurance System”) can have a benefit, if it is possible to certify hardware aspects, which is very difficult.

In general, the assessment and assurance of hardware changes is included in ATS.OR.205 (a) since <u>all</u> notified changes are subject to that rule. (And according to ATM/ANS.OR.A.045 all changes of the functional system are to be notified).
Therefore, the assurance of electronic hardware items is covered by 2017/373. Knowledgeable support for establishing assurance processes could be given by developing appropriate ED-standard.

There are many other areas, e.g. “procedures”, where no specific assurance requirements exist in addition to 2017/373 and the relevant assurance is covered by the general safety assessment processes from ATS.OR.205.

Therefore, additional regulation for hardware assurance is not necessary!

response *Noted*

The comment is noted and duly considered in the assessment of the stakeholders’ views as regards the hardware assurance level (HWAL).

comment *27* comment by: *ENAIRE*

Reliability, Availability and Maintainability (RAM) analysis assess the HW features.
HW firmware is a SW type that is covered for SWAL (ED-153 is clear in this aspect).
Electronic hardware items are study as a part of the RAM analysis.
The HW delevop should include specification and test at the level that HWAL demmand when a "HWAL standard" is defined.

response *Noted*

The comment is noted and duly considered in the assessment of the stakeholders' views as regards the hardware assurance level (HWAL).

comment *57* comment by: *CANSO*

The so called "potential safety weakness as regards the safety assurance aspects when dealing with the safety support" assessment of changes to a functional system in ATM/ANS and other ATM network functions" might result from the complexity of understanding the Common Requirements, especially when software is involved. Most people misunderstand what is software.
Adding AMC's will not solve the complexity. A better definition of what is a software and its place within an equipment being part of a system would help in the application of the regulation

Proposal:
In Annex I (below), you will find a simple proposed approach to understand what is a software and how the regulation should be understood for a correct application.
Annex I: Considerations on Software:
What is a Software?
We will consider here the technical approach, the safety approach and how they can match.

1. **Technical approach**
Software is an *intangible* part of the equipment.
Software can't execute without an underlying hardware. The hardware is the *tangible* part of the equipment.
Software is not really measurable, quantifiable but its contribution to the behaviour of the equipment is.
Software is a *Versatile* way to change the behaviour of the equipment.
Versatility is :
- A strength.
- A huge weakness.

Engineering defines working methods to cope with the versatility in order to achieve:
- Goals to be fulfilled by the software.
- Reduce as much as possible unwanted behaviour.
Be careful that the technical approach often neglects functional approach

2. Safety approach
Software is an equipment constituent contributing in the realization of functions within a context.
Due to its nature, software reproduces exactly the same behaviour in the same circumstances.

Software is causal: When it fails to fulfil a function for a specific reason, it is always in the same way.
Software is a versatile way to change the behaviour of an equipment. To avoid this to become a weakness, any change must be done in a controlled way

How to have the assurance of a controlled production of software ?
---> Via a quality process with measurable assurance level

3. Understanding Regulation EC-482/2008 in a real world context: matching the technical and the safety approaches
We will use here EU-1035/2011 and EC-482/2008 for a better understanding of the problematic. Both are now repealed as they are part of EU-2017/373 .
With this in mind, we have the following consideration:
- EC-482/2008 is an extension of EC1035/2011 (System approach).
- Software Safety Assurance System is a part of System Safety Assurance.
- Whatever the change, an ANSP is required to implement a risk assessment and mitigation process (EC 1035/2011).
- EC 482/2008 describes what is required for software specific aspects of the changes. It has to be seen as some kind of plugin to the safety assurance system.
- By change, we understand corrections, modifications and projects

response

Noted

Considering that the proposed text would fall more within a training context, the AMC & GM are not amended.

comment

108 comment by: *ENAV*

The so called “potential safety weakness as regards the safety assurance aspects when dealing with the safety support” assessment of changes to a functional system in ATM/ANS and other ATM network functions” might result from the complexity of understanding the Common Requirements, especially when software is involved. Most people misunderstand what is software.
Adding AMC’s will not solve the complexity. A better definition of what is a software and its place within an equipment being part of a system would help in the application of the regulation

Proposal:
In Annex I (below), you will find a simple proposed approach to understand what is a software and how the regulation should be understood for a correct application.
Annex I: Considerations on Software:
What is a Software?
We will consider here the technical approach, the safety approach and how they can match.

1. **Technical approach**
Software is an *intangible* part of the equipment.
Software can't execute without an underlying hardware. The hardware is the *tangible* part of the equipment.

Software is not really measurable, quantifiable but its contribution to the behaviour of the equipment is.
Software is a *Versatile* way to change the behaviour of the equipment.
Versatility is :
- A strength.
- A huge weakness.

Engineering defines working methods to cope with the versatility in order to achieve:
- Goals to be fulfilled by the software.
- Reduce as much as possible unwanted behaviour.
Be careful that the technical approach often neglects functional approach

2. Safety approach
Software is an equipment constituent contributing in the realization of functions within a context.
Due to its nature, software reproduces exactly the same behaviour in the same circumstances.
Software is causal: When it fails to fulfil a function for a specific reason, it is always in the same way.
Software is a versatile way to change the behaviour of an equipment. To avoid this to become a weakness, any change must be done in a controlled way

How to have the assurance of a controlled production of software ?
---> Via a quality process with measurable assurance level

3. Understanding Regulation EC-482/2008 in a real world context: matching the technical and the safety approaches
We will use here EU-1035/2011 and EC-482/2008 for a better understanding of the problematic. Both are now repealed as they are part of EU-2017/373 .
With this in mind, we have the following consideration:
- EC-482/2008 is an extension of EC1035/2011 (System approach).
- Software Safety Assurance System is a part of System Safety Assurance.
- Whatever the change, an ANSP is required to implement a risk assessment and mitigation process (EC 1035/2011).
- EC 482/2008 describes what is required for software specific aspects of the changes. It has to be seen as some kind of plugin to the safety assurance system.
- By change, we understand corrections, modifications and projects

response

Noted

Considering that the clarifications would fall more within a training context, the AMC & GM are not amended.

comment

136 comment by: *LFV*

An introduction of HWAL will most probably increase the cost for HW and decrease the competition in HW manufacturing. Since the process of HW development and verification is mature, EASA should evaluate if the benefit of an introduction of HWAL justifies the cost.

response *Noted*

Acknowledging the stakeholders' feedback from the NPA 2017-10 consultation, EASA will consider a separate rulemaking activity dedicated on the hardware assurance level requirements related to the assessment of changes to functional systems, where the comment will be taken into account.

comment *153* comment by: *DSNA*

"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."

The NPA is mentioning HWAL. It is premature to invoke HWAL where the ATM community is being doing quite a hard job to educate to SSAS. So, we are not in favour of addressing HWAL in AMC/GM.

response *Noted*

Acknowledging the stakeholders' feedback from the NPA 2017-10 consultation, EASA will consider a separate rulemaking activity dedicated on the hardware assurance level requirements related to the assessment of changes to functional systems, where the comment will be taken into account.

comment *184* comment by: *AESA/DSANA*

Hardware assurance (HWAL), if regulated, should be integrated with SW assurance (SWAL) and procedures assurance (PAL) as long as only the combination of the three perform each ATM/ANS function and all complement each other.
The hardware assurance regulation shall have the same level of detail than SW assurance as long as me electronic hardware items include nowadays its own software.

In response to "(…) 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."

response *Noted*

Acknowledging the stakeholders' feedback from the NPA 2017-10 consultation, EASA will consider a separate rulemaking activity dedicated on the hardware assurance level requirements related to the assessment of changes to functional systems, where the comment will be taken into account.

comment *267* comment by: *ASD/Thales Air Systems*

Regarding hardware assurance, a PIA with cost-benefit analysis seemes necessary to evaluate the expected added value. Indeed, the question is: what is the proportion

of electronic hardware items in the equipment covered by regulation (EU) 2017/373? In software-intensive systems, hardware is usually COTS and is covered by the current safety assurance practices and the main industrial standards. This question needs dedicated discussion (workshop, group, ...) with appropriate stakeholders, and industry is one of them.

response *Noted*

Acknowledging the stakeholders' feedback from the NPA 2017-10 consultation, EASA will consider a separate rulemaking activity dedicated on the hardware assurance level requirements related to the assessment of changes to functional systems, where the comment will be taken into account.

comment *278* comment by: *CANSO*

"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."

The NPA is mentioning HWAL. It could be premature to invoke HWAL where the ATM community is being doing quite a hard job to educate to SSAS. However, CANSO is open for discussion about how to address HWAL in order to improve its maturity.

response *Noted*

Acknowledging the stakeholders' feedback from the NPA 2017-10 consultation, EASA will consider a separate rulemaking activity dedicated on the hardware assurance level requirements related to the assessment of changes to functional systems, where the comment will be taken into account.

comment *352* comment by: *DWD*

"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 that establishes a software safety assurance system to be implemented by ATM/ANS providers."

Comment: Regulation (EC) No 482/2008 establishes a software assurance system to be implemented by ATS, ATFM, ASM and CNS providers. It does not establish such a system for MET SPs, which are also ANSP. Hence, the wording is misleading and should be corrected.

response *Accepted*

Considering the comment, the text has been amended to promote clarity.

2. In summary — why and what | 2.2. What we want to achieve — object p. 6

comment

79 comment by: *Swedish Transport Agency, Civil Aviation Department (Transportstyrelsen, Luftfartsavdelningen)*

This might not be the right place for this comment, but this is as good as it gets. In some countries, such as Sweden thera are alot of small service providers that benefit from exemptions to some requirements with current regulation. These are typically small regional airports that carry the own ANS certificates för ATS, MET and/or CN, the ATS service provided are predominantly AFIS but can be ATC and infrastructurevise they provide only basic equippage and with few, very few movements. nad yet provides an important service to the community.

We argue that it could be worth concidering criteras to exempt some ANSPs from these requirements, as thay today are exempted from some requirements in 1035/2011 as there are limited benefits to impose these requirements on such ANSPs.

response

Noted

EASA has duly assessed the comment.

No amendment is considered necessary to address the comment as it is mainly focusing on the applicability of safety vs safety support assessment principles and activities.

2. In summary — why and what | 2.3. How we want to achieveit — overview of the propo p. 6

comment

353 comment by: *DWD*

“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 and 1035/2011) define the ‘functional system’ as a combination of systems, procedures and human resources organised to perform a function within the context of ATM/ANS.”

Comment: The definition in Regulations (EU) Nos 1034/2011 and 1035/2011 specifies functional systems only for ATM:

· Reg (EU) No 1035/2011, Article 2:

(3)	‘functional system’ means a combination of systems, procedures and human resources organised to perform a function within the context of ATM;

The new Commission Implementing Regulation (EU) No. 2017/373 introduces functional systems for ANS

response

Noted

2.3.1. Proposed amendments to Subpart A 'General requirements' of Annex III 'AMC/GM to Part- ATM/ANS.OR — Common requirements for service pr p. 6-7

comment *176* comment by: *The Boeing Company*

Page: 6
Paragraph: 2.3.1

The proposed text states:
"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."

Requested change: We request that EASA specify which software is being referenced; the software used in house for production, or the software used in products delivered to the customer.

Justification: Clarification.

response *Noted*

The referenced software corresponds to the part of the functional system that is used by the ANSP for the service provision. Then, it would fall under the second option identified by the commentator.

comment *185* comment by: *AESA/DSANA*

It should be clearly stated in the NPA what documentation shall be provided by each type of service provide and the relationship between them:
- ATS providers produce Risk Assessments.
- Non- ATS providers produce Assurance Arguments able to support the Risk Assessments, as long as non-ATS providers may not be aware of the safety aspects of the ATS provider using their services.

Regulation is needed to support the NSAs to demand the correct documentation from each service provider type.

response *Noted*

The comment is duly noted and will be considered under a future rulemaking activity as it is outside the scope of the commented proposal.

comment *186* comment by: *AESA/DSANA*

What is it to be understood by criticality? Is the service provider the only responsible for its determination or should it be agreed with the NSA? A definition for " criticality of the software " is needed.

This is an issue which could be controversial and now seems a key factor to decide the depth od revision.

response *Not accepted*

The term 'software criticality' was already used in Regulation (EC) No 482/2008 with no particular definition and no major concern was reported by stakeholders when showing compliance. Therefore, no amendments to the text are introduced in this context.

comment *187* comment by: *AESA/DSANA*

In section 2.3.1 it is suggested to review the proposed GM2 ATM/ANS.OR.A.045(a), and to include a new AMC, in order to clearly establish, as it is said in the rationale of 2.3.1, that "the service provider is required to produce an assurance argument whether or not it is to be reviewed by the competent authority". This statement is not really found in the referred new GM.

It should be explictly stated in this NPA that the service providers should produce a SW assurance argument in order to demonstrate that the level of safety after a SW-related functional change will continue to be safe.

response *Noted*

The comment is duly considered.

It should be noted that the software is part of the functional system and the software assurance argument should be considered as a contributor to the functional system safety argument. It is noted that for non-ATS providers, the argument will be a safety support argument, focusing on the service requirements.

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 requirement p. 7

comment *109* comment by: *ENAV*

We propose to insert a new section "Coordination between ATS Service Provider and SW industry" in order to define the interactions between the Service Provider and the SW industry.

For example, can the SW industry propose a less restrictive SWAL and how can the SW industry justify it?

response *Noted*

The software assurance aspects are established at service provider level, as it is today regulated with Regulation (EC) No 482/2008.

In most of the cases, the ANSPs do not develop the software of their systems, thus, the coordination with the industry already exists.

In the example mentioned, the SW industry can propose a less restrictive SWAL that could lead to two possible situations:

1) it is not acceptable for the intended use; or

2) the ANSP modifies the conditions of usage of the affected equipment (adding mitigation techniques) in order to be able to make use of this lower SWAL equipment.

However, the coordination activities are necessary for the SWAL allocation, but also for the functionalities inside the equipment.

Consequently, the comment does not result in amendment to the proposed AMC & GM.

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 ser p. 7

comment *47* comment by: *CANSO*

We propose to insert a new section "Coordination between ATS Service Provider and SW industry" in order to define the interactions between the Service Provider and the SW industry.

For example, can the SW industry propose a less restrictive SWAL and how can the SW industry justify it?

response *Noted*

The software assurance aspects are established at service provider level, as it is today regulated with Regulation (EC) No 482/2008.

In most of the cases, the ANSPs do not develop the software of their systems, thus, the coordination with the industry already exists.

In the example mentioned, the SW industry can propose a less restrictive SWAL that could lead to two possible situations:

1) it is not acceptable for the intended use; or

2) the ANSP modifies the conditions of usage of the affected equipment (adding mitigation techniques) in order to be able to make use of this lower SWAL equipment.

However, the coordination activities are necessary for the SWAL allocation, but also for the functionalities inside the equipment.

Consequently, the comment does not result in amendment to the proposed AMC & GM.

2.4. What are the expected benefits and drawbacks of the proposals p. 7-8

comment *132* comment by: *LFV*

The NPA states that "service providers can continue with their existing SWAL systems … and hence, there are no drawbacks identified. … For this reason, no RIA has been developed for this task."
But an important change with NPA 2017-10 is that it covers all ATM/ANS services, while current requirements for software assurance only covers ATS, ATFM, ASM and CNS services.
For the "new" services covered by software assurance requirements, NPA 2017-10 might cause a considerable change, both for the service providers and for the system suppliers, why a RIA should be performed.

response *Noted*

EASA agrees that in the current regulatory framework, 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 air traffic services (ATS), airspace management (ASM), air traffic flow management (ATFM), and communication, navigation, or surveillance (CNS).

On the other hand, it should be noted that the software aspects for aeronautical information services (AIS) provision are included today in Regulation (EU) No 73/2010.

Consequently, the applicability of the proposed AMC & GM on software assurance would be novelty only for MET providers and DAT providers — the latter ones partially.

In this context, it should be considered also that AMC serve as a means by which the requirements contained in the IRs can be met. However, applicants may decide to show compliance with the requirements using other means and may propose an alternative means of compliance, based, or not, on those issued by the Agency. These alternative means of compliance (AltMoC) must only be used when it is demonstrated that the safety objective set out in the implementing rules, i.e. Regulation (EU) 2017/373 applicable also for MET providers, is met.

In conclusion, EASA performed a regulatory impact assessment (RIA) for a number of key regulatory developments proposed in NPA 2014-13 'Requirements for safety assessment of changes to ATM/ANS functional systems' and it addressed the impact

of changes affecting software (applicable also for MET providers) and Regulation (EC) No 482/2008.

Therefore, no RIA was developed with NPA 2017-10.

3.1. Draft AMC/GM p. 9

comment *236* comment by: *UK CAA*

Attachment #3

Page No: 9 to 19

Paragraph No: 3.1. Draft acceptable means of compliance and guidance material

Comment: We believe the proposed text duplicates AMC/GM already published in Regulation (EU) 2017/373. We are of the opinion that this has the potential to lead to inconsistent implementation of the related elements of Regulation (EU) 2017/373 amongst Member States. We strongly urge that the AMC/GM is not published. Instead, we strongly recommend that the approaches foreseen on CRD 2014-13 Issue 2 (see below), should be actively pursued as soon as possible.

· **Response to various comments in 'section 2. Explanatory Note — 2.4. Overview of the proposed amendments — 2.4.2. Proposed amendments to Article 8 'Transitional provision', Article 9 'Repeal' and Article 10 'Entry into force' in the Cover Regulation' (Pgs 97 – 125):** *"The work still to be done on the AMC/GM will address those elements of Regulation (EC) No 482/2008 which are not currently transposed and that contribute to ensuring safety of the software elements of the change. AMC/GM will also be provided in the future on how the rules may be applied in the other disciplines (i.e. hardware, people and procedures)"*

· **Response to comments 186 & 257 in 'section 4. Regulatory Impact Assessment (RIA) — 4.7. Changes affecting software and Regulation (EC) No 482/2008':**
"It is also acknowledged that the assurance of people, procedures and hardware is not fully covered. This will be tackled in the 2nd NPA and by future additions to the AMC/GM"

Justification: One of the objectives of the Regulation (EU) 2017/373 rulemaking group was to remove the need for Regulation (EC) 482/2008 (see Regulation (EU) 2017/373 - recital 19). It was held that Regulation (EC) 482/2008 gave undue importance (and inappropriate legislative status) to the assurance of software over that of People, Procedures and Hardware, which are responsible for the vast majority of safety occurrences in the CNS/ATM domain.

The 482/2008 content required to instantiate an assurance system that adequately covered People, Procedures and Hardware as well as software has already been included in Regulation (EU) 2017/373 and its supporting AMC and the GM (see Appendix II of NPA 2014-13).

NPA 2017-10 is considered contrary to these objectives. It introduces clauses specifically related to software that imply differences between the assurance of software and the assurance of People, Procedures and Equipment (hardware & software). These differences do not exist and we believe implying that they do is harmful to harmonisation. Consequently the proposals in NPA 2017-10 are unnecessary as they duplicate the IR, AMC and GM already provided with Regulation (EU) 2017/373.

It was recognised that guidance on assurance was insufficiently addressed by NPA 2014-13, however this did not result in a need for more specific software assurance guidance. Instead, guidance appropriate for People, Procedures and Equipment (hardware & software) was required to ensure harmonisation of the approach. See CRD 2014-13 Issue 2 responses to comments 186 and 257, and the explanatory note to Opinion No 03/2014 (*"Based on the consultation, it has been concluded that Regulation (EC) No 482/2008 can be repealed, but certain provisions should be moved to AMC. When the Agency completes the AMC/GM, these aspects will be addressed"*). This does not imply an additional NPA, rather it refers to changes to be made to the draft AMC/GM material prior to the decision (i.e. ED Decision 2017/001/R), which result from addressing comments in the CRD. Consequently these changes have already been addressed.

Additional material duplicating extant AMC/GM confuses the harmonised approach to regulating people, procedures and equipment. It implies differences that do not in fact exist, and encourages divergent local developments (see attached table). Such divergence will result in differences in interpretation and potentially cause disputes between competent authorities and service providers.

Proposed Text: Delete duplicated amendments proposed in section 3.1. Instead it is strongly recommended that EASA should consider the need to establish a rulemaking task to progress the assurance of People, Procedures and Equipment (hardware & software) in a more coherent and harmonised manner as proposed for the 2nd NPA, as described in CRD 2014–13 Issue 2.

response *Noted*

This rulemaking activity was based on a specific request from several competent authorities during the Comitology process of Regulation (EU) 2017/373. It was identified that in the existing set AMC & GM, there are no AMC & GM on the functional system aspects, especially in the software domain.

EASA concurs with the commentator's view on the need to address the other components of the functional system (hardware, procedures and people), which issues will be addressed through a different rulemaking task, in the future.

comment *294* comment by: *UK CAA*

Page No: 9 to 19

Paragraph No: 3.1. Draft acceptable means of compliance and guidance material

Comment: We are of the view that placement of Assurance Levels and SWALs at IR/AMC levels is inappropriate. In addition, that both are inadequately and inappropriately defined in the NPA is cause for concern to the UK CAA.

Justification:
Assurance Levels are very complex to define and use. When used correctly they are an expression of the confidence held in an element of a specification. Consequently, an element of a specification would have one or more Assurance Levels associated with it to express the confidence held in the various attributes of the element (e.g. reliability, accuracy, timing, robustness, etc).

As International Electrotechnical Commission (IEC) standard 61508: Functional Safety - 2010 is the only assurance standard that addresses all of the attributes of a specification, the use of any other assurance standards will require multiple types of Assurance Levels to facilitate the cross referencing to different standards (and note that, whilst IEC 61508 addresses all attributes, it does not address how they are related to risk as this is not considered technically possible). Due to the diversity of solutions available this is not a topic for legal material nor does the proposed material in the NPA address the problem adequately.

The requirements for SWALs from Regulation (EC) 482/2008 were deliberately omitted from Regulation (EU) 2017/373 as they were inadequately and inappropriately defined (see justification in Section 6.2. – Appendix II of NPA 2014-13). However, it was accepted that some assurance level material that relates assurance levels to confidence (an undefined concept that this NPA tries to use without defining but needs to address) for People, Procedures and Equipment (hardware & software) and not just software might be introduced as GM in the future and it is this that is proposed to be done in 'NPA 2'.

Furthermore, the argument for the removal of SWALs was challenged but not upheld in CRD 2014-13 Issue 2 and no subsequent evidence has been subsequently provided showing this argument to be flawed. See CRD 2014-13 Issue 2 responses to comments 186 and 257.

Moreover:

- the proposed material does not address the inadequacies described above
- such material should only be considered for GM.
- the meaning of SWALs is unfortunately, and inappropriately, ambiguous. It is unclear whether they are meant to be an expression of confidence in achieving a claim or effort expended in providing evidence.
- SWALs are not associated with any fixed objective or quantitative scale, their relationship to confidence is undefined, consequently they neither benefit harmonisation nor standardisation.

Proposed Text: Delete proposed amendments relating to SWALs and assurance levels proposed in section 3.1 as follows:

Reference to SWALs in the following should be removed:

· AMC5 ATM/ANS.OR.C.005(a)(2)
· GM1 to AMC6 ATM/ANS.OR.C.005(a)(2)

· GM2 to AMC6 ATM/ANS.OR.C.005(a)(2)
· GM3 to AMC6 ATM/ANS.OR.C.005(a)(2)
· GM1 to AMC4 ATS.OR.205(a)(2)
· GM2 to AMC4 ATS.OR.205(a)(2)
· GM3 to AMC4 ATS.OR.205(a)(2)

Reference to assurance levels in the following should be removed:

· AMC5 ATM/ANS.OR.C.005(a)(2)
· GM1 to AMC6 ATM/ANS.OR.C.005(a)(2)
AMC3 ATS.OR.205(a)(2)

response *Not accepted*

EASA agrees that there is no universal definition of assurance level, but the available industrial software standards make the link between the assurance levels and the activities (objectives) to be performed in order to gain the claimed confidence. When comparing different available software standards, there is a high degree of correlation between the different sets of assurance levels.

The software assurance level is an expression of confidence, including all the phases of the software development and verification activities. This is not quantitative, as quantitative aspects are not fully aligned with the software domain. On the other hand, the assurance level is widely used by the software development industry and ANSPs to cope with the possible contribution of the software to the different system failure conditions.

comment *295* comment by: *UK CAA*

Page No: 9 - 19

Paragraph No: 3.1. Draft acceptable means of compliance and guidance material

Comment: The existing AMC and GM to Regulation (EU) 2017/373 provides a harmonised approach to the assurance of People, Procedures and Equipment (hardware & software). We believe NPA 2017-10 inappropriately identifies the assurance of software as a special case and in doing so conflicts with AMC/GM already published in support of Regulation (EU) 2017/373. Additionally, we are of the view that NPA 2017-10 is ambiguous, inconsistent and incorrect and causes the UK CAA significant concern.

Justification:
A) NPA 2017-10 does not appear to conform to the concepts established in Regulation (EU) 2017/373, namely:

1. Procedures are approved prior to change and are intended to cover many changes, consequently they may be approved as part of the MS approval.

2. Assurance cases are provided for each change and contain arguments about that change only.

3. Assurance cases argue the product properties not the goodness of the procedures (it is a false argument that claims the product is safe/trustworthy because approved procedures have been followed (process evidence may be used as backing but is not prime).

4. Service providers other than ATS providers have no view of safety and so cannot use or create safety requirements, safety criteria or assurance levels related to safety. Regulation (EU) 2017/373 states that only ATS providers can actively intervene in an unsafe situation, only they can establish safety requirements and criteria. Other service providers cannot directly intervene in an unsafe situation and hence merely have requirements. This is reflected in the structure of Regulation (EU) 2017/373, namely Annex III and Annex IV,

Consequently, we suggest that the following NPA2017-10 proposals are invalid and/or impracticable:

· **GM2 ATM/ANS.OR.A.045(a)**

It is impracticable for the CA to agree the depth of safety assurance for every change. We are notified of over 1500 changes per year in UK

· **GM1 ATM/ANS.OR.A.050**

The assessment of the application of assurance processes (whether for software or any other part of the functional system) is performed as part of the assessment of the assurance cases and is governed by ATM/ANS.OR.C.005. Moreover the assurance case would be invalid if it did not contain all the necessary evidence or the evidence was inconsistent.

If it were felt necessary to highlight this co-operation it would have to include all regulatory interaction governed by the IR.

· **AMC6 ATM/ANS.OR.C.005(a)(2)**

We believe **t**his is in the wrong section. Processes are dealt with in ATM/ANS.OR.B.010.

This section appears to go against the fundamental philosophy of Regulation (EU) 2017/373, which sets objective criteria for judging the behaviour of the change to the system, as opposed to this AMC, which tries to judge the behaviour of the system from the process followed.

· **AMC6 ATM/ANS.OR.C.005(a)(2), (a)**

It is not possible for ANSPs to construct a logical argument as to why their procedures will, in all circumstances, achieve the 5 objectives listed. It adds no value if a valid assurance case has been provided. In addition, **t**his section appears to go against the fundamental philosophy of Regulation (EU) 2017/373, which is to set objective criteria for judging the behaviour of the change to the system, as opposed to this AMC, which tries to judge the behaviour of the system from the process followed.

· **AMC6 ATM/ANS.OR.C.005(a)(2), (a)(2)(ii)**

We believe this is incorrect. There is no view of safety in Annex III text.

· **AMC6 ATM/ANS.OR.C.005(a)(2), (a)(3)**

We believe this is incorrect. There is no view of safety in Annex III text.

· **AMC6 ATM/ANS.OR.C.005(a)(2), (c)**

The evidence and arguments described in (c) cannot contribute to the argument in (a), which is about the software assurance processes.

· **AMC6 ATM/ANS.OR.C.005(a)(2), (f)**
We believe this is incorrect: There is no view of safety in Annex III text.

· **GM1 to AMC6 ATM/ANS.OR.C.005(a)(2), (b)**
This implies a relationship between ATSP and other ANSPs that is not required by the rule text. The rule text does not require the ATSP to provide the ANSP with a SWAL. In fact it deliberately isolates the two parties.

· **AMC4 ATS.OR.205(a)(2)**
This section appears to go against the fundamental philosophy of Regulation (EU) 2017/373, which sets objective criteria for judging the behaviour of the change to the system, as opposed to this AMC, which tries to judge the behaviour of the system from the process followed.

· **AMC4 ATS.OR.205(a)(2), (a)**
It is not possible for ANSPs to construct a logical argument as to why their procedures will, in all circumstances, achieve the 5 objectives listed. This is why the safety cases have to be reviewed in addition to the processes that create them.

· **GM1 to AMC6 ATM/ANS.OR.C.005(a)(2), (a)**
We believe this is incorrect. Criticality in Annex III is not related to safety criticality because safety is outside of the scope of Annex III.

· **GM2 to AMC6 ATM/ANS.OR.C.005(a)(2), (a)**
There can be no foreseen criticality of the software as this will depend upon the air traffic service that uses it. Different services of different criticality may use the same software. Rules in Annex III can only require the confidence in the software's behaviour to be specified.

· **GM2 to AMC6 ATM/ANS.OR.C.005(a)(2), (b)**
We believe this is incorrect: the severity of the effect for the user cannot be known by the supplier, to any degree of certainty because by definition they do not have sight of safety.

· **AMC4 ATS.OR.205(a)(2), (b)**
The evidence and arguments described in (c) cannot contribute to the argument in (a), which is about the software assurance processes.

B) Elements of NPA 2017-10 are considered ambiguous. It uses many undefined terms and concepts. Additionally there are several ambiguous grammatical constructs. Numerous elements can be interpreted in several different ways; consequently, we are of the opinion that the proposals as presented have the potential to result in disparate approaches between ANSPs and Competent Authorities within and across states. Such ambiguities appear as follows:

· **AMC5 ATM/ANS.OR.C.005(a)(2), (b)**
As SWALs and Rigour are undefined, any judgements made about the behaviour in order to provide such feedback will be subjective and not only vary within an

organisation but vary from ANSP to ANSP. Consequently requiring such feedback is meaningless. It would only work if the CA harmonised all ANSP's schemes, an unrealistic expectation.

· **GM2 ATM/ANS.OR.A.045(a)**
This statement is considered ambiguous. The criteria for measuring the complexity of the change are not defined.

· **AMC6 ATM/ANS.OR.C.005(a)(2), (d)**
The processes can identify a need that may or may not be satisfied. If unsatisfied the user system will have to be redesigned. It is considered ambiguous because it is not clear whether it relates to the processes or the software itself. Furthermore it is incorrect because if it means software itself, it's inconsistent with (a) and if it means processes, it's impossible.

· **GM2 to AMC6 ATM/ANS.OR.C.005(a)(2)**
This is considered ambiguous because there are no criteria for (a), (b), (c) or (d) and hence it has no value as GM. Moreover there are no requirements for a SWAL allocation scheme. This undermines harmonisation as each ANSP across Europe will have a different scheme.

· **GM3 to AMC6 ATM/ANS.OR.C.005(a)(2)** This is considered an ambiguous statement. Safety Critical software is an undefined term that has been abandoned since 1990; it is considered impossible to define. It is suggested that it would be unproductive to try to define it as all previous attempts by the safety engineering community have failed to do so.

· **AMC3 ATS.OR.205(a)(2), (b)**
As the definition of SWALs and Rigour is left to individual service providers, any judgements made about the behaviour in order to provide such feedback will be subjective and not only vary within an organisation but vary from ATSP to ATSP. Consequently requiring such feedback brings no value to the process. It would only work if the CA harmonised all ATSP's schemes, an unrealistic expectation on the CAs, due to the resource required.

· **GM1 to AMC4 ATS.OR.205(a)(2), (a) & (b)**
Use of the term 'criticality of the software' is meaningless as software criticality is undefined

· **GM1 to AMC4 ATS.OR.205(a)(2), (c)(1)**
This is considered an ambiguous statement, software criticality is an undefined term

· **GM2 to AMC4 ATS.OR.205(a)(2)**
This is considered ambiguous because there are no criteria for (a), (b), (c) or (d) and hence it has no value as GM. Moreover there are no requirements for a SWAL allocation scheme. This undermines harmonisation as each ANSP will have a different scheme

· **GM3 to AMC4 ATS.OR.205(a)(2), (a) This is considered an ambiguous statement. Safety Critical software is an undefined term**

C) NPA 2017-10 is considered inconsistent in the following respects:

· **GM1 to AMC6 ATM/ANS.OR.C.005(a)(2), (c)**
This clause implies that multiple SWALs have already been introduced. They have not.

· **GM1 to AMC6 ATM/ANS.OR.C.005(a)(2), (d)**
This guidance is inconsistent with itself. It states that 'if processes do not exist use processes'. Moreover, it is generally accepted that there is no evidence that arguments and evidence cannot be provided for these types of software. Confidence does not depend on SWAL so there is no conflict between the requirement for confidence (ATM/ANS.OR.205(a)(2)) and the type of software.

D) NPA 2017-10 is considered incomplete and incorrect. It does not correctly explain the relationship between assurance standards and their use with safety cases and safety support cases. Furthermore the NPA is incomplete as it does not make it clear that the safety assurance standards listed need to be instantiated for the change and the change safety case that uses them. Nor does it make clear that the assurance standards listed do not address all of the attributes that are required to be addressed by Regulation (EU) 2017/373. Incompleteness and/or error has been identified as follows:

· **AMC5 ATM/ANS.OR.C.005(a)(2), (b)**
Incorrect reference: there is no requirement for SWALS, they are introduced only in GM.

· **AMC6 ATM/ANS.OR.C.005(a)(2), (a)(2)(i)**
The content is incorrect – tautology. Not specific to software. However, it is covered by: AMC2 ATM/ANS.OR.C.005(a)(2), (d) where it is correct.

· **AMC6 ATM/ANS.OR.C.005(a)(2), (f)**
Incorrect, this clause is not a requirement as it uses the word 'should' and provides no criteria for 'particularities' or what is to be done for these particularities. This is more appropriate as GM rather than AMC. The rule itself is adequate as it covers this and is not specific to software.

· **AMC6 ATM/ANS.OR.C.005(a)(2), (f)**
Incorrect, It is not a requirement as it uses the word 'should' and provides no criteria for 'sufficient'. This is more appropriate as GM rather than AMC. The rule itself is adequate as it covers this and is not specific to software.

· **GM1 to AMC6 ATM/ANS.OR.C.005(a)(2), (a)**
Incorrect reference – should be ATM/ANS.OR.C.005(a)(2).

· **GM1 to AMC6 ATM/ANS.OR.C.005(a)(2), (a)**
Undefined concept (relating confidence to rigour). In addition, **'**Software criticality' is undefined.

· **GM1 to AMC6 ATM/ANS.OR.C.005(a)(2), (a)**
The relationship between rigour and confidence is undefined and in a safety support case rigour does not imply correctness. A SWAL allocation scheme can only provide

a link between criticality and assurance processes. The appropriateness of the rigour of process followed and the robustness of the assurance data generated can only be judged for its adequacy with reference to the safety support case that uses it.

· **GM1 to AMC6 ATM/ANS.OR.C.005(a)(2), (b)**
It is not clear that in "many changes" the safety support case is written from the perspective of a non-ATS provider being a subcontractor of the ATS provider and, no guidance is provided for the case where the safety support case has been generated without knowledge of the level of confidence required of the specification. Guidance for both cases is already provided in GM Section 3.3. Multi Actor View. The GM in NPA 2017-10 therefore is considered incomplete and incorrect, and it contradicts the guidance already provided. Furthermore, while the confidence in the claim for a property of a service that is assured in a safety support case should be the same as the confidence required of that property in the safety case, there may be no relationship between the SWAL schemes used for the assurance of safety and the assurance of trustworthiness.

· **GM1 to AMC6 ATM/ANS.OR.C.005(a)(2), (c)**
We believe this is unworkable as the text allows each ANSP to declare their own SWALS and processes. If SWALS are to be used they have to be harmonised, at the European level, to be useable, as intended by NPA 2017-10, by industry. There is no evidence that rigour relates to correctness and neither is there any evidence that these criteria affect rigour. Rigour is undefined and the need for this is unexplained and is considered unjustified. It is questioned where these three classes have come from – as there appears to be no justification.

· **GM2 to AMC6 ATM/ANS.OR.C.005(a)(2), (a)**
There is no direct relationship between the rigour required and criticality. This is a false relationship. Rigour should be related to the difficulty in arguing the satisfaction of a requirement to a given level of confidence and not to its criticality. Furthermore, in this instance, a requirement may relate to criticality but this will be unknown to a service provider other than an ATS provider. Whilst SWALs are related to software practices whose aim is to increase confidence, the relationship between rigour and confidence is undefined and may or may not be relevant to the assurance being made.

· **GM3 to AMC6 ATM/ANS.OR.C.005(a)(2)**
We believe these standards do not satisfy the rule text well and suggest that IEC 61508 Functional Safety 2010 would be far better. It covers the same scope as the regulation and addresses People, Procedures and Equipment (hardware & software). Also as a multi sector standard it is more likely to be used by the ATM/CNS supply chain better.

· **AMC3 ATS.OR.205(a)(2), (b)**
This is not a correct statement. There is no requirement for assurance levels in (EU) 2017/373

· **AMC4 ATS.OR.205(a)(2), (c)**
We believe this cannot work in practice as the text allows each ANSP to declare their own SWALS and processes. If SWALS are to be used they have to be harmonised, at least at the state level, to be useable by industry. There is no evidence that rigour

relates to correctness and neither is there any evidence that these criteria affect rigour. Rigour is undefined and the need for this is unexplained in NPA 2017-10 and is therefore considered unjustified. The origin of these three classes is unclear, nor are the clauses justified in NPA 2017-10.

· **AMC4 ATS.OR.205(a)(2), (e)**
It is not possible to define a process that guarantees to provide sufficient confidence for all safety cases. This is why assurance standards have to be instantiated for particular changes. This needs to be argued in the safety case.

· **GM1 to AMC4 ATS.OR.205(a)(2), (a)**
Incorrect reference – should be ATS.OR.205(a)(2)

· **GM1 to AMC4 ATS.OR.205(a)(2), (b)**
SWALs are related to software practices whose aim is to increase confidence. The relation between rigour and criticality whilst required by NPA 2017-10 is undefined and may or may not help in providing sufficient confidence for the argument being made.

· **GM1 to AMC4 ATS.OR.205(a)(2), (c)(1)**
There is no direct relationship between the rigour required and criticality. This is a false relationship. Rigour should be related to the difficulty in arguing the satisfaction of a requirement to a given level of confidence and not to its criticality. Furthermore, the criticality will already have been expressed in setting the requirement as a level of confidence. Whilst SWALs are related to software practices whose aim is to increase confidence, the relation between rigour and confidence is undefined and may or may not be relevant to the assurance being made.

· **GM1 to AMC4 ATS.OR.205(a)(2), (c)(2)**
We believe this is unworkable in practice as the text allows each ANSP to declare their own SWALS and processes. If SWALS are to be used they have to be harmonised, at least at the state level, to be useable by industry. There is no evidence that rigour relates to correctness and neither is there any evidence that these criteria affect rigour. Rigour is undefined; the need for this is unexplained in NPA 2017–10 and is therefore considered unjustified. It is questioned where these three classes have come from – there appears to be no justification.

· **GM1 to AMC4 ATS.OR.205(a)(2), (d)**
There is no evidence that arguments and evidence cannot be provided for these types of software. Confidence does not depend on SWAL so there is no conflict between the requirement for confidence (ATM/ANS.OR.205(a)(2)) and the type of software.

· **GM2 to AMC4 ATS.OR.205(a)(2)**
Incorrect. There is no requirement for SWALs in Regulation (EU) 2017/373.

· **GM2 to AMC4 ATS.OR.205(a)(2), (a) & (b)**
Neither rigour nor software criticality are defined and neither is the purpose of relating one to the other. There is no direct relationship between the rigour required and criticality. This is a false relationship. Rigour should be related to the difficulty in arguing the satisfaction of a requirement to a given level of confidence and not to its

criticality. Furthermore, the criticality will already have been expressed in setting the requirement as a level of confidence. Whilst SWALs are related to software practices whose aim is to increase confidence, the relationship between rigour and confidence is undefined and may or may not be relevant to the assurance being made.

· **GM2 to AMC4 ATS.OR.205(a)(2), (d)**
This is considered incorrect. Software criticalities for ATSPs are harm based while those for non ATSPs are trustworthiness based. They are not comparable so there can be no notion of consistency. Additionally the rigour and confidence required of the safety case is not dictated by the rigour and confidence provided by the safety support cases.

· **GM3 to AMC4 ATS.OR.205(a)(2)**
We believe these standards do not satisfy the rule text well and suggest IEC 61508 Functional Safety 2010 would be far better. It covers the same scope as the regulation and addresses People, Procedures and Equipment (hardware & software). Also as a multi sector standard it is more likely to address the ATM/CNS supply chain better.

Proposed Text: It is strongly recommended that the following proposed texts are withdrawn:
· AMC5 ATM/ANS.OR.C.005(a)(2)
· AMC6 ATM/ANS.OR.C.005(a)(2)
· GM1 to AMC6 ATM/ANS.OR.C.005(a)(2)
· GM2 to AMC6 ATM/ANS.OR.C.005(a)(2)
· GM3 to AMC6 ATM/ANS.OR.C.005(a)(2)
· AMC3 ATS.OR.205(a)(2)
· AMC4 ATS.OR.205(a)(2)
· GM1 to AMC4 ATS.OR.205(a)(2)
· GM3 to AMC4 ATS.OR.205(a)(2)
· GM4 to AMC4 ATS.OR.205(a)(2)

We believe there are too many errors, ambiguities and inconsistencies in section 3.1 to allow for individual correction. Additionally the section does not comply with the intent of Regulation (EU) 2017/373 with respect to changes to functional systems. Section 3.1 requires further development work, to which end EASA is encouraged not to proceed with the elements identified above. Further rulemaking activity to develop text addressing assurance of People, Procedures and Equipment (HW & SW) in a coherent and harmonised manner is proposed as the most appropriate course of action.

response

Partially accepted

Following the order of the comments, below please see the responses to them:

GM2 ATM/ANS.OR.A.045(a): The text was presented as guidance material, and such coordination should exist between the ANSP and the competent authority in a more general way for the changes to the functional system. Nevertheless, the text has been amended to remove GM2.

GM1 ATM/ANS.OR.A.050: The main purpose of the guidance material is to highlight the possible need of performing audits for the software assurance aspects. It is to be noted that Regulation (EU) 2017/373 already considers the use of audits for the continuous oversight activities, but it was considered necessary to make a more specific guidance for the software related audits.

AMC6 ATM/ANS.OR.C.005(a)(2): The reference could be changed to the OR.B.010 requirement, but the mentioned procedures would need to be approved by the competent authority. Furthermore, the proposal is following the philosophy of Regulation (EU) 2017/373 as it is requested that not only the processes are followed but also the behaviour of the system (as done with the change management procedures). Finally, it has been decided to keep it separate due to the link to the functional system.

AMC6 ATM/ANS.OR.C.005(a)(2), (a): The five principles are considered fundamental elements of any software assurance process, for any SWAL, covering the requirements, implementation and verification, complemented by the traceability.

AMC6 ATM/ANS.OR.C.005(a)(2), (a)(2)(ii): The text has been amended to refer to safety support requirements instead of safety requirements.

AMC6 ATM/ANS.OR.C.005(a)(2), (a)(3): The text has been amended to refer to safety support requirements instead of safety requirements

AMC6 ATM/ANS.OR.C.005(a)(2), (c): The text has been amended to make the link with the software assurance processes.

AMC6 ATM/ANS.OR.C.005(a)(2), (f): The text has been amended to address the identified inconsistency.

GM1 to AMC6 ATM/ANS.OR.C.005(a)(2), (b). It is found necessary to mention that this guidance material intends to address the use of software assurance levels (SWALs), so the statement about this relationship between ATSP and other ANSPs is considered valid.

AMC4 ATS.OR.205(a)(2): The reference could be changed to the ATM/ANS.OR.B.010 requirement, but the procedures mentioned would need to be approved by the competent authority. The provision is following the philosophy of Regulation (EU) 2017/373, as it is requested that not only the processes are followed but also the behaviour of the system (as done with the change management procedures). Finally, it has been decided to keep it separate due to the link to the functional system.

AMC4 ATS.OR.205(a)(2), (a): The five principles are considered fundamental elements of the any software assurance process, for any SWAL, covering the requirements, implementation and verification, complemented by the traceability.

GM1 to AMC6 ATM/ANS.OR.C.005(a)(2), (a): The term ‘criticality’ was used to differentiate between the different potential contributions of the software component for the intended services. In the context of this guidance material, it is understood that the term ‘criticality’ is correctly used as it refers to safety criticality.

GM2 to AMC6 ATM/ANS.OR.C.005(a)(2), (a): This guidance material states that the SWAL allocation relates the rigour of the software assurance to the foreseen criticality of the software. The text has been updated in order to make this link clearer.

GM2 to AMC6 ATM/ANS.OR.C.005(a)(2), (b): The comment is not well understood as this item is the result of the safety support assessment. It refers to the most severe effect that software malfunctions or failures may cause.

AMC4 ATS.OR.205(a)(2), (b): Considering the comment, the text has been amended to make the link with the software assurance processes.

AMC5 ATM/ANS.OR.C.005(a)(2), (b): The comment is duly noted.

GM2 ATM/ANS.OR.A.045(a): The commented guidance material has been removed.

AMC6 ATM/ANS.OR.C.005(a)(2), (d): It should be taken into account that this AMC aims to address the need for the processes to determine the rigour for evidence and arguments. In other words, this is requirement for the process definition.

GM2 to AMC6 ATM/ANS.OR.C.005(a)(2): No information about SWAL allocation scheme is included following the same principles as in Regulation (EU) 2017/373, where no severity classification scheme or risk classification scheme is defined.

GM3 to AMC6 ATM/ANS.OR.C.005(a)(2): Considering the comment, the text has been amended to avoid the potential misunderstanding.

AMC3 ATS.OR.205(a)(2), (b): The comment is duly noted.

GM1 to AMC4 ATS.OR.205(a)(2), (a) & (b): The comment is duly noted.

GM1 to AMC4 ATS.OR.205(a)(2), (c)(1): The comment is duly noted.

GM2 to AMC4 ATS.OR.205(a)(2): No information about SWAL allocation scheme is included, following the same principles as in Regulation (EU) 2017/373, where no severity classification scheme or risk classification scheme is defined.

GM3 to AMC4 ATS.OR.205(a)(2), (a): Considering the comment, the text has been amended to avoid the potential misunderstanding.

GM1 to AMC6 ATM/ANS.OR.C.005(a)(2), (c): it should be noted that the use of multiple SWALs is introduced by this point.

GM1 to AMC6 ATM/ANS.OR.C.005(a)(2), (d): The inconsistency mentioned is not acknowledged.

AMC5 ATM/ANS.OR.C.005(a)(2), (b): It is to be noted that the paragraph states ‘when applicable’.

AMC6 ATM/ANS.OR.C.005(a)(2), (a)(2)(i): It is to be noted that this AMC & GM might be applied to different level of software requirements. This is considered to be an important element to be addressed.

AMC6 ATM/ANS.OR.C.005(a)(2), (f): It is to be considered more appropriate to keep at the same level as the previous points, because they belong to the definition of the software assurance processes for this specific type of software components.

GM1 to AMC6 ATM/ANS.OR.C.005(a)(2), (a): It is to be noted that this is guidance material for AMC6.

GM1 to AMC6 ATM/ANS.OR.C.005(a)(2), (a): The comment is duly noted.

GM1 to AMC6 ATM/ANS.OR.C.005(a)(2), (a): Amendments have been introduced in the text to solve the aspect identified as the term 'rigour' has been reworded.

GM1 to AMC6 ATM/ANS.OR.C.005(a)(2), (b): The comment is not well understood, if it refers to the term 'many changes' or the fact that a non-ATS provider may have a safety support case without knowledge of the level of confidence required by the specification (ATS provider). Under the second scenario, it is not considered to be a realistic scenario and, even for non-ATS providers, providing service to several ATS providers, it will be necessary to have a consolidation process to define the more demanding specification confidence level.

GM1 to AMC6 ATM/ANS.OR.C.005(a)(2), (c): The comment is duly noted. However, it should be noted that the same situation occurs at European level with the risk classification schemes in Regulation (EU) 2017/373.

GM2 to AMC6 ATM/ANS.OR.C.005(a)(2), (a): The direct relationship would be between the rigour and the confidence with which a particular requirement is met by the software in operation, which at the end can be related with the criticality.

GM3 to AMC6 ATM/ANS.OR.C.005(a)(2): The proposed standard has been added in the list.

AMC3 ATS.OR.205(a)(2), (b): The comment is duly noted. The presence of 'when applicable' in the commented text should be noted.

AMC4 ATS.OR.205(a)(2), (c): No information about SWAL allocation scheme is included following the same principles as in Regulation (EU) 2017/373, where no severity classification scheme or risk classification scheme are defined.

AMC4 ATS.OR.205(a)(2), (e): The assurance standards include several methods that can be used for all these types of COTS software. In fact, this is the current situation, where the same software standards describe techniques that are used for several types of COTS software. The dependence for each safety case is not shared by EASA.

GM1 to AMC4 ATS.OR.205(a)(2), (a): It is to be noted that this is guidance material for the associated AMC.

GM1 to AMC4 ATS.OR.205(a)(2), (b): The comment is duly considered.

GM1 to AMC4 ATS.OR.205(a)(2), (c)(1): The comment is duly considered.

GM1 to AMC4 ATS.OR.205(a)(2), (c)(2): The comment is duly noted and understood. Nevertheless, it is to be noted that the same situation occurs at European level with the risk classification schemes in Regulation (EU) 2017/373.

GM1 to AMC4 ATS.OR.205(a)(2), (d): The comment is duly considered.

GM2 to AMC4 ATS.OR.205(a)(2): The comment is duly considered.

GM2 to AMC4 ATS.OR.205(a)(2), (a) & (b): The comment is duly considered.

GM2 to AMC4 ATS.OR.205(a)(2), (d): The comment is duly considered.

GM3 to AMC4 ATS.OR.205(a)(2): The proposed standard has been added in the list.

GM2 ATM/ANS.OR.A.045(a) Changes to a functional system p. 9

comment *3* comment by: *DFS Deutsche Flugsicherung GmbH*

This GM implies a new procedure, which is neither subject to Regulations (EU) 2017/373 nor (EC) 482/2008. This is not proportionate and inconsistent as no similar GM is provided to the AR rules. Change review activities are already sufficiently addressed through existing AMC/GM.
We therefore suggest to delete this GM. If particular interest of the NSA shall be drawn on software, we suggest to add the first paragraph of the GM into the current GM1 (not subject to this NPA) point a):

GM1 ATM/ANS.OR.A.045(a) Changes to a functional system
NOTIFICATION
(a) A change should be notified as soon as the data defined in AMC1 ATM/ANS.OR.A.045(a) is available. The decision to review a change by the competent authority will be based, in most circumstances, on the notification data. Exceptions to this are cases where the competent authority is not familiar with the type of change or the complexity of the change requires a more thorough consideration. Depending on the complexity of the change to the functional system and the criticality of the software, the depth of the evaluation may vary.
(b) Early and accurate notification facilitates….

response *Accepted*

Considering the comment, the text has been amended accordingly.

comment *9* comment by: *D Winship*

For 2nd sentence the current wording could be interpreted as giving joint responsibility between SP & CA for the definition of a software oversight strategy.

In addition there is an implication in this text that the CA will be defining a software oversight strategy for each individual change – this is not practicable when most CAs receive hundreds of change notifications per year. In practice the CA is likely to employ a standard change oversight process with the level of review conducted commensurate with the complexity/criticality/level of risk.

Suggest revision to;
"The service provider should coordinate as soon as practicable with the competent authority taking into consideration that the CA's review timelines will be partially dependent on the complexity and criticality of the change."

response *Partially accepted*

Taking into account this comment as well as other comments, the sentence about software oversight strategy has been removed from the set of AMC & GM.

comment *30* comment by: *ENAIRE*

We do not agree to define a software oversight strategy as part of the change review with the NSA. The ANSP shall define a software strategy and the NSA shall validate for all changes.
This is not proportionate and inconsistent as no similar GM is provided to the AR rules. Change review activities are already sufficiently addressed through existing AMC/GM.
We therefore suggest to delete this GM.

response *Partially accepted*

Taking into account this comment as well as other comments, the sentence about software oversight strategy has been removed from the set of AMC & GM.

comment *41* comment by: *CANSO*

This GM implies a new procedure, which is neither subject to Regulations (EU) 2017/373 nor (EC) 482/2008. This is not proportionate and inconsistent as no similar GM is provided to the AR rules. Change review activities are already sufficiently addressed through existing AMC/GM.
We therefore suggest to delete this GM. If particular interest of the NSA shall be drawn on software, we suggest to add the first paragraph of the GM into the current GM1 (not subject to this NPA) point a):

GM1 ATM/ANS.OR.A.045(a) Changes to a functional system
NOTIFICATION
(a) A change should be notified as soon as the data defined in AMC1 ATM/ANS.OR.A.045(a) is available. The decision to review a change by the competent authority will be based, in most circumstances, on the notification data. Exceptions to this are cases where the competent authority is not familiar with the type of change or the complexity of the change requires a more thorough consideration. Depending on the complexity of the change to the functional system and the criticality of the software, the depth of the evaluation may vary.
(b) Early and accurate notification facilitates….

response *Accepted*

Considering the comment, the text has been amended accordingly.

comment *76* comment by: *Swedish Transport Agency, Civil Aviation Department (Transportstyrelsen, Luftfartsavdelningen)*

What is the rational for changing the overall procedure for oversight of change and encurage ANSPs to request early feedback from the CA/NSA to verify the level of details in the software assurance strategy for an individual change, rather than including the software criticality as one aspect to be assessed during the oversight of change.

The obvious drawback of this proposal is that the CA/NSA does not have all the facts on the table and therefore might mislead the service provider. We know that from experience that it is not beneficial from the ANSPs nor from the NSA perspective to handle a specific subset of the change interdependently. The Software assurance Processes has to be agreed by the ANSP and the CA/NSA before any feedback can be given to the ANSP

response *Partially accepted*

Taking into account this comment as well as other comments, the sentence about software oversight strategy has been removed from the set of AMC & GM.

comment *110* comment by: *ENAV*

This GM implies a new procedure, which is neither subject to Regulations (EU) 2017/373 nor (EC) 482/2008. This is not proportionate and inconsistent as no similar GM is provided to the AR rules. Change review activities are already sufficiently addressed through existing AMC/GM.
We therefore suggest to delete this GM. If particular interest of the NSA shall be drawn on software, we suggest to add the first paragraph of the GM into the current GM1 (not subject to this NPA) point a):

GM1 ATM/ANS.OR.A.045(a) Changes to a functional system
NOTIFICATION
(a) A change should be notified as soon as the data defined in AMC1 ATM/ANS.OR.A.045(a) is available. The decision to review a change by the competent authority will be based, in most circumstances, on the notification data. Exceptions to this are cases where the competent authority is not familiar with the type of change or the complexity of the change requires a more thorough consideration. Depending on the complexity of the change to the functional system and the criticality of the software, the depth of the evaluation may vary.
(b) Early and accurate notification facilitates….

response | *Accepted*

Considering the comment, the text has been amended accordingly.

comment | *177* comment by: *The Boeing Company*

Page: 9
Paragraph: GM2 ATM/ANS.OR.A.045(a)

The proposed text states: "NOTIFICATION — SOFTWARE CRITICALITY"

Requested Change: We request that EASA specify which software is being referenced; the software used in house for production, or the software used in products delivered to the customer.

Justification: Clarification.

response | *Noted*

The software mentioned is that part of the functional system, which is used by the ANSP for the service provision. Then, it will fall under the second option identified by the commenter.

comment | *188* comment by: *AESA/DSANA*

Change "as soon as possible" to the following text: "prior to the implementation of the software assurance processes".

A regulation should not define requirements that cannot be assessed.

response | *Partially accepted*

Taking into account this comment as well as other comments, the sentence about software oversight strategy has been removed from the set of AMC & GM.

comment | *189* comment by: *AESA/DSANA*

The depth of the evaluation should depend on the criticality of the SW according to the service provided and not on the complexity of the change.

According to GM2 ATM/ANS.OR.A.045(a), each change could, in principle, have different oversight strategies, even if the criticality of the service they are providing is the same.

response | *Noted*

The complexity of the change would have a clear contribution to the depth of the evaluation of a particular change.

comment | *190* comment by: *AESA/DSANA*

What is it to be understood by complexity? Is the service provider the only responsible for its determination or should it be agreed with the NSA?

This is an issue which could be controversial and now seems a key factor to decide the depth of the revision.

response *Noted*

The comment is not well understood. The complexity of the change or activities would not require a particular definition.

comment *191* comment by: *AESA/DSANA*

It is not clear which SW - related information should be included by the Service Provider in the Notification of the change, if any.

Some key SW-related aspects should be identified and included in the list of data to notify to the Competent Authority in order to help them to decide whether to review or not (AMC1 ATM/ANS.OR.A.045(a); GM1 ATM/ANS.OR.A.045(a)).

response *Partially accepted*

Taking into account this comment as well as other comments, the sentence about software oversight strategy has been removed from the set of AMC & GM.

comment *192* comment by: *AESA/DSANA*

An important concept is included without guidelines to interpretation or application: "criticality of the software". A definition should be included.

The concept "criticality of the software" is used to determine the depth of the evaluation. The level of confidence to "ensure the existence of documented software assurance processes necessary to produce evidence and arguments that demonstrate that the software behaves as intended (software requirements)", and the rigour to which the assurances are established to achieve compliance with the objectives of the software assurance processes are, among other things, also depending on the "criticality of the software".
Due to the importance of the concept, it is considered necessary to establish some guidance material on how to determinate the criticality of the software. Some examples, or a scale of criticality would be also useful for the sake of harmonisation.

response *Not accepted*

The term software criticality was already used in Regulation (EC) No 482/2008 with no particular definition and no major concern was reported by stakeholders when showing compliance. Therefore, no amendments to the text are introduced in this context.

comment *214* comment by: *DSAC - FR NSA*

French NSA fully supports the idea of early coordination between CA and SP for software aspects. However, this GM is refering to the "Notification" process and may be misinterprated as in some cases it is more than likely that the criticality and the SWAL of involved software will be unknown at the moment of the notification. Suggestion would be to mention explicitly that SWAL is not due in the initial notification form but should be communicated as soon as known.

response *Noted*

Based on this comment and considering other comments, it has been decided to remove GM2 ATM/ANS.OR.A.045(a) on Notification – Software Criticality. The provisions presented in the AMC & GM for 'ATM/ANS.AR.C.035(a) Decision to review a notified change to the functional system' cover this aspect.

comment *268* comment by: *ASD/Thales Air Systems*

The concept of "software criticality" may be interprated in various manner since the term criticality is not defined. It may be useful to link it to the concept of SWAL (allocation) who is the translation of this criticality in terms of evaluation of the direct or indirect crontribution of the software to a feared event having with a given severity.

response *Noted*

Based on this comment and considering other comments, it has been decided to remove GM2 ATM/ANS.OR.A.045(a) on Notification – Software Criticality. The provisions presented in the AMC & GM for 'ATM/ANS.AR.C.035(a) Decision to review a notified change to the functional system' cover this aspect.

comment *297* comment by: *UK CAA*

Equivalent coverage in EC 2017/373 text:

GM1 ATM/ANS.OR.A.045(a) (b), (c), (d) (e) & (f)

General GM – 3.2

Comments:

Not specific to software. Removal of the SW related terms would have no effect on the meaning of the text and would broaden it to include PPE.Covered in GM1 and General GM – 3.2 to a much greater depth.

response *Accepted*

Considering this comment, it has been concluded that the proposed amendment to GM1 ATM/ANS.OR.A.045(a) on Notification should be removed. The provisions presented in the AMC & GM for 'ATM/ANS.AR.C.035(a) Decision to review a notified change to the functional system' already cover this aspect.

GM1 ATM/ANS.OR.A.050 Facilitation and cooperation p. 9

comment	*4* comment by: *DFS Deutsche Flugsicherung GmbH* Access right of the competent authority is crucial to a contract between an ANSP and sub-contracted organisations. Probably a lot of contracts need to be updated accordingly. A simple explanation within GM may not be the right place to address such facilitation and its empowerment. Furthermore, if it's essential to provide information how a CA should review a change by which software is affected, this should be subject to Part AR.
response	*Noted* As correctly mentioned by the commentator, the access right of the competent authority is crucial. This is why it is required under Article 5 of Regulation (EU) 2017/373 and further regulated in ATM/ANS.OR.B.015 'Contracted activities' that stipulates that contracts with software suppliers shall already consider the possibility to offer the access to the compliance demonstration data to the competent authority. The purpose of this GM to illustrate the actions to be taken by the ATM/ANS providers in this context.

comment	*10* comment by: *D Winship* Consider revision to Paragraph (a) - readability issues. Specifically "In this context,…access to the development environment and to the configuration management system to the competent authority that needs to verify:… Also editorial below: "the fact that all the evidence ***{missing is}*** derived from a known version of software."
response	*Partially accepted* Considering the comments, the text has been amended.

comment	*11* comment by: *D Winship* Para b(1) appears to add little value and isn't specifically relevant to software assurance processes – the principle that the CA has the right to conduct audits as appropriate is well established in the legislation and doesn't need to be restated specifically within the software assurance AMC/GM.
response	*Noted* EASA shares the commentator's view that on-site audits and inspections are already covered by other parts of the legislation. Nevertheless, the potential software audits/inspections might be necessary in the frame of the review of a particular

change, for which specific considerations should be paid by the ATM/ANS providers when planning the introduction of a particular type of changes (e.g. new systems).

comment *12* comment by: *D Winship*

Para b(2)
"rights to audit into the contractual provisions" – intent unclear – the CA may wish to comment or obtain more detailed evidence from the service provider on assurance material provided by a supplier but generally it isn't specifically "contractual provisions" that would be audited – it is just as likely that technical information would be requested as opposed to "contractual provisions". Again this section adds little to what is a 'normal' oversight task not specific to the oversight of software.

response *Partially accepted*

The purpose of this GM is to stress the fact that ATM/ANS providers should clarify with the suppliers the requirement from the competent authority about the need of providing such visibility even from the supplier activities, as far as this is related to the regulatory compliance demonstration or the safety/safety support argument demonstration. Considering the comment, the text has been amended.

comment *31* comment by: *ENAIRE*

Access to the configuration management system to the component authority should be enough. For this reason, it is suggested to change the paragraph as follows: "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".

response *Accepted*

comment *42* comment by: *CANSO*

Access right of the competent authority is crucial to a contract between an ANSP and sub-contracted organisations. Probably a lot of contracts need to be updated accordingly.
A simple explanation within GM may not be the right place to address such facilitation and its empowerment.
Furthermore, if it's essential to provide information how a CA should review a change by which software is affected, this should be subject to Part AR.

response *Noted*

As correctly mentioned by the commentator, the access right of the competent authority is crucial. This is why it is required under Article 5 of Regulation (EU) 2017/373 and further regulated in ATM/ANS.OR.B.015 'Contracted activities' that

stipulates that contracts with software suppliers shall already consider the possibility to offer the access to the compliance demonstration data to the competent authority. The purpose of this GM to illustrate the actions to be taken by the ATM/ANS providers in this context.

comment *50* comment by: *CANSO*

Access to the configuration management system to the component authority should be enough. We suggest to change GM1(a) as follows:

"(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".

response *Accepted*

comment *83* comment by: *Copenhagen Airport*

a) Providing access to the development environment and configuration management at contracted organizations to the competent authority may prove to be without value or even produce false evidence. The competences of the authorities will be significantly challenged as software development is a highly complicated process.
The service provider is in a far better position to do quality audits at contracted organizations. The suggestion is therefore to let the authority assess the service provider and his quality management system as well as the safety arguments provided.

b.2) Refer to a)

response *Noted*

EASA shares the commentator's view that as part of the compliance monitoring, the ATM/ANS providers will evaluate in detail the necessary aspects from the contracted organisation to support the regulatory compliance. Nevertheless, the competent authority should have the possibility to decide either to rely on the quality audit results obtained by the ATM/ANS provider or to perform independent evaluation of the software assurance compliance records. Based on this second scenario, it is considered necessary to keep the proposed GM.

comment *85* comment by: *EASA Focal Point for AustroControl ANSP-issues*

GM1 ATM/ANS.OR.A.050 Facilitation and cooperation
(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).

AUSTROCONTROL Comment:
It should be clear stated, that access for Competent Authorities to developing environment u. configuration management can only be ensured for ANSP inhouse development and never for an external supplier.

response *Noted*

The comment is duly noted.

However, it should be highlighted that the commented GM is in line with the currently applicable Regulation (please refer to Articles 6 and 7 of Regulation (EU) No 1035/2011) and Article 5 of Regulation (EU) 2017/373. Therefore, contracts with software suppliers shall already consider the possibility to offer access to the compliance demonstration data to the competent authority.

comment *86* comment by: *EASA Focal Point for AustroControl ANSP-issues*

GM1 ATM/ANS.OR.A.050 Facilitation and cooperation
.....

(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.

AUSTRO CONTROL Comment:
Point (2) could be read or understood in the way **that the ANSP should also include the corresponding right to audit of contracted organisations for CA**. This requires clarification and probably goes beyond the scope of a GM.

response *Noted*

The comment is duly noted.

However, it should be highlighted that the commented GM is in line with the currently applicable Regulation (please refer to Articles 6 and 7 of Regulation (EU) No 1035/2011) and Article 5 of Regulation (EU) 2017/373. Therefore, contracts with software suppliers shall already consider the possibility to offer the access to the compliance demonstration data to the competent authority, including the possibility to perform on-site audits, as it would be the case for the software assurance processes.

comment	*111* comment by: *ENAV* Access right of the competent authority is crucial to a contract between an ANSP and sub-contracted organisations. Probably a lot of contracts need to be updated accordingly. A simple explanation within GM may not be the right place to address such facilitation and its empowerment. Furthermore, if it's essential to provide information how a CA should review a change by which software is affected, this should be subject to Part AR.
response	*Noted* The comment is duly noted. However, it should be highlighted that the commented GM is in line with the currently applicable Regulation (please refer to Articles 6 and 7 of Regulation (EU) No 1035/2011) and Article 5 of Regulation (EU) 2017/373. Therefore, contracts with software suppliers shall already consider the possibility to offer the access to the compliance demonstration data to the competent authority. Furthermore, it is to be noted that the current AMC & GM for review of changes to functional system do not establish the means to be followed by the competent authority for the review of changes.

comment	*112* comment by: *ENAV* Access to the configuration management system to the component authority should be enough. We suggest to change GM1(a) as follows: "(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".
response	*Accepted*

comment	*127* comment by: *ENAV* **GM1 ATM/ANS.OR.A.050 Facilitation and cooperation** (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).

Comment:
It should be clear stated, that access for Competent Authorities to developing environment u. configuration management can only be ensured for ANSP inhouse development and never for an external supplier.

response *Noted*

The comment is duly noted.

However, it should be highlighted that the commented GM is in line with the currently applicable Regulation (please refer to Articles 6 and 7 of Regulation (EU) No 1035/2011) and Article 5 of Regulation (EU) 2017/373. Therefore, contracts with software suppliers shall already consider the possibility to offer the access to the compliance demonstration data to the competent authority.

comment *128* comment by: *ENAV*

GM1 ATM/ANS.OR.A.050 Facilitation and cooperation
.....
(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.

Comment:
Point (2) could be read or understood in the way **that the ANSP should also include the corresponding right to audit of contracted organisations for CA.** This requires clarification and probably goes beyond the scope of a GM.

response *Noted*

The comment is duly noted.

However, it should be highlighted that the commented GM is in line with the currently applicable Regulation (please refer to Articles 6 and 7 of Regulation (EU) No 1035/2011) and Article 5 of Regulation (EU) 2017/373. Therefore, contracts with software suppliers shall already consider the possibility to offer the access to the compliance demonstration data to the competent authority. Furthermore, the current AMC & GM for review of changes to functional system do not establish the means to be followed by the competent authority for the review of changes, including the possibility to perform on-site audits, as it would be the case for the software assurance processes.

comment *133* comment by: *LFV*

It may be difficult to contractually ensure the right for the competent authority to access a supplier's development environment and to audit system suppliers. Please consider whether GM1 ATM/ANS.OR.A.050 is feasible.

response | *Noted*

The comment is duly noted.

However, it should be highlighted that the commented GM is in line with the currently applicable Regulation (please refer to Articles 6 and 7 of Regulation (EU) No 1035/2011) and Article 5 of Regulation (EU) 2017/373. Therefore, contracts with software suppliers shall already consider the possibility to offer the access to the compliance demonstration data to the competent authority. Furthermore, the current AMC & GM for review of changes to functional system do not establish the means to be followed by the competent authority for the review of changes, including the possibility to perform on-site audits, as it would be the case for the software assurance processes.

comment | *139* comment by: *CANSO*

GM1 ATM/ANS.OR.A.050 Facilitation and cooperation
(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).

CANSO Comment:
It should be clear stated, that access for Competent Authorities to developing environment u. configuration management can only be ensured for ANSP inhouse development and never for an external supplier.

response | *Noted*

The comment is duly noted.

However, it should be highlighted that the commented GM is in line with the currently applicable Regulation (please refer to Articles 6 and 7 of Regulation (EU) No 1035/2011) and Article 5 of Regulation (EU) 2017/373. Therefore, contracts with software suppliers shall already consider the possibility to offer the access to the compliance demonstration data to the competent authority. Furthermore, the current AMC & GM for review of changes to functional system do not establish the means to be followed by the competent authority for the review of changes, including the possibility to perform on-site audits, as it would be the case for the software assurance processes.

comment | *140* comment by: *CANSO*

GM1 ATM/ANS.OR.A.050 Facilitation and cooperation
.....
(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.

CANSO Comment:
Point (2) could be read or understood in the way **that the ANSP should also include the corresponding right to audit of contracted organisations for CA.** This requires clarification and probably goes beyond the scope of a GM.

response *Noted*

The comment is duly noted.

However, it should be highlighted that the commented GM is in line with the currently applicable Regulation (please refer to Articles 6 and 7 of Regulation (EU) No 1035/2011) and Article 5 of Regulation (EU) 2017/373. Therefore, contracts with software suppliers shall already consider the possibility to offer the access to the compliance demonstration data to the competent authority. Furthermore, the current AMC & GM for review of changes to functional system do not establish the means to be followed by the competent authority for the review of changes, including the possibility to perform on-site audits, as it would be the case for the software assurance processes.

comment *178* comment by: *The Boeing Company*

Page: 9
Paragraph: GM1 ATM/ANS.OR.A.050 (b) (2)

The proposed text states:

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

Requested Change:
We request that EASA specify which contractual provisions, in particular.

Justification: Contractual provisions may be confidential. In some cases, it may even be impossible to reveal that there is a contract and who the contract partner is.

response *Noted*

It should be highlighted that the commented GM is in line with the currently applicable Regulation (please refer to Articles 6 and 7 of Regulation (EU) No 1035/2011) and Article 5 of Regulation (EU) 2017/373. Therefore, contracts with software suppliers shall already consider the possibility to offer the access to the compliance demonstration data to the competent authority.

comment	*194* comment by: *AESA/DSANA* Consider to include GM2 ATM/ANS.OR.A.050(a) in NPA 2017/373 AR. GM2 ATM/ANS.OR.A.050(a)involves, in fact, requirements for the NSA.
response	*Noted* The commented GM is limited to the service providers. The involvement of the competent authority is covered by the existing AMC & GM where the aspects on the level of involvement are addressed, covering the software as one of the elements in the change management.

comment	*210* comment by: *European Transport Workers Federation - ETF* ETF welcomes this approach and encourages EASA to closely monitor that system manufacturers enable ANSPs to go down this path.
response	*Noted*

comment	*273* comment by: *German NSA (BAF)* "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." Proposal: Replace "should" be by "shall".
response	*Not accepted* The use of ‘shall’ is reserved for the implementing rules, which stipulate an obligation for the person or organisation that is subject to the rule. An AMC or GM, having a non-binding nature, cannot use any language that expresses an obligation (neither ‘shall’ nor ‘must’); thus, the use of ‘should’.

comment	*284* comment by: *Swedish Transport Agency, Civil Aviation Department (Transportstyrelsen, Luftfartsavdelningen)* This implies that the CA/NSA has to have competency in assesment of software development to be able review the proposed software assurance processes from the ANSP
response	*Noted* Considering the requirements laid down in Regulation (EU) 2017/373 on competent authority training aspects, the answer is affirmative.

comment	*298* comment by: *UK CAA*

Equivalent coverage in EC 2017/373 text:

ATM/ANS.OR.A.045 (c)
ATM/ANS.OR.B.010 (a)
ATM/ANS.OR.C.005 (a)(2) & (b)(2)

Comments:
Not specific to software. Removal of the SW related terms would have no effect on the meaning of the text and would broaden it to include PPE.
This section is out of context. Content and application of assurance cases is covered in AMC/GM associated with ATM/ANS.OR.C.005(a). The approval of processes is covered in ATM/ANS.OR.B.10 and its associated AMC/GM
If the evidence required by (b)(2) is necessary but not included in the assurance case then the assurance case would not be valid and could not be approved – see ATM/ANS.OR.C.005(a)(2) and its associated AMC/GM
Co-operation between the service provider and the CA during change is covered, in detail, in section 3 of the General GM.
If it were felt necessary to highlight this co-operation it would have to include all regulatory interaction governed by the IR.

response *Noted*

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

AMC5 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system p. 10

comment *13* comment by: *D Winship*

The service provider should "ensure the existence of documented software assurance processes"…

Even though 482/2008 is repealed, by requiring "software assurance processes" rather than a system assurance process the AMC effectively still enforces an obligation on the ANSP to have a stand-alone software assurance system as very few ANSPs/CAs have the time and resources required to develop suitable AltMoCs. This requires careful consideration given that a more 'systems oriented' assurance approach is suggested in the introduction.

response *Noted*

The reference to the software assurance processes follows the same approach as in Regulation (EC) No 482/2008. The approach followed is to address the software elements and to ask about the HW assurance aspects. It is noted that the scope of a system assurance process is not covering the software aspects at the level requested by Regulation (EC) No 482/2008. However, the reference to the development of suitable AltMoC is not understood as, according to the currently applicable

Regulation (EC) No 482/2008, all the ANSPs should have in place a software safety assurance system.

comment *14* comment by: *D Winship*

"For that purposes, 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…."

This text could be open to several interpretations and requires enhancement to improve clarity. Specific concerns include use of "reported according to the relevant requirements on **reporting and assessment of service occurrences**" – as written this could be interpreted as stating only those failures/malfunctions reported under the Occurrence Reporting Regulation are considered/assessed which would not in practice be advisable – for most systems the majority of software-related errors/failures would not be likely to result in the generation of an "occurrence report" falling within the scope of the OR regulation (e.g. those detected during testing or those having no actual impact on the service).

response *Partially accepted*

Considering the comment, the text has been amended to avoid misunderstandings.

comment *15* comment by: *D Winship*

For section (b)
The intent of the requirement to assess the effect of a software 'occurrence' in comparison with the "effects identified for the system concerned as per the service specification" is also unclear. The intent/meaning of this sentence could be open to widely varying interpretations. In 482/2008 the effects were referenced to the severity classification scheme in the common requirements. If this is no longer relevant then consideration should be given to rewording as "effects in a service specification" doesn't appear to be meaningful – specifications normally contain system requirements, behaviours, interface definitions etc. rather than "effects".

response *Accepted*

Considering the comment, the text has been amended by adding the demonstration of the service specification.

comment *62* comment by: *CANSO*

As stated in explanatory note on NPA 2014-13 "While today CNS providers are seen to try to comply with these requirements, they cannot always do so. This is because CNS providers, as other non-ATS providers, do not have a dynamic view of the use of the service and, therefore, cannot intervene in order to alter a developing situation. Furthermore, the non-ATS provider may not know how the service it offers is being used by the ATS provider, either in normal circumstances or in circumstances where immediate intervention is necessary in order to maintain safety".

	Therefore, service providers other than ATS providers cannot assess the software **"criticality of the required application**" as described at the end of item (a). Service providers other than ATS providers can only assess the PERFORMANCE of the service provided. In the same spirit of previous comment, considering that service providers other than ATS providers are not the user of the software, it is not possible for them to realize a feedback of software experience, => These items shall be deleted on this AMC or modified to address PERFORMANCE instead of safety.
response	*Accepted* Considering the comment, amendments have been made to the text. However, it is necessary to clarify two aspects: - Service providers other than ATS providers can assess the satisfaction of the service requirements (not only the performance, understood as performance requirements). - Service providers other than ATS are users of the software (at least, they should monitor the service and the system status) and, hence, they have information to provide feedback on software experience.

comment	*64* comment by: *CANSO* Remark: In item (a), in case of modifications to existing software, the existence of documented software assurance processes could not be systematically available, especially if the development was performed several years before. Additionally, the state of art at the moment for the previous development could be significantly different as the current standards. In these cases, the service history could be claimed without any existence of documentation. => The following sentence is proposed for amendment: *(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. In case of incomplete or absence to this expected documentation, the service experience, if exists, could be considered as a relevant complementary way.*
response	*Not accepted* It is necessary to point out that, as described in AMC6 ATM/ANC.OR.C.005(a)(2), (f), it is always possible to have specific software assurance processes for managing previously developed software and to use the technique that is mentioned in the comment. Based on the existence of this provision, it is not considered necessary to include the additional clarification proposed by the commentator.

comment	*82* comment by: *EUROCONTROL*

ATM/ANS.OR.C.205(a)(2) - Pages 10 to 14

(Same comment as for ATS.OR.205(a)(2)).

The EUROCONTROL Agency finds that there is no AMC/GM explaining how the criticality of the software (SWAL) is linked to the criticality of the application. This might lead, for the same functional system, to a situation with different SWAL allocations by different ANSPs, although for the same required application. It would be therefore beneficial at European level to rely on a standardised mechanism for SWAL allocation, depending on the criticality of the application.

response *Noted*

The comment is duly considered.

It is agreed that there is a difference between the criticality of the software and the criticality of the particular application by an ANSP. The same software can be used in different contexts by several ANSPs. Nevertheless, the objective of the AMC & GM is to address the software assurance aspects associated with the software, once the criticality of the application has been addressed by the ANSP.

On the other hand, EASA concurs with the idea of having a common European SWAL allocation matrix, as currently presented in some of the software standards. However, Regulation (EU) 2017/373 and the existing AMC & GM do not go in that direction regarding the severity classification scheme and risk classification scheme, where there is no harmonised severity classification scheme (as there is today under Regulation (EU) No 1035/2011). Then, this limits the possibility of establishing a common European SWAL allocation matrix.

comment *113* comment by: *ENAV*

In item (a), in case of modifications to existing software, the existence of documented software assurance processes could not be systematically available, especially if the development was performed several years before.
Additionally, the state of art at the moment for the previous development could be significantly different as the current standards.
In these cases, the service history could be claimed without any existence of documentation.
=> The following sentence is proposed for amendment:
(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. In case of incomplete or absence to this expected documentation, the service experience, if exists, could be considered as a relevant complementary way

response *Not accepted*

It is necessary to point out that, as described in AMC6 ATM/ANC.OR.C.005(a)(2), (f), it is always possible to have specific software assurance processes for managing previously developed software and to use the technique that is mentioned in the comment. Based on the existence of this provision, it is not considered necessary to include the additional clarification proposed by the commentator.

comment *143* comment by: *DSNA*

In some specific cases, some Risk Mitigation Means are foreseen in order to be a response for some hazards. These Risk Mitigation Means could be considered as an acceptable alternative way instead of software safety support assessment. => The following sentence is proposed for amendment and should be added : *"An acceptable alternative way for software safety support assessment could be the demonstration of existence of adequate Risk Mitigation Means."*

response *Not accepted*

The term 'software safety support assessment' is not used in the proposed set of AMC & GM.

comment *154* comment by: *DSNA*

Regarding CE482/2008 matrix on §6 of this NPA, item (b) of this AMC is linked to the article 4(5), so the use of the feedback of software experience is a transverse and ongoing process which is not related to a specific change and specific software. More globally, this AMC is related to safety assessment by ATS proviver and is already covered by "ATS.OR.200 Safety management system" (a Software safety Assurance System is part of a Safety Management System). Therefore, item (b) shall be deleted

response *Not accepted*

The use of software experience is a transverse process but provides results at the time of implementing a specific change. This could be the case for the introduction of a new COTS version. Then, EASA considers that item (b) is still relevant.

comment *155* comment by: *DSNA*

As stated in explanatory note on NPA 2014-13 "While today CNS providers are seen to try to comply with these requirements, they cannot always do so. This is because CNS providers, as other non-ATS providers, do not have a dynamic view of the use of the service and, therefore, cannot intervene in order to alter a developing situation. Furthermore, the non-ATS provider may not know how the service it offers is being used by the ATS provider, either in normal circumstances or in circumstances where immediate intervention is necessary in order to maintain safety". Therefore, service providers other than ATS providers can not assess the software *"criticality of the required application"* as described at the end of item (a). Service providers other than ATS providers can only assess the PERFORMANCE of the service provided.

In the same spirit of previous comment, considering that service providers other than ATS providers are not the user of the software, it is not possible for them to realize a feedback of software experience,
=> These items shall be deleted on this AMC or modified to address PERFORMANCE instead of safety..

response

Accepted

Considering the comment, amendments have been made to the text.

However, it is necessary to clarify two aspects:

- Service providers other than ATS providers can assess the satisfaction of the service requirements (not only the performances, understood as performance requirements)

- Service providers other than ATS are users of the software (at least, should monitor the service and the system status) and, hence, with information to provide feedback of software experience.

comment

156 comment by: *DSNA*

In item (a), in case of modifications to existing software, the existence of documented software assurance processes could not be systematically available, especially if the development was performed several years before.
Additionally, the state of art at the moment for the previous development could be significantly different as the current standards.
In these cases, the service history could be claimed without any existence of documentation.
=> The following sentence is proposed for amendment:
(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. ***In case of incomplete or absence to this expected documentation, the service experience, if exists, could be considered as a relevant alternative way.***

response

Not accepted

It is necessary to point out that, as described in AMC6 ATM/ANC.OR.C.005(a)(2), (f), it is always possible to have specific software assurance processes for managing previously developed software and to use the technique that is mentioned in the comment. Based on the existence of this provision, it is not considered necessary to include the additional clarification proposed by the commentator.

comment

179 comment by: *DSNA*

In some specific cases, for instance, meteorological services, the assessment of the software providing the service support is out of the managerial control scope from the ANSP. Therefore, software assessment of support services can't be assessed by

	the ANSP. => The following sentence is proposed for amendment and should be added : *"In case the support is out of the definition and/or managerial control scope, the safety support assessment will be specifically not foreseen."*
response	*Not accepted* In the current regulatory framework, 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 air traffic services (ATS), airspace management (ASM), and air traffic flow management (ATFM), i.e. air traffic management (ATM) and communication, navigation, or surveillance (CNS). Additionally, the software aspects for aeronautical information services (AIS) provision are included in Regulation (EU) No 73/2010. On the other hand, it is acknowledged that the MET providers will be affected as regards the software assurance AMC & GM. EASA considers that some of the service providers other than the ones that are subject to Regulation (EC) No 482/2008 today have a contribution to software (e.g. MET providers, FPD) and it was concluded that some features of the MET systems are affected by the current regulatory requirements, which also supports the approach taken for the proposed set of AMC & GM; that is, to apply for all service providers of ATM/ANS, including AIS and MET providers, towards software assurance level standardisation.

comment	*195* comment by: *AESA/DSANA* A definition for "Software Assurance Level (SWAL)" should be included. For the sake of a better understanding of the AMC/GM a definition for what should be understood for "Software Assurance Level (SWAL)" should be included. The ED153 definition is proposed.
response	*Accepted* Considering the comment, the text has been amended to address the proposal.

comment	*196* comment by: *AESA/DSANA* The need of a "documented software assurance process" should be more evident and unambiguous. It is considered that requirements about defining and establishing SW safety assessment and assurance procedures should be stated as an AMC of ATM/ANS.OR.B.010 (a) "Change management procedures". Additionally, in that framework of pre-established a approved SW procedures, criteria about how to define a software oversight strategy and guidelines to include it in the notification should be developed by the service providers in their documented procedures. For the sake of an easier and a clearer understanding of the requirements, as an AMC of ATM/ANS.OR.B.010 (a), it should be stated that "The service provider should have

documented software assurance processes to assure the introduction of new software or the modification to existing software included in a change to a functional system." Also at this level could be moved the wording: "Those processes are 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."
These procedures should be under approval of the Competent Authority, like the rest of change management procedures.
Hence, it is proposed to rely the software oversight strategies on proper defined procedures of both sides the NSA (notification and oversight procedures) and the ANSPs (documented procedures of software assurance).

response *Not accepted*

It was considered more relevant to maintain the link with the functional system and the associated changes rather to include it as part of the service provider's management system. It is noted that the software assurance processes might also be at the level of the system suppliers.

comment *211* comment by: *European Transport Workers Federation - ETF*

ETF calls for transparency by ANSPs and system manufacturers to make this feedback effective.
ETF believes it would be useful to include a regulatory requirement to establish a responsibility by system manufacturers on the system provided during the time of implementation and if a problem stemming from this occurs, the associated update to the system should be done by system manufacturers with no additional costs.

response *Noted*

The comment is duly noted that is outside the scope of the proposed set of AMC & GM.

comment *232* comment by: *NATS*

para (b) The wording as stated places the confirmation of the SWAL allocation and rigour of the SWAL processes on the Service Provider, "when applicable", when SWAL is an ATS provider concept.
Impact: As currently stated this is likely to cause confusion, especially in cases where the service provider has no concept of SWAL. The service provider should be using software experience to confirms that (their) software assurance processes are effective and can provide data to confirm that the SWAL is appropriate (rather than providing confirmation themselves).
Suggestion: Suggest amending the wording to remove the implied need for the service provider to confirm the allocated SWAL and rigour of the allocated SWAL.

response *Accepted*

Considering the comment, the text has been amended.

comment	*279* comment by: *CANSO* AMC5 ATM.OR.C.005(a)(2)(b), The wording as stated places the confirmation of the SWAL allocation and rigour of the SWAL processes on the Service Provider, “when applicable”, when SWAL is an ATS provider concept. Impact: As currently stated this is likely to cause confusion, especially in cases where the service provider has no concept of SWAL. The service provider should be using software experience to confirms that (their) software assurance processes are effective and can provide data to confirm that the SWAL is appropriate (rather than providing confirmation themselves). Suggestion: Suggest amending the wording to remove the implied need for the service provider to confirm the allocated SWAL and rigour of the allocated SWAL.
response	*Accepted* Considering the comment, the text has been amended.

comment	*288* comment by: *ASD/Thales Air Systems* It is not clear why the concept of safety **support** assessement is introduced specifically in SUBPART C (and is not mentionned in SUBPART A which contains the same requirements). At least, this concept should be clearly defined.
response	*Noted* The comment is noted. It should be pointed out that the set of AMC & GM follows the order of the requirements as laid down in Regulation (EU) 2017/373, which is not subject to this consultation.

comment	*291* comment by: *ASD/Thales Air Systems* AMC5 (b): "... and, **when applicable**, the allocated SWAL..." criteria of applicability is not clear and needs to be clarified.
response	*Partially accepted* Considering the comment, the text has been amended to clarify the message that it refers more to the usage than the applicability.

comment	*299* comment by: *UK CAA* Comments: Not specific to software. Removal of the SW related terms would have no effect on the meaning of the text and would broaden it to include PPE.

	Most of these points (see below) are covered by AMC/GM related to ATM/ANS.OR.B.005, B.010 & C.005
response	*Noted* The comment is duly noted. However, EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment	*300* comment by: *UK CAA* **AMC5 ATM/ANS.OR.C.005(a)(2), point (a)** **Equivalent coverage in EC 2017/373 text:** **ATM/ANS.OR.B.010 (a)** **ATM/ANS.OR.C.005 (a)(2)** **Comments:** SW is part of a functional system. Before changing any part of a functional system the service provider must ensure that the procedures to be used are approved by the CA. This is covered in ATM/ANS.OR.B.010.
response	*Not accepted* It was considered more relevant to maintain the link with the functional system and the associated changes rather to include it as part of the service provider's management system. It is noted that the software assurance processes might also be at the level of the system suppliers.

comment	*301* comment by: *UK CAA* **AMC5 ATM/ANS.OR.C.005(a)(2) point (b)** **Equivalent coverage in EC 2017/373 text:** ATM/ANS.OR.B.005 (a)(4), (c) & (d) ATM/ANS.OR.B.010 (b) & (c) **Comments:** The management system rules cover the reporting, analysis and correction of failures of the functional system and adequate performance of procedures. They cover the complete functional system and change management procedures and therefore, by definition, cover software.
response	*Noted* It should be pointed out that the level of granularity would not be enough in order to confirm the effectiveness of the software assurance process. Based on this specific

need, it is considered necessary to provide additional guidance compared with the general one at functional system level.

AMC6 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system p. 10-11

comment *16* comment by: *D Winship*

para (a) (1) (i)
Software requirements "correct, complete and compliant with the upper level requirements"
Use of "compliant …upper level" requirements implies a multi-layered requirements set which may, or may not be, the case. The different levels of system/software requirements should be consistent, coherent and 'aligned with', rather than 'compliant with', each other (as compliance is normally verified *for* each requirement as opposed to *between* different levels of requirements).

Replacing this text with "aligned with the system requirements" would appear to be more appropriate.

response *Not accepted*

It is considered preferable to keep the current wording in order to allow this multi-layered software architecture, as it is the case in most of the current implementations.

comment *18* comment by: *D Winship*

section a(5)
"following verification methods…agreed with the CA" –
It is essential to recognise that the CA focus is on the adequacy of the verification results/assurance – it is neither practical, achievable or desirable for the CA to engage in approving "verification methods" for individual changes. In addition, the text as written doesn't take into account the reality that, in most projects, much of the software is not unique or custom designed specifically for a single service provider – some of the verification work on core functionality may have been completed long before the service provider and CA became involved (i.e. re-used software from other projects). Some of the results of this earlier verification activity could be permissible as evidence (e.g. 'core' algorithm testing) even though the CA hasn't been engaged in agreeing the "verification method".

This text should be reconsidered – the original text from 482 (with NSA replaced by CA) appears more appropriate.
"The EATMN software shall be adequately verified by analysis and/or testing and/or equivalent means, as agreed with
the…"

response *Accepted*

The commented provision has been amended following the suggestion to align with Regulation (EC) No 482/2008.

comment *32* comment by: *ENAIRE*

Regarding "software resource usage on the target hardware" there is the following potential interpretation: Hardware resource usage on the target hardware could be excluded. I.e. The number of CPU cores required by the software or the I/o interface types available to the software.

Problem arising: Hardware resource may not be verified as complete and correct. Especially when dealing with COTS or unintended software as these may cause the software to function unexpectedly when different hardware configurations are used.

Suggested improvement: Either of the following would solve the problem:

- Remove the Word software to leave to following "…accuracy, resource usage on the target hardware…"

or

- Add hardware leaving the following "... accuracy, software and hardware resource usage on the target hardware..."

response *Accepted*

The commented provision has been amended following the first suggestion of the commentator.

comment *33* comment by: *ENAIRE*

Regarding the sentence "if a requirement cannot be traced", there is the following potential interpretation: Software requirements may be tagged as safety or integrity requirements because its parent requirement (the upper level requirement it traces to) is tagged as safety or integrity related. Therefore a software requirement that does not trace to a requirement above may never be identified as software safety or integrity requirement.

Problem arising: Any software fix implemented in order to solve a problem reported from testing at a higher level, should require the retest of all affected requirements (i.e. all requirements that trace to the requirement associated with the problem) should be verified as not being affected. Any requirement without traceability will never benefit from this relationship and potential fault may be overlooked.

Suggested improvement: Add de following:
Nevertheless all requirements determined as potentially affecting safety, if not implemented correctly or completely, should be traced to a corresponding upper level requirement.

response | *Not accepted*

It should be pointed out that the concept of derived (non-traced) requirements is not only applicable to safety integrity requirements. Even in Regulation (EC) No 482/2008, it is necessary to ensure that the software implementation does not have a safety impact. Based on that, any non-traced requirement should be justified and assessed as non-impacting either the satisfaction of the safety requirements or safety support requirements, as appropriate.

comment | *34* comment by: *ENAIRE*

Regarding AMC6 ATM/ANS.OR.C.005(a)(2) - (a)(5) "The verification of the software is correct an complete, following verification methods...", there is the following potential interpretation: This can mean that the objective is to determine if the verification process is correct and not that the Software being verified is complete and correct.

Problem arising: The result of applying the objective as read means that the verification process could be correct and complete but the software being verified may not.

Suggested improvement: Change to the following:
"The verification that the software is correct and complete, ….."

response | *Not accepted*

It should be pointed out that the correctness and completeness refer to the software verification.

The text as it stands states 'the software verification is correct and complete …'

comment | *35* comment by: *ENAIRE*

AMC6 ATM/ANS.OR.C.005(a)(2) - (f)(6) "monitoring":
Potential interpretation: This could be read that a software could be put into operation, monitored, and then an argument be established.

Problem arising: Monitoring can only happen during operation. Therefore using monitoring in order to argue that a product meets a desired rigour could mean that the software could be used during a period without an established argument.

Suggested improvement: Suggest removing monitoring as existing service level experience should cover the same.
If monitoring is used for proving that the rigour argument is correct then this is covered by "AMC5 ATM/ANS.OR.C.005 (a)(2) – (b)".

response | *Not accepted*

It should be highlighted that they are complementary mitigation ways, one based on the assurance level and the other highlighting some safety or safety support

requirements derived from the need of monitoring a particular COTS. Therefore, it is preferable to keep the wording as initially proposed.

comment *52* comment by: *CANSO*

(1)(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.

Potential interpretation of (1) (ii):
Hardware resource usage on the target hardware could be excluded. I.e. The number of CPU cores required by the software or the I/o interface types available to the software.

Issue:
Hardware resource may not be verified as complete and correct. Especially when dealing with COTS or unintended software as these may cause the software to function unexpectedly when different hardware configurations are used.

Suggested improvement:
Either of the following would solve the problem:
Remove the Word software to leave to following "…accuracy, resource usage on the target hardware…"
Or
Add hardware leaving the following "…accuracy", software and hardware

response *Accepted*

The text has been amended considering the first proposal.

comment *55* comment by: *CANSO*

(f) (6)
Potential interpretation:
This could be read that a software could be put into operation, monitored, and then an argument be established.

Issue:
Monitoring can only be done during operation. Therefore using monitoring in order to argue that a product meets the desired rigour could mean that the software could be used during a period without an established argument.

Suggested improvement:
We suggest to remove '(6) monitoring' as existing service level experience should cover the same.
If monitoring is used for proving that the rigour argument is correct then this is covered by "AMC5 ATM/ANS.OR.C.005 (a)(2) – (b)".

response *Not accepted*

It should be highlighted that they are complementary mitigation ways, one based on the assurance level and the other highlighting some safety or safety support requirements derived from the need of monitoring a particular COTS. Therefore, it is preferable to keep the wording as initially proposed.

comment *60* comment by: *CANSO*

Pages 10-14
In some specific cases, for instance, meteorological services, the assessment of the software providing the service support is out of the managerial control scope from the ANSP. Therefore, software assessment of support services can't be assessed by the ANSP.
=> The following sentence is proposed for amendment and should be added in each concerned AMC (see below):
In case the support is out of the definition and/or managerial control scope, the safety support assessment will be specifically not foreseen.

response *Not accepted*

It should be highlighted that in the current regulatory framework, 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 air traffic services (ATS), airspace management (ASM), air traffic flow management (ATFM), i.e. air traffic management (ATM) and communication, navigation, or surveillance (CNS). Additionally, the software aspects for aeronautical information services (AIS) provision are included in Regulation (EU) No 73/2010. On the other hand, it is acknowledged that the MET providers will be affected as regards the software assurance AMC & GM.

EASA considers that some of the service providers other than the ones that are subject to Regulation (EC) No 482/2008 today have a contribution to software (e.g. MET providers, FPD) and in order EASA to take an informed decision, a specific meeting with other stakeholders was organised to address this issue (among others). The discussion clearly concluded that some features of the MET systems are affected by the current regulatory requirements, which also supports the approach taken for the proposed set of AMC & GM; that is, to apply for all service providers of ATM/ANS, including AIS and MET providers, towards software assurance level standardisation.

comment *67* comment by: *CANSO*

Remark:
Item (b) is missing.

response *Accepted*

The text has been amended accordingly.

comment	*68* comment by: *CANSO* Remark: Items (f)(1), (f)(2),(f)(3) are missing.
response	*Accepted* The text has been amended accordingly.

comment	*114* comment by: *ENAV* Remark: Sentence of item (2)(i) seems to be ambiguous and clarification is expected. => The following sentence is proposed for amendment: *(i) Each software requirement introduced at each level in the ~~design~~ lifecycle should be traced to the same level of ~~design~~ lifecycle at which its satisfaction is demonstrated.*
response	*Partially accepted* Considering the comment the text has been amended to promote clarity. However, it should be noted that the proposed solution was different from the original text and the intent of the rule.

comment	*115* comment by: *ENAV* Remark: Item (b) is missing. Items (f)(1), (f)(2),(f)(3) are missing.
response	*Accepted* The text has been amended accordingly.

comment	*116* comment by: *ENAV* §3.1 Annexe III, subpart C AMC5 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system - As stated in explanatory note on NPA 2014-13 *"While today CNS providers are seen to try to comply with these requirements, they cannot always do so. This is because CNS providers, as other non-ATS providers, do not have a dynamic view of the use of the service and, therefore, cannot intervene in order to alter a developing situation. Furthermore, the non-ATS provider may not know how the service it offers is being used by the ATS provider, either in normal circumstances or in circumstances where immediate intervention is necessary in order to maintain safety".* Therefore, service providers other than ATS providers can not assess the software *"criticality of the required application"* as described at the end of item (a). Service providers other than ATS providers can only assess the PERFORMANCE of the service provided.

In the same spirit of previous comment, considering that service providers other than ATS providers are not the user of the software, it is not possible for them to realize a feedback of software experience,
=> These items shall be deleted on this AMC or modified to address PERFORMANCE instead of safety..

response

Accepted

Considering the comment, amendments have been made to the text.

However, it is necessary to clarify two aspects:

- Service providers other than ATS providers can assess the satisfaction of the service requirements (not only the performance, understood as performance requirements).

- Service providers other than ATS are users of the software (at least, they should monitor the service and the system status) and, hence, they have information to provide feedback on software experience.

comment

117 comment by: *ENAV*

Remark:
Sentence of item (2)(i) seems to be ambiguous and clarification is expected.
=> The following sentence is proposed for amendment:
*(i) Each software requirement introduced at each level in the ~~design~~ **lifecycle** should be traced to the same level of ~~design~~ **lifecycle** at which its satisfaction is demonstrated.*

response

Partially accepted

Considering the comment, the text has been amended to promote clarity.

However, it should be noted that the proposed solution was different from the original text and the intent of the rule.

comment

134 comment by: *LFV*

Bullet number b) is missing.

response

Accepted

The text has been amended accordingly.

comment

141 comment by: *CANSO*

Remark:
Sentence of item (2)(i) seems to be ambiguous and clarification is expected.
=> The following sentence is proposed for amendment:
(i) Each software requirement introduced at each level in the ~~design~~ lifecycle should be traced to the same level of ~~design~~ lifecycle at which its satisfaction is demonstrated.

response | *Partially accepted*

Considering the comment, the text has been amended to promote clarity.

However, it should be noted that the proposed solution was different from the original text and the intent of the rule.

comment | *144* comment by: *DSNA*

In some specific cases, some Risk Mitigation Means are foreseen in order to be a response for some hazards. These Risk Mitigation Means could be considered as an acceptable alternative way instead of software safety support assessment. => The following sentence is proposed for amendment and should be added : *"An acceptable alternative way for software safety support assessment could be the demonstration of existence of adequate Risk Mitigation Means."*

response | *Not accepted*

The term 'software safety support assessment' is not used in the proposed set of AMC & GM.

comment | *161* comment by: *DSNA*

In some specific cases, for instance, meteorological services, the assessment of the software providing the service support is out of the managerial control scope from the ANSP. Therefore, software assessment of support services can't be assessed by the ANSP.

The following sentence is proposed for amendment:

In case the support is out of the definition and/or managerial control scope, the safety support assessment will be specifically not foreseen.

response | *Not accepted*

It should be highlighted that in the current regulatory framework, 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 air traffic services (ATS), airspace management (ASM), air traffic flow management (ATFM), i.e. air traffic management (ATM) and communication, navigation, or surveillance (CNS). Additionally, the software aspects for aeronautical information services (AIS) provision are included in Regulation (EU) No 73/2010. On the other hand, it is acknowledged that the MET providers will be affected as regards the software assurance AMC & GM.

EASA considers that some of the service providers other than the ones that are subject to Regulation (EC) No 482/2008 today have a contribution to software (e.g. MET providers, FPD) and in order EASA to take an informed decision, a specific meeting with other stakeholders was organised to address this issue (among others). The discussion clearly concluded that some features of the MET systems are affected by the current regulatory requirements, which also supports the approach taken for

the proposed set of AMC & GM; that is, to apply for all service providers of ATM/ANS, including AIS and MET providers, towards software assurance level standardisation.

In addition, the AMC could not elevate an objective laid down in the rule.

comment

162 comment by: *DSNA*

Justification of " derived" requirements (e.g no traced to upper level) is state of the art and in line with ED109A. Assessing that it does not affect the satisfaction of the safety requierements goes beyond the existing industrial standards In point (2) (ii). Please change : *"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~~"*
Into *"If a requirement cannot be traced to any upper level requirement, its need should be justified"*
(remove text after "justified")

response

Not accepted

It is considered relevant to address the main criteria to be used for the justification (and acceptance) of the requirement. Removing this information could open the door to other criteria which might not be consistent with the intended purpose.

comment

163 comment by: *DSNA*

As stated in item (a)(1)(ii), one may understand that the demonstration is covering all the software. Actually, the demonstration should only cover the scope of the change.
=> The following sentence is proposed for amendment:
*(a)(1)(ii) specify **in the scope of the change**,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 **new software or modified** software **part**.*

response

Not accepted

It must be highlighted that the requirement refers to features requested in the software assurance process. They can be applied for a particular change but the processes should be change-independent.

comment

164 comment by: *DSNA*

Sentence of item (2)(i) seems to be ambiguous and clarification is expected.
=> The following sentence is proposed for amendment:
*"(i) Each software requirement introduced at each level in the ~~design~~ **lifecycle** should be traced to the same level of ~~design~~ **lifecycle** at which its satisfaction is demonstrated."*

response

Partially accepted

Considering the comment, the text has been amended to promote clarity.

However, it should be noted that the proposed solution was different from the original text and the intent of the rule.

comment *165* comment by: *DSNA*

Item (b) is missing.

response *Accepted*

comment *166* comment by: *DSNA*

Items (f)(1), (f)(2),(f)(3) are missing.

response *Accepted*

comment *180* comment by: *DSNA*

In some specific cases, for instance, meteorological services, the assessment of the software providing the service support is out of the managerial control scope from the ANSP. Therefore, software assessment of support services can't be assessed by the ANSP.
=> The following sentence is proposed for amendment and should be added : *"In case the support is out of the definition and/or managerial control scope, the safety support assessment will be specifically not foreseen."*

response *Not accepted*

It should be highlighted that in the current regulatory framework, 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 air traffic services (ATS), airspace management (ASM), air traffic flow management (ATFM), i.e. air traffic management (ATM) and communication, navigation, or surveillance (CNS). Additionally, the software aspects for aeronautical information services (AIS) provision are included in Regulation (EU) No 73/2010. On the other hand, it is acknowledged that the MET providers will be affected as regards the software assurance AMC & GM.

EASA considers that some of the service providers other than the ones that are subject to Regulation (EC) No 482/2008 today have a contribution to software (e.g. MET providers, FPD) and in order EASA to take an informed decision, a specific meeting with other stakeholders was organised to address this issue (among others). The discussion clearly concluded that some features of the MET systems are affected by the current regulatory requirements, which also supports the approach taken for the proposed set of AMC & GM; that is, to apply for all service providers of ATM/ANS, including AIS and MET providers, towards software assurance level standardisation.

comment *193* comment by: *AESA/DSANA*

SW legacy, referred to as used software in EC 482/2008 and as previously developed software in this NPA needs to be defined.
What is the reason for changing "used SW" for "previously developed SW" which seems to be more general? NSAs are not notified of SW development unless the software is expected to be in operational service.
What has to be done with previously existing SW at which this NPA would apply and at which the former Regulation (EC) No 482/2008 did not?

Time indications on what to consider SW legacy s are lost when repealing Regulation (EC) No 482/2008 as long as they were gathered in its article 7 :
Article 7
Entry into force
This Regulation shall enter into force on the 20th day following that of its publication in the Official Journal of the European Union.
It shall apply from 1 January 2009 to the new software of EATMN systems referred to in Article 1(2), first subparagraph.
It shall apply from 1 July 2010 to any changes to the software of EATMN systems referred to in Article 1(2), first subparagraph, in operation by that date.

response *Noted*

It should be noted that Regulation (EC) No 482/2008 entered into force in 2010 and, hence, after several years of application, it is understood that the concept of software legacy does not require a particular treatment. Consequently, any new software or modifications to existing software should follow the software assurance processes.

comment *197* comment by: *AESA/DSANA*

Renumbering is required.

Errata in number scheme. There is no (b) in the main scheme.

response *Accepted*

comment *198* comment by: *AESA/DSANA*

A definition of "Configuration data" should be included.

For the sake of a better understanding of the AMC/GM, a definition of what should it be understood by "Configuration Data" should be introduced. The ED153 definition is proposed.

response *Accepted*

Considering the comment, the text has been amended.

comment *199* comment by: *AESA/DSANA*

A definition for "Commercial Off The Shelf (COTS)" should be included.

For the sake of a better understanding of the AMC/GM, a definition of what should it be understood by "Commercial Off The Shelf (COTS)" should be introduced. The ED153 definition is proposed.

response *Accepted*

Considering the comment, the text has been amended.

comment *204* comment by: *AESA/DSANA*

Guidelines to clarify which is the purpose of a set of SWALs and to establish that the service provider should define its own set of SWALs, should be included.

No requirement is included for service providers to define its own set of SWALs in its own procedures.
In the same way that a "severity (classification) scheme" is addressed in "GM1 ATS.OR.205(b)(4) Safety assessment and assurance of changes to the functional system", even if non SWAL classification is adopted, at least the indication that each service provider should define its own set of SWALs and also the explanation of what is expected from a set of SWALs should be made.
It is considered that the Software Assurance Processes and the Software Assurance Levels of an organization should be defined in its procedures before the organization starts providing its service. An AMC related to "ATM/ANS.OR.B.010 Change management procedures" should be established in order to clarify this issue.

response *Not accepted*

It was considered more relevant to maintain the link with the functional system and the associated changes rather to include it as part of the service provider's management system. It is noted that the software assurance processes might also be at the level of the system suppliers.

comment *205* comment by: *European Transport Workers Federation - ETF*

ETF notes that a bullet (b) is missing.

response *Accepted*

Considering the comment, the text has been amended.

comment *207* comment by: *European Transport Workers Federation - ETF*

p10 : non-ATS services AMC6 (a)(2)(ii) Each software requirement [...] **should be traced** to an upper level requirement [...]	Is the difference intended ? From a regulatory perspective, it does not seem to create any difference in the provision or at least we do not understand it.

p15 : ATS services : AMC4 (a)(2)(ii) Each software requirement [...] **is traced to** an upper level requirement [...]	

response *Accepted*

The text has been amended to address the inconsistency.

comment *208* comment by: *European Transport Workers Federation - ETF*

p11 : non-ATS services : AMC6 (f) [...] If no sufficient assurance **can** be provided [...] p16 : ATS services : AMC4 (e) [...] If no sufficient assurance **may** be provided [...]	Is the difference intended ? From a regulatory perspective, it does not seem to create any difference in the provision or at least we do not understand it.

response *Accepted*

The text has been amended to address the inconsistency.

comment *215* comment by: *DSAC - FR NSA*

In paragraph (a)(3), the demonstration that the software implementation contains no functions which adversely affect safety may be difficult to achieve especially for COTS.
This paragraph may be rephrased as "the functions contained in the software implementation do not adversely affect safety".

response *Not accepted*

For COTS, a specific assurance process can be defined by the service provider as highlighted in point (f) of the AMC. The reference to the software implementation is considered relevant and covers the case of the COTS, where activated functions need to be assessed for the potential impact on safety or service specifications.

comment	*234* comment by: *NATS* Para (a) (2) (ii) The first sentence establishes a requirement. The second provides a requirement for when the first requirement cannot be met. The commas in the first sentence make unclear what the qualifier "at which its satisfaction is demonstrated" applies to. The last sentence introduces a "component" without defining what this component is. **Impact:** Ambiguity as to what the first statement means and whether it must actually be met. Ambiguity in the second sentence as to what the requirement must be assessed against. **Suggested wording**: "Each software requirement allocated to a component should EITHER be traced to an upper level requirement OR its need should be justified and the requirement assessed to ensure that it does not affect the satisfaction of the safety requirements allocated to the component.
response	*Accepted* Considering the comment, the text has been amended.

comment	*235* comment by: *NATS* para (a) (3) The requirement is too restrictive. For instance a training mode built into the software may adversely affect safety if enabled during operation, but there is no risk if this mode is effectively disabled. It is also not clear what the "software implementation" is: does it mean the source code or the executable? This matters because compile-time switches can be used to disable functions that were built into the source code. **Impact:** Service providers will be forced to develop multiple versions of their products with overlapping functionality, increasing costs without improving safety. **Suggested resolution:** Replace with "Any functions of the software that could adversely affect safety are disabled".
response	*Not accepted* It is considered that the current wording is appropriate for the case mentioned and offers the possibility to include disabled elements in the software implementation, provided that the disabling mechanism is appropriate.

comment	*237* comment by: *NATS* para (f) The sub-paragraphs are numbered 4 – 6 not 1 – 3. This could cause confusion. Suggest renumber the sub paragraphs
response	*Accepted* Considering the comment, the text has been amended.

comment	*238* comment by: *NATS*

	para (c) (1) “a known executable version of the software” seems too imprecise; the “known” version should be the one that is to be deployed into operation. **Suggest:** rewording to “the executable version of the software which is to be deployed into operation” Similar changes should be made to (2) and (3) of clause (c)
response	*Not accepted* It should be considered that the verification activities can be based on several (known) versions of the software, without mandatorily being the last one. An assessment of the versions evolutions might allow to take credit of the verification in previous versions of particular requirements, subject to a non-regression policy.

comment	*240* comment by: *NATS* par (a) (1) (ii) Although a straight copy of the EC 482/2008 requirement the concept of “software resource usage on target hardware” is not required. It could be argued that to meet the other software requirements as stated (such as performance and overload tolerance) “software resource usage” must be met. **Impact:** Difficult to specify and meet especially for software deployed within a virtualised environment. **Suggest** the removal of the statement “software resource usage on target hardware” from the list.
response	*Partially accepted* The text has been amended considering also other comments and the word ‘software’ has been removed.

comment	*241* comment by: *NATS* para (a) (2) (ii) The text as stated refers to non interference with the safety requirements allocated to the component. Whilst this is technically correct a service provider may not recognise a ‘safety requirement’ on their service provision **Impact:** Lack of clarity across service provision boundary with respect to performance/integrity requirements that support safety requirements. **Suggestion:** Removal of the term “safety” from the statement to become “does not affect the satisfaction of the requirements allocated to the component”.
response	*Accepted* Considering the comment, the text has been amended.

comment	*242* comment by: *NATS* para (a) (3) The service provider may not have any knowledge of how their service is to be used, and may not be in the position to know how their software implementation could “affect safety”. **Issue:** Impact assessment may not occur or may be inappropriate from a safety perspective.

Suggested resolution: More generically this is a non-interference statement, and therefore should state "which adversely affect other software functions"

response *Accepted*

It is noted that the proposal made by the commentator does not refer to the potential effect on safety or service specification but on the non-interference. The associated paragraph is intended to avoid particular functions in the software that might have an impact on safety. This would require the implementation of reliable disabling mechanisms for those functions that should remain in the software although not active operationally.

comment *243* comment by: *NATS*

para (a) (4) Although a straight copy of the EC 482/2008 requirement the concept of "software resource usage on target hardware" is not required. It could be argued that to meet the other software requirements as stated (such as performance and overload tolerance) "software resource usage" must be met.
Impact: Difficult to specify and meet especially for software deployed within a virtualised environment.
Resolution: Suggest the removal of the statement "software resource usage on target hardware" from the list.

response *Accepted*

Considering the comment, the text has been amended.

comment *244* comment by: *NATS*

para (a) (5) Its unclear as to the scope of the agreement with respect to verification with the CA i.e. is the intention a strategy or a requirement by requirement verification method or selection from an agreed set of verification methods?
Impact: Potential inconsistency of application. Effort required from CA associated with agreeing software verification approach.
Resolution: Clarification with regards to the intention of the statement.

response *Accepted*

This potential misunderstanding has been acknowledged, leading to the possible understanding that the verification methods shall be subject to approval by the competent authority. The intention of the paragraph was to focus the approval of the competent authority on the equivalent means. Rewording of this paragraph has been introduced.

comment *245* comment by: *NATS*

(c) List item (b) is either missing or item (c) should be modified (along with following list items) to be item (b) etc.
Issue: Integrity of requirement
Suggest modifying as appropriate

response | *Accepted*

Considering the comment, the text has been amended.

comment | *246* comment by: *NATS*

para (c) As written there is no means to use arguments or evidence from previous versions of software if suitably justified.
Impact: Unnecessary re-generation of assurance evidence, with associated cost.
Suggested resolution: Modify (3) to read "that have been used in the production of that version, or can be justified as applicable to that version.'

response | *Accepted*

Considering the comment, the text has been amended.

comment | *247* comment by: *NATS*

para (f) It is not necessarily true that "generic assurance processes cannot be applied" to COTS, NDS or PDS. It is however unlikely
Impact: the inference that generic assurance approach is not applicable to these types of software.
suggested resolution: Modify "generic assurance processes cannot be applied" to "generic assurance processes may not be applicable"

response | *Not accepted*

It was considered more relevant to keep the current wording to highlight the impossibility to apply the generic assurance process. There would be some COTS or NDS where the generic assurance process is possible and can be provided by the COTS supplier.

comment | *248* comment by: *NATS*

Para (f) Modify last sentence for readability.
Issue: Needs clarity
Suggestion: Modify to read "If sufficient assurance cannot be provided, complementary…."

response | *Accepted*

Considering the comment, the text has been amended.

comment | *249* comment by: *NATS*

para (f) In themselves neither "existing service level experience" nor "monitoring" are a "mitigation means aiming at decreasing the impact of specific failure modes of this type of software", whereas software/system architectural considerations are.
Impact: Confusion between failure mode mitigation and means of addressing assurance shortfalls. General clarity.

Suggestion: Reword preceding text to read "If sufficient assurance cannot be provided, complementary mitigation should be applied. This may include but is not limited to:"

response *Not accepted*

It is to be noted that the three cases presented would belong to the mitigation of specific failure modes pre- and post-implementation. Therefore, the current wording is maintained.

comment *281* comment by: *CANSO*

AMC6 ATM/ANS.OR.C.005(a)(2) para (a) (2) (ii)
The first sentence establishes a requirement. The second provides a requirement for when the first requirement cannot be met. The commas in the first sentence make unclear what the qualifier "at which its satisfaction is demonstrated" applies to. The last sentence introduces a "component" without defining what this component is.

Impact: Ambiguity as to what the first statement means and whether it must actually be met. Ambiguity in the second sentence as to what the requirement must be assessed against.

Suggestion: Suggested wording: "Each software requirement allocated to a component should EITHER be traced to an upper level requirement OR its need should be justified and the requirement assessed to ensure that it does not affect the satisfaction of the safety requirements allocated to the component.

response *Accepted*

Considering the comment, the text has been amended.

comment *285* comment by: *Swedish Transport Agency, Civil Aviation Department (Transportstyrelsen, Luftfartsavdelningen)*

Open-source (eg. Linux) should to be mentioned,

The software assurance process should address Cyber security in the context that the ANSP has to verify that the software is resilient and checked against harmful software.

response *Partially accepted*

As regards 'open source' software, it is considered preferable not to mention it explicitly due to the particular considerations in the possible usage of open source. The example presented by the commentator could be subject of confusion as the ANSPs are using Linux implementations supplied by software suppliers, belonging to the COTS domain.

As regards 'cyber security' aspects, the point has been taken and discussed in specific sessions with stakeholders. It has been concluded that this should not be addressed in the frame of this set of AMC & GM. A transversal regulatory activity to all the

domains is under development and the cyber security aspects will be better covered in that way.

comment *286* comment by: *ASD/Thales Air Systems*

In the item (a)(1)(ii), it is mentionned "specify the functional behaviour in ... downgraded modes ..." and later "... robustness to abnormal operating conditions ...". What is the difference between the 2 points? It seems that these 2 points are redundant o at least linked since requirements on "downgraded modes" cover "robustness to abnormal operating conditions". May be the last part of the sentence could be used as an example of downgraded mode.

response *Noted*

The comment is duly noted.

Downgraded modes might correspond to a situation in which the software provides lower performances but works under normal operating conditions. Then, both concepts are separate and would need to be maintained in this way.

comment *289* comment by: *ASD/Thales Air Systems*

In AMC6, item (b) is missing.

response *Accepted*

The text has been amended.

comment *296* comment by: *UK CAA*

Page No: 10/11

Paragraph No: AMC6 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system 'ASSURANCE — SOFTWARE ASSURANCE PROCESSES'

Comment: The draft text jumps from paragraph (a)(5) to paragraph (c). It is questioned whether paragraph (b) is missing or the subsequent paragraphs are erroneously numbered.

Justification: Missing text or erroneous paragraph numbering.

Proposed Text: Renumber paragraphs after paragraph (a)(5)

response *Accepted*

comment *302* comment by: *UK CAA*

AMC6 ATM/ANS.OR.C.005(a)(2)

Equivalent coverage in EC 2017/373 text: —

Comments:
Not specific to software. Removal of the SW related terms would have no effect on the meaning of the text and would broaden it to include PPE.
Most of these points (see below) are covered by AMC/GM related to ATM/ANS.OR.C.005
This section is out of context. Processes are dealt with in ATM/ANS.OR.B.010 and its associated AMC/GM. This section of the IR and its associated AMC/GM deals with the criteria for safety support assurance cases and not the processes that created a safety support case.

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *303* comment by: *UK CAA*

AMC6 ATM/ANS.OR.C.005(a)(2), point (a)(1)(i)
See also:#
AMC4 ATS.OR.205(a)(2), point (a)(1)(i)

Equivalent coverage in EC 2017/373 text: AMC2 ATM/ANS.OR.C.005(a)(2) (b), (c), (d)

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *304* comment by: *UK CAA*

AMC6 ATM/ANS.OR.C.005(a)(2), point (a)(1)(ii)

Equivalent coverage in EC 2017/373 text:
ATM/ANS.OR.C.005(a)(1)(v)
GM3 ATM/ANS.OR.C.005(a)(2) (a)

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *305* comment by: *UK CAA*

AMC6 ATM/ANS.OR.C.005(a)(2), point (a)(2)(i)

Equivalent coverage in EC 2017/373 text: AMC2 ATM/ANS.OR.C.005(a)(2) (d)

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *306* comment by: *UK CAA*

AMC6 ATM/ANS.OR.C.005(a)(2), point (a)(2)(ii)

Equivalent coverage in EC 2017/373 text: AMC2 ATM/ANS.OR.C.005(a)(2) (d)

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *307* comment by: *UK CAA*

AMC6 ATM/ANS.OR.C.005(a)(2), point (a)(3)

Equivalent coverage in EC 2017/373 text: N/A

Comments: Incorrect: There is no view of safety in Annex III text

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *308* comment by: *UK CAA*

AMC6 ATM/ANS.OR.C.005(a)(2) point (a)(4)

Equivalent coverage in EC 2017/373 text:
ATM/ANS.OR.C.005 (a)(1)(ii)
AMC1 ATM/ANS.OR.C.005(b)(1) (h)

response

Noted

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *309* comment by: *UK CAA*

AMC6 ATM/ANS.OR.C.005(a)(2), point (a)(5)

Equivalent coverage in EC 2017/373 text:
ATM/ANS.OR.C.005 (a)(2), (b)(1)
AMC1 ATM/ANS.OR.C.005(b)(1)

Comments: The procedures for verification are covered in ATM/ANS.OR.B.010 and its associated AMC/GM and will have been agreed with the CA prior to their use.

response

Accepted

Considering the comment, the text has been amended.

comment *310* comment by: *UK CAA*

AMC6 ATM/ANS.OR.C.005(a)(2) point (c)

Equivalent coverage in EC 2017/373 text: AMC2 ATM/ANS.OR.C.005(a)(2) (f)

response

Noted

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *311* comment by: *UK CAA*

AMC6 ATM/ANS.OR.C.005(a)(2) point (d)
See also:
GM1 to AMC6 ATM/ANS.OR.C.005(a)(2) points (a) (b) & (c)
GM2 to AMC6 ATM/ANS.OR.C.005(a)(2) points (a), (b), (c) & (d)

Equivalent coverage in EC 2017/373 text: N/A

Comments: The concept of rigour is not used in the IR, confidence is used. Assurance levels are used in Regulation (EC) No 482/2008 to determine 'the rigour to which the assurances are established'. This can only be understood as a means to provide the required level of confidence. Hence this clause is incorrect.

response *Accepted*

Considering the comment, the text has been amended.

comment *312* comment by: *UK CAA*

AMC6 ATM/ANS.OR.C.005(a)(2), point (e)(1)

Equivalent coverage in EC 2017/373 text:
ATM/ANS.OR.B.030 (a), (b) & (c).
AMC2 ATM/ANS.OR.C.005(a)(2) (f)

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *313* comment by: *UK CAA*

AMC6 ATM/ANS.OR.C.005(a)(2), point (e)(2)

Equivalent coverage in EC 2017/373 text:
ATM/ANS.OR.B.005 (a)(4), (c) & (d)
ATM/ANS.OR.B.030 (a), (b) & (c)

Comments: The management system rules cover the reporting, analysis and correction of failures of the functional system.

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *314* comment by: *UK CAA*

AMC6 ATM/ANS.OR.C.005(a)(2), point (e)(3)
See also:
AMC4 ATS.OR.205(a)(2), point (d)(3)

Equivalent coverage in EC 2017/373 text: ATM/ANS.OR.B.030 (a), (b) & (c)

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *315* comment by: *UK CAA*

AMC6 ATM/ANS.OR.C.005(a)(2), point (f)

Equivalent coverage in EC 2017/373 text: N/A

Comments:
Incorrect.
The requirement for assurance (ATS.OR.205(a)(2)) applies to all parts of the functional system and therefore includes software, no matter whether it is bespoke, COTS or previously developed.
This is GM not AMC. The rule itself is adequate, it covers this and is not specific to software.

response *Not accepted*

It was considered relevant to address the particular situation of this type of software as far as generic assurance processes cannot be applied.

GM1 to AMC6 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system p. 12

comment *20* comment by: *D Winship*

para (c)
"The use of multiple SWALs…several criticalities of software …by same set of software assurance processes". This text is potentially misleading as the software assurance system may be designed to invoke more comprehensive and rigorous processes for more critical code – in other words not employing the **same** set of processes.

response *Not accepted*

The processes are written in general terms. Typically, software suppliers have a unique set of software development processes that are able to cope with several

software assurance levels, depending on the activities carried out. Therefore, it was considered relevant to maintain the text as proposed.

comment *23* comment by: *D Winship*

Para (c)
“processes are **intended to rely on** several software assurance levels”. Suggest replace ‘intended to rely on’ with ‘employ’. Assurance processes don’t ‘**rely’** on SWALs, assurance evidence rigour is driven by the software’s designated SWAL(s).

response *Accepted*

Considering the comment, the text has been amended.

comment *36* comment by: *ENAIRE*

GM1 to AMC6 ATM/ANS.OR.C.005(a)(2) - (c)(1):
Regarding the sentence "the rigour should increase as the software increases in criticality", there is the following potential interpretation: In general, software is not critical. The correct wording is mission critical software or safety critical software.

Problem arising: A solution could be a mixture between SW and hardware where a hardware element could be a fall back element if the software fails. In this case, the criticality of the service provided by the system may not directly affect the software itself but the overall solution. i.e. introduce a third hardware fall-back element.

Suggested improvement: Suggest rewording as “the rigour should increase as the criticality of the service supported by the software solution increases;"

response *Accepted*

Considering the comment, the text has been amended.

comment *200* comment by: *AESA/DSANA*

A definition for "Software Component" should be included.

For the sake of a better understanding of the AMC/GM, a definition of what should it be understood by "Software Component" should be introduced. The ED153 definition is proposed.

response *Accepted*

Considering the comment, the text has been amended.

comment *206* comment by: *European Transport Workers Federation - ETF*

ETF is of the opinion that it is of tremendous importance that the software assurance level is to be determined by the ATS provider (under the appropriate

	oversight by the competent authority) and not by the system manufacturer if any.
response	*Noted* The comment is duly noted.

comment	*216* comment by: *DSAC - FR NSA* Paragraph (d) is somehow contradictory and difficult to understand since it says that the SWAL concept can be useful, but not relevant for non-ATS providers. This paragraph only provides an introduction to paragraph (b), they thus could be merged.
response	*Accepted* Considering the comment, the text has been amended.

comment	*217* comment by: *DSAC - FR NSA* Paragraph (d) doesn't provide added guidance to AMC6 ATM/ANS.OR.C.005(a)(2) - (f) regarding the "alternative means […] to demonstrate", therefore it could be removed.
response	*Accepted* Considering the comment, the text has been amended in Part-ATS as well as in Section 3 to Part-ATM/ANS.OR.

comment	*226* comment by: *DSAC - FR NSA* Only ED-153 provides a methodology to allocate SWAL and it is not sufficiently detailed and "constraining" to assure that SWAL will be allocated on the same way by all users. A more detailed GM would help to harmonize SWAL allocation.
response	*Noted* The commented provision is linked to the way, in which the safety (support) assessment is performed by each of the ANSPs. The proposal will be considered in future rulemaking activities on the subject.

comment	*250* comment by: *NATS* **para (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." Where this is the case, appropriate partitioning needs to be demonstrated **Issue:** Suggests it is OK to have components of different criticality in the same system without partitioning

Suggestion: Reword to “The use of multiple SWALs would also allow the possibility of managing several criticalities of the different software components within the system (with appropriate partitioning) by the same set of software assurance processes.”

response *Accepted*

Considering the comment, the text has been amended.

comment *251* comment by: *NATS*

Para (d) It is not necessarily true that “generic assurance processes cannot be applied” to COTS, NDS or PDS. It is however unlikely.
Issue: Remove the inference that generic assurance approach is not applicable to these types of software
Suggestion: Modify “generic assurance processes cannot be applied” to “generic assurance processes may not be applicable”

response *Partially accepted*

The commented point was removed as it is redundant given the presence of point (f) of AMC6 ATM/ANS.OR.C.005(a)(2).

comment *252* comment by: *NATS*

Para (b) "When tools are used during the software development lifecycle”. It is difficult to imagine a software development lifecycle that does not include at least one tool (such as a compiler or development environment). In those terms “Tool Qualification” always exists for a software development lifecycle.
Issue Clarify that tool qualification it not ‘optional’ as implied by the statement.
Suggestion: Add ED-215 to the list of ED-109A related supplements

response *Accepted*

EASA agrees that tools are widely used for software development and verification. Nevertheless, it might be possible that the tools do not require qualification because the output is verified independently.

comment *290* comment by: *ASD/Thales Air Systems*

GM1 to AMC6 item (a): the last sentence "non-ATS providers may not be aware of the safety aspects of ATS providers using their services" is not understood as from a classical top-down safety methodology approach, the ATS provider (using a service or equipment coming from a non-ATS provider) will allocate a safety objective (e.g. target SWAL level) to any service or equipment having an identified impact on a hazard (defined in its FHA). In the case where there is no identified impact, there will be no allocation of safety objective. The problem described in this last sentence can come from an ATS provider who does not do allocate safety objectives to its providers.

GM1 to AMC6 item (b): this item is explaining that what is written in item (a) above is not relevant in most of the cases ... this makes item (a) and (b) very confusing and with poor added value.

To improve both item (a) and (b), the definition of the minimal interface between ATS providers and non-ATS providers might be described with a guidance on what is expected in terms of inputs/outputs by both sides.

response *Not accepted*

The non-ATS provider would not have the full picture about how the service is going to be used by the ATS provider. Nevertheless, the interactions ATS/non-ATS might depend on the non-ATS services and the particular set-up. A similar situation might occur between safety case and safety support case(s) for a particular change. Then, it is found not realistic to be precise enough on a possible guidance for the inputs/outputs by both sides, with the high risk of being incomplete.

comment *316* comment by: *UK CAA*

GM1 to AMC6 ATM/ANS.OR.C.005(a)(2)
See also:
AMC6 ATM/ANS.OR.C.005(a)(2) point (d)
GM2 to AMC6 ATM/ANS.OR.C.005(a)(2) points (a), (b), (c) & (d)

Equivalent coverage in EC 2017/373 text: N/A
SWALS as defined in EC 482 cannot be applied to the software covered by Annex III. The ATM IR does not define assurance levels. It allows their use but points out that there can be many different types and that their use does not imply satisfaction of requirement …

Comments:
Not specific to software. Removal of the SW related terms would have no effect on the meaning of the text and would broaden it to include PPE.
Assurance levels can be used in other fields as well e.g. DALs, HWALs
The relationship between confidence and SWALs is not defined and so introducing SWALs should not be done until there is some solid underpinning evidence for such a relationship

response *Noted*

The comment is duly noted.

GM2 to AMC6 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system p. 12-13

comment *37* comment by: *ENAIRE*

AMC6 ATM/ANS.OR.C.005(a)(2) – (a)

ED-153 does not allow requirements without traceabillity (explicit requirement with indepence of the SWAL level). This paragraph should be changed.
Software requirements may be tagged as safety or integrity requirements because its parent requirement (the upper level requirement it traces to) is tagged as safety or integrity related. Therefore a software requirement that does not trace to a requirement above may never be identified as software safety or integrity requirement.

Problem arising: Any software fix implemented in order to solve a problem reported from testing at a higher level, should require the retest of all affected requirements (i.e. all requirements that trace to the requirement associated with the problem) should be verified as not being affected. Any requirement without traceability will never benefit from this relationship and potential fault may be overlooked.

Suggested improvement: Add the following: "Nevertheless all requirements determined as potentially affecting safety, if not implemented correctly or completely, should be traced to a corresponding upper level requirement".

response *Not accepted*

It should be pointed out that derived (non-traced) requirements are possible for other standards different from ED-153. It is considered that both strategies are possible and provide equivalent assurance levels, when applied correctly.

comment *69* comment by: *CANSO*

Remark:
Item (c):Partitioning between several software components with distinct SWAL should be acceptable taken into account the integrity control between data exchanged. It could be an alternative way to reduce SWAL from some sub-components.
Space and timing partitioning consideration should be demonstrated depending on the SWAL criticality.
=> The following sentence is proposed for amendment:
(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. ***In case of integrity control of data exchanges between software components or in case of with space and timing partitioning argumentation, distinct SWAL could be considered.***

response *Not accepted*

It is to be noted that the integrity control between data exchanged is only valid when there is design and implementation independence between the control component and the controlled component. Then, point (c) would not be applicable.

comment *145* comment by: *DSNA*

In some specific cases, some Risk Mitigation Means are foreseen in order to be a response for some hazards. These Risk Mitigation Means could be considered as an acceptable alternative way instead of software safety support assessment.
=> The following sentence is proposed for amendment and should be added : *"An acceptable alternative way for software safety support assessment could be the demonstration of existence of adequate Risk Mitigation Means."*

response *Not accepted*

The term 'software safety support assessment' is not used in the proposed set of AMC & GM.

comment *167* comment by: *DSNA*

Item (c):Partitioning between several software components with distinct SWAL should be acceptable taken into account the integrity control between data exchanged. It could be an alternative way to reduce SWAL from some sub-components.
Space and timing partitioning consideration should be demonstrated depending the SWAL criticality.
=> The following sentence is proposed for amendment:
"(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. ***In case of integrity control of data exchanges between software components or in case of with space and timing partitioning argumentation, distinct SWAL could be considered.****"*

response *Not accepted*

It is to be noted that the integrity control between data exchanged is only valid when there is design and implementation independence between the control component and the controlled component. Then, point (c) would not be applicable.

comment *181* comment by: *DSNA*

In some specific cases, for instance, meteorological services, the assessment of the software providing the service support is out of the managerial control scope from the ANSP. Therefore, software assessment of support services can't be assessed by the ANSP.
=> The following sentence is proposed for amendment and should be added : *"In case the support is out of the definition and/or managerial control scope, the safety support assessment will be specifically not foreseen."*

response *Not accepted*

It should be highlighted that in the current regulatory framework, 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 air traffic services (ATS), airspace management (ASM), air traffic flow management (ATFM), i.e. air traffic management (ATM) and communication, navigation, or surveillance (CNS). Additionally, the

software aspects for aeronautical information services (AIS) provision are included in Regulation (EU) No 73/2010. On the other hand, it is acknowledged that the MET providers will be affected as regards the software assurance AMC & GM.

EASA considers that some of the service providers other than the ones that are subject to Regulation (EC) No 482/2008 today have a contribution to software (e.g. MET providers, FPD) and in order EASA to take an informed decision, a specific meeting with other stakeholders was organised to address this issue (among others). The discussion clearly concluded that some features of the MET systems are affected by the current regulatory requirements, which also supports the approach taken for the proposed set of AMC & GM; that is, to apply for all service providers of ATM/ANS, including AIS and MET providers, towards software assurance level standardisation.

comment *253* comment by: *NATS*

Para (b) The requirement is that the allocated SWAL be commensurate with the most severe effect that software […] may cause. This fails to take into account the likelihood of the effect. In many cases effects of high severity are less likely, and this likelihood may be reduced by other mitigations in the system.
Issue Software assurance effort will be diverted into reducing likelihoods of severe effects that are already very low, while lower severity effects with higher likelihoods are neglected
Suggestion: Include the likelihood of an outcome in the evaluation of the severity.

response *Not accepted*

There is no general consensus about the need of considering the likelihood in the software assurance level allocation. Even in the software standards, several approaches are presented.

comment *317* comment by: *UK CAA*

GM2 to AMC6 ATM/ANS.OR.C.005(a)(2)
See also
AMC6 ATM/ANS.OR.C.005(a)(2) point (d)
GM1 to AMC6 ATM/ANS.OR.C.005(a)(2) points (a) (b) & (c)

Equivalent coverage in EC 2017/373 text: N/A
SWALS as defined in EC 482 cannot be applied to the software covered by Annex III. The ATM IR does not define assurance levels. It allows their use but points out that there can be many different types and that their use does not imply satisfaction of requirement …

Comments:
Not specific to software. Removal of the SW related terms would have no effect on the meaning of the text and would broaden it to include PPE.

	Assurance levels can be used in other fields as well e.g. DALs, HWALs The relationship between confidence and SWALs is not defined and so introducing SWALs should not be done until there is some solid underpinning evidence for such a relationship
response	*Noted* The comment is duly noted.

GM3 to AMC6 ATM/ANS.OR.C.005(a)(2) Safety support assessment and assurance of changes to the functional system p. 13-14

comment	*24* comment by: *D Winship* para (c) "The definition of the software assurance processes may be based on one of these industrial standards without…." The intent of this statement requires consideration – there is no reason why the service provider can't utilise best practices from a number of the relevant standards. The sentence as currently written could be interpreted as stating they can only select one due to the use of "without combining provisions for different standards". Please clarify intent of this paragraph and consider revision.
response	*Noted* As already explained in the guidance material, it would not be considered as a good practice to combine objectives from different standards as they were developed separately under different considerations and there could be some internal compensation means (one objective is less demanding in a particular standard because another objective is more demanding). On the other hand, the use of the verb 'may' allows the service provider to use the best practices to complement one of the standards or to define the full set of software assurance processes.
comment	*146* comment by: *DSNA* In some specific cases, some Risk Mitigation Means are foreseen in order to be a response for some hazards. These Risk Mitigation Means could be considered as an acceptable alternative way instead of software safety support assessment. => The following sentence is proposed for amendment and should be added : *"An acceptable alternative way for software safety support assessment could be the demonstration of existence of adequate Risk Mitigation Means."*
response	*Not accepted* The term 'software safety support assessment' is not used in the proposed set of AMC & GM.
comment	*151* comment by: *DSNA*

	In item (b), The DO-200B defines constraints on the development and the maintenance of aeronautical data. It is generally used in aeronautical embedded contexts and associated suppliers are familiar to. Moreover, in ATM/AIS context, these objectives could lead to a significant gap which will impact the development cost/planning. This document should be removed from this table. The ED-12C/DO-178C should be removed too due to the fact that the ED-109A/DO-278A already covers same assumptions for ATM context. Note also that DO-278B doesn't exist yet, and should be replaced by DO-278A. Finally, ED109 also should be considered as it is a standard currently used in industry right now (not all software development have switched from ed109 to ed109A).
response	*Partially accepted* The comment is duly considered. Following the order of the referenced Standards, the following should be noted: - DO200B should be retained as the DAT providers are part of the scope of the Regulation as non-ATS providers; - ED12C/DO178C should be retained due to the fact that it is being used as reference by some service providers in Europe; and - the text as regards DO278B has been amended.

comment	*152* comment by: *DSNA* Even if the service provider may be able to validate pre-defined/standard additional software assurance processes, it may not be always able to _define_ them because it requires a high level of expertise on the subject which may not be its core business.
response	*Noted* In order to mitigate such effect, the guidance material includes the reference to these software standards that can be used as reference by the service provider to build the software assurance process. Nevertheless, it is to be pointed out that the software assurance is not a new domain for the ANSPs that were previously implementing Regulation (EC) No 482/2008.

comment	*182* comment by: *DSNA* In some specific cases, for instance, meteorological services, the assessment of the software providing the service support is out of the managerial control scope from the ANSP. Therefore, software assessment of support services can't be assessed by the ANSP. => The following sentence is proposed for amendment and should be added : *"In case the support is out of the definition and/or managerial control scope, the safety support assessment will be specifically not foreseen."*
response	*Not accepted*

It should be highlighted that in the current regulatory framework, 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 air traffic services (ATS), airspace management (ASM), air traffic flow management (ATFM), i.e. air traffic management (ATM) and communication, navigation, or surveillance (CNS). Additionally, the software aspects for aeronautical information services (AIS) provision are included in Regulation (EU) No 73/2010. On the other hand, it is acknowledged that the MET providers will be affected as regards the software assurance AMC & GM.

EASA considers that some of the service providers other than the ones that are subject to Regulation (EC) No 482/2008 today have a contribution to software (e.g. MET providers, FPD) and in order EASA to take an informed decision, a specific meeting with other stakeholders was organised to address this issue (among others). The discussion clearly concluded that some features of the MET systems are affected by the current regulatory requirements, which also supports the approach taken for the proposed set of AMC & GM; that is, to apply for all service providers of ATM/ANS, including AIS and MET providers, towards software assurance level standardisation.

comment *269* comment by: *ASD/Thales Air Systems*

To not create confusion, it is very important to not mix standards for airborne systems like DO-178C and standards for ground systems like ED-109A. A unique list may be confusing for a Service Provider that is not aware about the techncal content of those standards and may require the compliance to DO-178C to ground systems manufacturers. This confusion between standards could create a climate of incomprehension that could hinder functional improvement initiatives in ATM systems. Moreover, safety management systems put in place by ATM ground manufacturers are based on ATM standards (e.g. ED-109A, ED-153), and it will represent a blocking industrial issue to comply with standards, such as DO-178C, not adapted to ATM ground systems.

That is the reason why i**t appears necessary to separate these 2 different categories of standards** (airborne standards vs ground standards).

response *Not accepted*

It should be acknowledged that the scope of each document, i.e. standard, indicates the intended domain of applicability. This is especially relevant taking into account the possibility of identifying ATM/ANS systems with ground and space components.

comment *283* comment by: *ASD/Thales Air Systems*

In the item (c), it is written that "The definition of the software assurance processes **may be** based on one of these industrial standards ...". From an industrial point of view, we know very well the technical content of these standards and we also know that requiring a compliance to provisions/requirements coming from different

standards is a strong source of confusion. This is the reason why it appears useful to be more strict on this topic by writting for example: "The definition of the software assurance processes **should be** based on one of these industrial standards ...".

response *Not accepted*

Being guidance material and providing a non-exhaustive list of standards, the current wording is considered more suitable. It is acknowledged that there are other ANSPs that base the software assurance process on other standards (CMMI).

comment *318* comment by: *UK CAA*

GM3 to AMC6 ATM/ANS.OR.C.005(a)(2) point (a)

Equivalent coverage in EC 2017/373 text: N/A

Comments:
Not specific to software. Removal of the SW related terms would have no effect on the meaning of the text and would broaden it to include PPE.
This section is out of context. The approval of processes is covered in ATM/ANS.OR.B.10 and its associated AMC/GM

response *Noted*

The comment is duly noted.

It is preferred to keep this material linked to the functional system. It is noted that the software development process can also be established at system supplier level, supporting a special treatment for these processes.

comment *319* comment by: *UK CAA*

GM3 to AMC6 ATM/ANS.OR.C.005(a)(2) point (c)

Equivalent coverage in EC 2017/373 text: N/A

Comments:
Not specific to software. Removal of the SW related terms would have no effect on the meaning of the text and would broaden it to include PPE.
This section is out of context. The approval of processes is covered in ATM/ANS.OR.B.10 and its associated AMC/GM

response *Noted*

The comment is duly noted.

AMC3 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system p. 14

comment *70* comment by: *CANSO*

Remark:
In item (a), in case of modifications to existing software, the existence of documented software assurance processes could not be systematically available, especially if the development was performed several years before.
Additionally, the state of art at the moment for the previous development could be significantly different as the current standards.
In these cases, the effective software experience could be claimed without any existence of documentation. It is noted that the software experience is already well addressed by the bullet (b), nevertheless, as written, it seems not being an alternative way to the bullet (a).
=> The following sentence is proposed for amendment:

(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. In case of incomplete or absence to this expected documentation, the effective software experience, if exists, could be considered as a relevant alternative way.

response *Not accepted*

It is necessary to point out that as described in AMC6 ATM/ANC.OR.C.005(a)(2), (f), it is always possible to have specific software assurance processes for managing previously developed software and to use the technique that is mentioned in the comment. Based on the existence of this provision, it is not considered necessary to include the additional clarification proposed by the commentator.

comment *81* comment by: *EUROCONTROL*

ATS.OR.205(a)(2) - Pages 14 to 19

(Same comment as for ATM/ANS.OR.C.205(a)(2)).

The EUROCONTROL Agency finds that there is no AMC/GM explaining how the criticality of the software (SWAL) is linked to the criticality of the application. This might lead, for the same functional system, to a situation with different SWAL allocations by different ANSPs, although for the same required application. It would be therefore beneficial at European level to rely on a standardised mechanism for SWAL allocation, depending on the criticality of the application.

response *Noted*

The comment is duly considered.

It is agreed that there is a difference between the criticality of the software and the criticality of the particular application by an ANSP. The same software can be used in different contexts by several ANSPs. Nevertheless, the objective of the AMC & GM is

to address the software assurance aspects associated with the software, once the criticality of the application has been addressed by the ANSP.

On the other hand, EASA concurs with the idea of having a common European SWAL allocation matrix, as currently presented in some of the software standards. However, Regulation (EU) 2017/373 and the existing AMC & GM do not go in that direction regarding the severity classification scheme and risk classification scheme, where there is no harmonised severity classification scheme (as there is today under Regulation (EU) No 1035/2011). Then, this limits the possibility of establishing a common European SWAL allocation matrix.

comment *118* comment by: *ENAV*

In item (a), in case of modifications to existing software, the existence of documented software assurance processes could not be systematically available, especially if the development was performed several years before.
Additionally, the state of art at the moment for the previous development could be significantly different as the current standards.
In these cases, the effective software experience could be claimed without any existence of documentation. It is noted that the software experience is already well addressed by the bullet (b), nevertheless, as written, it seems not being an alternative way to the bullet (a).
=> The following sentence is proposed for amendment:

(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. In case of incomplete or absence to this expected documentation, the effective software experience, if exists, could be considered as a relevant complementary way.

response *Not accepted*

It is necessary to point out that as described in AMC6 ATM/ANC.OR.C.005(a)(2), (f), it is always possible to have specific software assurance processes for managing previously developed software and to use the technique that is mentioned in the comment. Based on the existence of this provision, it is not considered necessary to include the additional clarification proposed by the commentator.

comment *168* comment by: *DSNA*

In item (a), in case of modifications to existing software, the existence of documented software assurance processes could not be systematically available, especially if the development was performed several years before.
Additionally, the state of art at the moment for the previous development could be significantly different as the current standards.
In these cases, the effective software experience could be claimed without any

existence of documentation. It is noted that the software experience is already well addressed by the bullet (b), nevertheless, as written, it seems not being an alternative way to the bullet (a).
=> The following sentence is proposed for amendment:
"(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. ***In case of incomplete or absence to this expected documentation, the effective software experience, if exists, could be considered as a relevant alternative way****."*

response *Not accepted*

It is necessary to point out that as described in AMC6 ATM/ANC.OR.C.005(a)(2), (f), it is always possible to have specific software assurance processes for managing previously developed software and to use the technique that is mentioned in the comment. Based on the existence of this provision, it is not considered necessary to include the additional clarification proposed by the commentator.

comment *201* comment by: *AESA/DSANA*

As it is suggested for "AMC5 ATM/ANS.OR.C.005(a)(2)", the need of a "documented software assurance process" should be more evident and unambiguous. It is considered that requirements about defining and establishing SW safety assessment and assurance procedures should be stated as an AMC of ATM/ANS.OR.B.010 (a) "Change management procedures".

The wording proposed for the previous comment is also applicable here.

response *Not accepted*

It is preferred to keep this material linked to the functional system. It is also noted that the software development process can also be established at system supplier level, supporting a special treatment for these processes.

comment *202* comment by: *AESA/DSANA*

AMC3 ATS.OR.205(a)(2) should include Software Assurance Levels (SWALs) instead of only "Assurance Levels"

AMC3 ATS.OR.205(a)(2) paragraph (b) should include SWAL to be consistent with AMC5 ATM/ANS.OR.C.005(a)(2) paragraph (b).
In general "Software Assurance Level"/SWAL is used as synonymous of "assurance level" in the NPA. Since Software Assurance Level (SWAL) has specific connotations in the ED-153, the wording should be reviewed in order to avoid misunderstanding.

response *Partially accepted*

It is noted that the term 'SWAL' is not used in other standards (e.g. ED-109A). However, it is preferred to keep the assurance level term in a more generic way, at least, in this point, while in other points the term 'SWAL' is introduced.

comment *227* comment by: *DSAC - FR NSA*

Which is the severity classification scheme refered to in this paragraph ? The service provider's SCS ? The SCS defines by the Competent Authority ?

response *Noted*

According to Regulation (EU) 2017/373, the severity classification scheme is defined/proposed by the service providers. This is further illustrated in the associated AMC & GM.

comment *320* comment by: *UK CAA*

Annex IV

AMC3 ATS.OR.205(a)(2)

Equivalent coverage in EC 2017/373 text: ATS.OR.205 (a)(2)

Comments:
Not specific to software. Removal of the SW related terms would have no effect on the meaning of the text and would broaden it to include PPE.
Most of these points (see below) are covered by AMC/GM related to ATM/ANS.OR.B.005, B.010 & ATS.OR.200 & 205

response *Noted*

It is preferred to keep this material linked to the functional system. It is noted that the software development process can also be established at system supplier level, supporting a special treatment for these processes.

comment *321* comment by: *UK CAA*

AMC3 ATS.OR.205(a)(2), point (a)

Equivalent coverage in EC 2017/373 text:
ATM/ANS.OR.B.010 (a)
ATS.OR.205 (a)(2)Comments:
SW is part of a functional system. Before changing any part of a functional system the service provider must ensure that the procedures to be used are approved by the CA. This is covered in ATM/ANS.OR.B.010.

response *Noted*

The comment is duly noted.

comment *322* comment by: *UK CAA*

AMC3 ATS.OR.205(a)(2) point (b)

Equivalent coverage in EC 2017/373 text:
ATM/ANS.OR.B.005 (a)(4), (c) & (d)
ATM/ANS.OR.B.010 (b) & (c)
ATS.OR.200 (3)

Comments:
The management system rules cover the reporting, analysis and correction of failures of the functional system and adequate performance of procedures. They cover the complete functional system and change management procedures and therefore, by definition, cover software.

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

AMC4 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system p. 15-16

comment *5* comment by: *DFS Deutsche Flugsicherung GmbH*

The text of Regulation 482/2008 has not always been copied identically within the AMC, e.g. point AMC4 ATS.OR.205 (a) (2) ii) has been modified. ED-153 is in line with Regulation 482/2008, however is not with Regulation 2017/373 ATS.OR.205.
GMs contain both copies from ED documents as well as additional and modified parts. This mixture between referencing, copying and modifying is not acceptable.
When the requirements are being changed, then also the ED documents need to be modified as well. Previous means to comply become partially non-compliant by new GM. This creates legal confusion rather than clarity.
Therefore, a complete revisiting of the IR and AMC/GM material is recommended.

response *Noted*

The aim of the proposed set of AMC & GM is to provide means of compliance for the software assurance when introducing changes to the functional system. The need for this additional material regarding software assurance was expressed by several stakeholders, especially authorities, during the Comitology process that resulted in Regulation (EU) 2017/373. Other ways for demonstration of compliance are also possible and need to be evaluated by the corresponding regulated parties.

On the other hand, EASA has established RMT.0719 on regular updates of the subject implementing measures. And based on standardisation and implementation

feedback, EASA will perform, on a regular basis, a review of identified or notified subjects, which could lead to amendments to the rules, and, where appropriate, may propose amendments to the IRs and/or AMC & GM.

comment *6* comment by: *DFS Deutsche Flugsicherung GmbH*

The following contradiction should be removed or better explained under GM:
The traceability as required by (a) (2) is not supported by ED-153, as ED-153 explicitly does not allow "derived requirements".
GM3 to AMC4 ATS.OR.205 (a)(2) however refers to ED-153.

response *Noted*

There are two separate aspects that require attention:

- Derived requirements are allowed by other software standards. Both approaches (ED-153 or ED-109A) would be acceptable, provided that they are applied according to the corresponding standard.
- ED-153 is listed in GM3 to AMC4 as an example of the different alternatives.

comment *17* comment by: *D Winship*

Software requirements "correct, complete and compliant with the upper level requirements"
Use of "compliant …upper level" requirements implies a multi-layered requirements set which may, or may not be, the case. The different levels of system/software requirements should be consistent, coherent and 'aligned with', rather than 'compliant with', each other (as compliance is normally verified *for* each requirement as opposed to *between* different levels of requirements).

Replacing this text with "aligned with the system requirements" would appear to be more appropriate.

response *Not accepted*

Based on existing software standards (ED-153, ED-109A), it is preferred to maintain the term 'compliant'. Regarding the upper-level and system requirements, the use of the term 'upper level' gives the possibility to address a multi-layered software component, as it is the case in most of the software applications in the ATM/ANS domain.

comment *19* comment by: *D Winship*

section a(5)
"following verification methods…agreed with the CA" –
It is essential to recognise that the CA focus is on the adequacy of the verification results/assurance – it is neither practical, achievable or desirable for the CA to engage in approving "verification methods" for individual changes. In addition, the

	text as written doesn't take into account the reality that, in most projects, much of the software is not unique or custom designed specifically for a single service provider – some of the verification work on core functionality may have been completed long before the service provider and CA became involved (i.e. re-used software from other projects). Some of the results of this earlier verification activity could be permissible as evidence (e.g. 'core' algorithm testing) even though the CA hasn't been engaged in agreeing the "verification method". This text should be reconsidered – the original text from 482 (with NSA replaced by CA) appears more appropriate. "The EATMN software shall be adequately verified by analysis and/or testing and/or equivalent means, as agreed with the…"
response	*Accepted* Considering the comment, the text has been amended.

comment	*38* comment by: *ENAIRE* AMC4 ATS.OR.205 (a) is confuse. It should be explained in order to system requirements, software requirements, software design requirements. It is easier than talk in terms of "upper level requirements".
response	*Partially accepted* Considering the comment the text has been amended to promote clarity.

comment	*43* comment by: *CANSO* The text of Regulation 482/2008 has not always been copied identically within the AMC, e.g. point AMC4 ATS.OR.205 (a) (2) ii) has been modified. ED-153 is in line with Regulation 482/2008, however is not with Regulation 2017/373 ATS.OR.205. GMs contain both copies from ED documents as well as additional and modified parts. This mixture between referencing, copying and modifying is not acceptable. When the requirements are being changed, then also the ED documents need to be modified as well. Previous means to comply become partially non-compliant by new GM. This creates legal confusion rather than clarity. Therefore, a complete revisiting of the IR and AMC/GM material is recommended.
response	*Noted* The aim of the proposed set of AMC & GM is to provide means of compliance for the software assurance when introducing changes to the functional system. The need for this additional material regarding software assurance was expressed by several stakeholders, especially authorities, during the Comitology process that resulted in Regulation (EU) 2017/373. Other ways for demonstration of compliance are also possible and need to be evaluated by the corresponding regulated parties. On the other hand, EASA has established RMT.0719 on regular updates of the subject implementing measures. And based on standardisation and implementation

feedback, EASA will perform, on a regular basis, a review of identified or notified subjects, which could lead to amendments to the rules, and, where appropriate, may propose amendments to the IRs and/or AMC & GM.

comment *71* comment by: *CANSO*

Remark:
As stated in item (a)(1)(ii), one may understand that the demonstration is covering all the software. Actually, the demonstration should only cover the scope of the change.
=> The following sentence is proposed for amendment:

(a)(1)(ii) specify in the scope of the change,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 new software or modified software part.

response *Not accepted*

It must be highlighted that the requirement refers to features requested in the software assurance process. They can be applied for a particular change but the processes should be change-independent.

comment *72* comment by: *CANSO*

Remark:
Sentence of item (2)(i) seems to be ambiguous and clarification is expected.
=> The following sentence is proposed for amendment:

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

response *Partially accepted*

Considering the comment, the text has been amended to promote clarity.

However, it should be noted that the proposed solution was different from the original text and the intent of the rule.

comment *77* comment by: *Swedish Transport Agency, Civil Aviation Department (Transportstyrelsen, Luftfartsavdelningen)*

Part a 1
Provides a clear link between software assurance and safety assessment of changes... good!

response *Noted*

comment	*119* comment by: *ENAV* The text of Regulation 482/2008 has not always been copied identically within the AMC, e.g. point AMC4 ATS.OR.205 (a) (2) ii) has been modified. ED-153 is in line with Regulation (EC) No 482/2008; however, it is not with Regulation (EU) 2017/373 ATS.OR.205. GM contain both copies from ED documents as well as additional and modified parts. This mixture between referencing, copying and modifying is not acceptable. When the requirements are being changed, then also the ED documents need to be modified as well. Previous means to comply become partially non-compliant by new GM. This creates legal confusion rather than clarity. Therefore, a complete revisiting of the IR and AMC & GM is recommended.
response	*Noted* The aim of the proposed set of AMC & GM is to provide means of compliance for the software assurance when introducing changes to the functional system. The need for this additional material regarding software assurance was expressed by several stakeholders, especially authorities, during the Comitology process that resulted in Regulation (EU) 2017/373. Other ways for demonstration of compliance are also possible and need to be evaluated by the corresponding regulated parties. On the other hand, EASA has established RMT.0719 on regular updates of the subject implementing measures. And based on standardisation and implementation feedback, EASA will perform, on a regular basis, a review of identified or notified subjects, which could lead to amendments to the rules, and, where appropriate, may propose amendments to the IRs and/or AMC & GM.

comment	*120* comment by: *ENAV* Remark: Sentence of item (2)(i) seems to be ambiguous and clarification is expected. => The following sentence is proposed for amendment: (i) Each software requirement introduced at each level in the design lifecycle should be traced to the same level of ~~design~~ lifecycle at which its satisfaction is demonstrated.
response	*Partially accepted* Considering the comment, the text has been amended to promote clarity. However, it should be noted that the proposed solution was different from the original text and the intent of the rule.

comment	*137* comment by: *ISAVIA ohf.* Comment to AMC4 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system (page 15-16):

Please note that according to Regulation (EU) 2017/373 there is no requirement to identify safety objectives as part of the safety risk assessment. The text should be reworded to reflect this.

response *Accepted*

Considering the comment, the text has been amended.

comment *169* comment by: *DSNA*

As stated in item (a)(1)(ii), one may understand that the demonstration is covering all the software. Actually, the demonstration should only cover the scope of the change.
=> The following sentence is proposed for amendment: *"(a)(1)(ii) specify in the scope of the change,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 new software or modified software part."*

response *Not accepted*

It must be highlighted that the requirement refers to features requested in the software assurance process. They can be applied for a particular change but the processes should be change-independent.

comment *172* comment by: *DSNA*

Sentence of item (2)(i) seems to be ambiguous and clarification is expected.
=> The following sentence is proposed for amendment: *"(i) Each software requirement introduced at each level in the ~~design~~ **lifecycle** should be traced to the same level of ~~design~~ **lifecycle** at which its satisfaction is demonstrated."*

response *Partially accepted*

Considering the comment, the text has been amended to promote clarity.

However, it should be noted that the proposed solution was different from the original text and the intent of the rule.

comment *207* ❖ comment by: *European Transport Workers Federation - ETF*

p10 : non-ATS services AMC6 (a)(2)(ii) Each software requirement [...] **should be traced** to an upper level requirement [...] p15 : ATS services : AMC4 (a)(2)(ii) Each software requirement [...] **is traced to** an upper level requirement [...]	Is the difference intended ? From a regulatory perspective, it does not seem to create any difference in the provision or at least we do not understand it.

response *Accepted*

The text has been amended to address the inconsistency.

comment *208* ❖ comment by: *European Transport Workers Federation - ETF*

p11 : non-ATS services : AMC6 (f) [...] If no sufficient assurance **can** be provided [...] p16 : ATS services : AMC4 (e) [...] If no sufficient assurance **may** be provided [...]	Is the difference intended ? From a regulatory perspective, it does not seem to create any difference in the provision or at least we do not understand it.

response *Accepted*

The text has been amended to address the inconsistency.

comment *228* comment by: *DSAC - FR NSA*

In paragraph (3), The demonstration that the software implementation contains no functions which adversely affect safety may be difficult to achieve especially for COTS.
This paragraph may be rephrased as "the functions contained in the software implementation do not adversely affect safety".

response *Partially accepted*

For COTS, specific assurance process can be defined by the service provider as highlighted in point (f) of the AMC. The reference to the software implementation is considered equivalent to the wording and covers the case of the COTS where activated functions need to be assessed from the potential impact on safety or service specifications.

comment *239* comment by: *NATS*

para (b) (1) “a known executable version of the software” seems too imprecise; the “known” version should be the one that is to be deployed into operation

Suggest: rewording to "the executable version of the software which is to be deployed into operation"

response *Not accepted*

The verification activities can be based on several (known) versions of the software, without mandatorily being the last one. An assessment of the versions evolutions might allow to take credit of the verification in previous versions of particular requirements, subject to a non-regression policy.

comment *255* comment by: *NATS*

para (a) (1) (ii) and (a) (4) Although a straight copy of the EC 482/2008 requirement the concept of "software resource usage on target hardware" is not required. It could be argued that to meet the other software requirements as stated (such as performance and overload tolerance) "software resource usage" must be met.

Issue: Difficult to specify and meet especially for software deployed within a virtualised environment.
Suggest the removal of the statement "software resource usage on target hardware" from the list.

response *Accepted*

comment *256* comment by: *NATS*

Para (a) (5) Its unclear as to the scope of the agreement with respect to verification with the CA i.e. is the intention a strategy or a requirement by requirement verification method or selection from an agreed set of verification methods?
Issue: Potential inconsistency of application. Effort required from CA associated with agreeing software verification approach.
Suggested resoultion; Clarification dependent upon the intention of the statement.

response *Accepted*

The text has been updated to promote clarity in order to avoid this potential misunderstanding.

comment *257* comment by: *NATS*

Para (b) As written there is no means to use arguments or evidence from previous versions of software if suitably justified.
Impact: Unnecessary re-generation of assurance evidence, with associated cost.
Suggested Resolution: Modify (3) to read "that have been used in the production of that version, or can be justified as applicable to that version.'

response *Accepted*

comment *258* comment by: *NATS*

Para (e) It is not necessarily true that “generic assurance processes cannot be applied” to COTS, NDS or PDS. It is however unlikely.
Issue: Remove the inference that generic assurance approach is not applicable to these types of software.
Suggested resolution: Modify “generic assurance processes cannot be applied” to “generic assurance processes may not be applicable”

response *Not accepted*

The intent of the current wording is to highlight the impossibility to apply the generic assurance process. There would be some COTS or NDS where the generic assurance process is possible and can be provided by the COTS supplier.

comment *259* comment by: *NATS*

Para (e) Modify last sentace for readability - it requires clarity
Suggestion: Modify to read “If sufficient assurance cannot be provided, complementary….”

response *Accepted*

comment *260* comment by: *NATS*

Para (e) In themselves neither “existing service level experience” nor “monitoring” are a “mitigation means aiming at decreasing the impact of specific failure modes of this type of software”, whereas software/system architectural considerations are.
Issue: Confusion between failure mode mitigation and means of addressing assurance shortfalls. General clarity
Suggestion: Reword preceding test to read “If sufficient assurance cannot be provided, complementary mitigation should be applied. This may include but is not limited to:”

response *Not accepted*

It should be noted that the three cases presented would belong to the mitigation of specific failure modes pre- and post-implementation.

comment *286* ❖ comment by: *ASD/Thales Air Systems*

In the item (a)(1)(ii), it is mentionned "specify the functional behaviour in ... downgraded modes ..." and later "... robustness to abnormal operating conditions ...". What is the difference between the 2 points? It seems that these 2 points are redundant o at least linked since requirements on "downgraded modes" cover "robustness to abnormal operating conditions". May be the last part of the sentence could be used as an example of downgraded mode.

response *Noted*

Downgraded modes might correspond to a situation in which the software provides lower performances but works under normal operating conditions. Then, both concepts are separate and would need to be maintained in this way.

comment *323* comment by: *UK CAA*

AMC4 ATS.OR.205(a)(2)

Comments:
Not specific to software. Removal of the SW related terms would have no effect on the meaning of the text and would broaden it to include PPE.
Most of these points (see below) are covered by AMC/GM related to ATS.OR.205
This section is out of context. Processes are dealt with in ATM/ANS.OR.B.010 and its associated AMC/GM. This section of the IR and its associated AMC/GM deals with the criteria for safety assurance cases and not the processes that created a safety case.

response *Noted*

comment *324* comment by: *UK CAA*

AMC4 ATS.OR.205(a)(2), point (a)(1)(i)

Equivalent coverage in EC 2017/373 text:
AMC2 ATS.OR.205 (a)(2) (b), (c), (d)

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *325* comment by: *UK CAA*

AMC4 ATS.OR.205(a)(2), point (a)(1)(ii)

Equivalent coverage in EC 2017/373 text:
ATS.OR.205 (a)(1)(v)
GM3 ATS.OR.205(a)(2) (a)

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *326* comment by: *UK CAA*

AMC4 ATS.OR.205(a)(2), point (a)(2)(i)

Equivalent coverage in EC 2017/373 text: AMC2 ATS.OR.205(a)(2) (d)

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *327* comment by: *UK CAA*

AMC4 ATS.OR.205(a)(2), point (a)(2)(ii)

Equivalent coverage in EC 2017/373 text: AMC2 ATS.OR.205(a)(2) (d)

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *328* comment by: *UK CAA*

AMC4 ATS.OR.205(a)(2), point (a)(3)

Equivalent coverage in EC 2017/373 text:
ATS.OR.205 (a)(2) & (b)(2)(ii)
AMC2 ATS.OR.205 (a)(2) (a) & (c)

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *329* comment by: *UK CAA*

AMC4 ATS.OR.205(a)(2) point (a)(4)

Equivalent coverage in EC 2017/373 text:
ATS.OR.205 (a)(5)(ii)
AMC2 ATS.OR.205(a)(2) (c) & (e)

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *330* comment by: *UK CAA*

AMC4 ATS.OR.205(a)(2), point (a)(5)

Equivalent coverage in EC 2017/373 text:
ATS.OR.205 (a)(2), (b)(1)
AMC1 ATS.OR.205 (b)(5)

Comments:
The procedures for verification are covered in ATM/ANS.OR.B.010 and its associated AMC/GM and will have been agreed with the CA prior to their use.

response *Noted*

It should be noted that software verification procedures may also be available at system supplier level. Therefore, the link to these procedures to the functional system change is considered also relevant.

comment *331* comment by: *UK CAA*

AMC4 ATS.OR.205(a)(2), point (b)

Equivalent coverage in EC 2017/373 text: AMC2 ATS.OR.205 (a)(2) (f)

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *332* comment by: *UK CAA*

AMC4 ATS.OR.205(a)(2) point (c)
See also:
GM1 to AMC4 ATS.OR.205(a)(2)
(Text identical to GM1 to AMC6 ATM/ANS.C.005(a)(2))
GM2 to AMC4 ATS.OR.205(a)(2) points (a), (b) & (c)
(Text the same as GM2 to AMC6 ATM/ANS.C.005(a)(2))

Equivalent coverage in EC 2017/373 text: N/A

Comments:
The concept of rigour is not used in the IR, confidence is used. Assurance levels are used in Regulation (EC) No 482/2008 to determine 'the rigour to which the assurances are established'. This can only be understood as a means to provide the required level of confidence. Hence this clause is incorrect.

response *Accepted*

Considering the comment, the text has been amended.

comment *333* comment by: *UK CAA*

AMC4 ATS.OR.205(a)(2), point (d)(1)

Equivalent coverage in EC 2017/373 text:
ATM/ANS.OR.B.030 (a), (b) & (c)
AMC2 ATS.OR.205 (a)(2) (f)

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *334* comment by: *UK CAA*

AMC4 ATS.OR.205(a)(2), point (d)(2)

Equivalent coverage in EC 2017/373 text:
ATM/ANS.OR.B.005 (a)(4), (c) & (d)
ATM/ANS.OR.B.030 (a), (b) & (c)

Comments:
The management system rules cover the reporting, analysis and correction of failures of the functional system.

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *335* comment by: *UK CAA*

AMC4 ATS.OR.205(a)(2), point (d)(3)
See also:
AMC6 ATM/ANS.OR.C.005(a)(2), point (e)(3)

Equivalent coverage in EC 2017/373 text: ATM/ANS.OR.B.030 (a), (b) & (c)

Comments: Not specific to software.

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment *336* comment by: *UK CAA*

AMC4 ATS.OR.205(a)(2), point (e)

Equivalent coverage in EC 2017/373 text: None

Comments:
Incorrect.
The requirement for assurance (ATS.OR.205(a)(2)) applies to all parts of the functional system and therefore includes software, no matter whether it is bespoke, COTS or previously developed.
This is GM not AMC. The rule itself is adequate, it covers this and is not specific to software.

response *Noted*

The comment is duly noted.

EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

AMC4 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system p. 16-17

comment	*7* comment by: *DFS Deutsche Flugsicherung GmbH* GM1 to AMC4 The structure of the GM is misleading, since the classification criteria in sub-para (c) (2) (i)-(iii) are always applicable, not only for multiple SWALs. We suggest to restructure the paragraph to avoid misunderstanding.
response	*Not accepted* It should be noted that the considerations included in this point are only applicable where there are several SWALs covered by the same set of software assurance processes.

comment	*21* comment by: *D Winship* Para (c) "The use of multiple SWALs…several criticalities of software …by same set of software assurance processes". This text is potentially misleading as the software assurance system may be designed to invoke more comprehensive and rigorous processes for more critical code – in other words not employing the **same** set of processes.
response	*Noted* It should be noted that the processes are written in general terms. Typically, software suppliers have a unique set of software development process that are able to cope with several software assurance levels, depending on the activities carried out.

comment	*22* comment by: *D Winship* Para (c) "processes are **intended to rely on** several software assurance levels". Suggest replace 'intended to rely on' with 'employ'. Assurance processes don't '**rely'** on SWALs, assurance evidence rigour is driven by the software's designated SWAL(s).
response	*Accepted*

comment	*45* comment by: *CANSO* GM1 to AMC4 The structure of the GM is misleading, since the classification criteria in sub-para (c) (2) (i)-(iii) are always applicable, not only for multiple SWALs. We suggest to restructure the paragraph to avoid misunderstanding.
response	*Not accepted* It should be noted that the considerations included in this point are only applicable where there are several SWALs covered by the same set of software assurance process.

comment	*121* comment by: *ENAV* GM1 to AMC4 The structure of the GM is misleading, since the classification criteria in sub-para (c) (2) (i)-(iii) are always applicable, not only for multiple SWALs. We suggest to restructure the paragraph to avoid misunderstanding
response	*Not accepted* It should be noted that the considerations included in this point are only applicable where there are several SWALs covered by the same set of software assurance process.

comment	*131* comment by: *Avinor Air Navigation Services (Avinor Flysikring AS)* **Comment to GM1 to AMC4 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the fundtional system** **(c)(2)(i) required to be achieved with independence;** It should be more precisely described what is required by the term "independence" for requirements which needs to be achieved with independence. **Justification:** The term "independence" is vaguely described in ED-153.
response	*Noted* It should be noted that 'independence' is defined in ED-109A as 'Verification independence is achieved when the verification activity is performed by a person(s) other than the developer of the item being verified'. ED-109A Standard is considered within the standards list.

comment	*229* comment by: *DSAC - FR NSA* Paragraph (d) doesn't provide added guidance to AMC4 ATS.OR.205(a)(2) - € regarding the "alternative means […] to demonstrate", therefore it could be removed.
response	*Accepted*

comment	*261* comment by: *NATS* **Para (d)** It is not necessarily true that "generic assurance processes cannot be applied" to COTS, NDS or PDS. It is however unlikely. **Issue:** Remove the inference that generic assurance approach is not applicable to these types of software. **Suggestion:** Modify "generic assurance processes cannot be applied" to "generic assurance processes may not be applicable"
response	*Not accepted*

It should be noted that the current wording intends to highlight the impossibility to apply the generic assurance process. There would be some COTS or NDS where the generic assurance process is possible and can be provided by the COTS supplier.

comment *337* comment by: *UK CAA*

GM1 to AMC4 ATS.OR.205(a)(2)
(Text nearly the same as GM1 to AMC6 ATM/ANS.C.005(a)(2))
See also:
AMC4 ATS.OR.205(a)(2) point (c)
GM1 to AMC4 ATS.OR.205(a)(2)
(Text identical to GM1 to AMC6 ATM/ANS.C.005(a)(2))

Equivalent coverage in EC 2017/373 text: N/A
The ATM IR does not define assurance levels. It allows their use but points out that there can be many different types and that their use does not imply satisfaction of requirement …
See GM2 ATS.OR.205(a)(2)

Comments:
Not specific to software. Removal of the SW related terms would have no effect on the meaning of the text and would broaden it to include PPE.
Assurance levels can be used in other fields as well e.g. DALs, HWALs
The relationship between confidence and SWALs is not defined and so introducing SWALs should not be done until there is some solid underpinning evidence for such a relationship

response *Noted*

The comment has been duly considered.

comment *338* comment by: *UK CAA*

GM1 to AMC4 ATS.OR.205(a)(2) points (a)

Equivalent coverage in EC 2017/373 text: ATS.OR.205(a)(2)

Comments:
Incorrect ref – should be ATS.OR.205(a)(2)
Tautology – This simply says that the assurance should be provided with the required level of confidence.

response *Not accepted*

comment *339* comment by: *UK CAA*

GM1 to AMC4 ATS.OR.205(a)(2) points (b)

Equivalent coverage in EC 2017/373 text: GM2 ATS.OR.205(a)(2)

response	*Noted* EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment	*340* comment by: *UK CAA* **GM1 to AMC4 ATS.OR.205(a)(2) points (c)** **Equivalent coverage in EC 2017/373 text: None**
response	*Noted* EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

comment	*341* comment by: *UK CAA* **GM1 to AMC4 ATS.OR.205(a)(2) points (d)** **Equivalent coverage in EC 2017/373 text: None**
response	*Noted* EASA believes that the aspects identified in the AMC & GM are not covered in the existing AMC & GM with the necessary level of detail, taking into account the particularities and specificities of the software-related activities.

GM2 to AMC4 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system p. 17

comment	*48* comment by: *CANSO* *(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."* Clarify if the architecture and/or procedural defences identified are existing defences, defences that have to be implemented (Safety Requirement) or both of them.
response	*Accepted*

Considering the comment and the intent to correspond to 'both of cases', the text has been amended accordingly to promote clarity.

comment *73* comment by: *CANSO*

Remark:
Item (c):Partitioning between several software components with distinct SWAL should be acceptable taken into account the integrity control between data exchanged. It could be an alternative way to reduce SWAL from some sub-components.
Space and timing partitioning consideration should be demonstrated depending on the SWAL criticality.
=> The following sentence is proposed for amendment:
(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. ***In case of integrity control of data exchanges between software components or in case of with space and timing partitioning argumentation, distinct SWAL could be considered***

response *Not accepted*

It should be noted that that the integrity control between data exchanged is only valid when there is design and implementation independence between the control component and the controlled component. Then, point (c) would not be applicable.

comment *122* comment by: *ENAV*

(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."

Clarify if the architecture and/or procedural defences identified are existing defences, defences that have to be implemented (Safety Requirement) or both of them

response *Accepted*

Considering the comment and the intent to correspond to 'both of cases', the text has been amended accordingly to promote clarity.

comment *130* comment by: *Avinor Air Navigation Services (Avinor Flysikring AS)*

Comment to (b):
Worst effect should be replaced with worst *credible* effect and other mitigations in place should be taken into account.

Justification: One of the weaknesses with SWAL is the likelihood x most severe effect. Most severe effect will most likely be very serious (using worst case effect, instead of worst credible, and not taking other mitigations into account), and the definitions of likelihood is very vague, resulting in that the outcome/derived SWAL level can be whatever the people working on it wants it to be.

response *Accepted*

Considering the comment, the text has been amended accordingly.

comment *170* comment by: *DSNA*

Item (c):Partitioning between several software components with distinct SWAL should be acceptable taken into account the integrity control between data exchanged. It could be an alternative way to reduce SWAL from some sub-components.
Space and timing partitioning consideration should be demonstrated depending the SWAL criticality.
=> The following sentence is proposed for amendment:
"(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. ***In case of integrity control of data exchanges between software components or in case of with space and timing partitioning argumentation, distinct SWAL could be considered****."*

response *Not accepted*

It should be noted that that the integrity control between data exchanged is only valid when there is design and implementation independence between the control component and the controlled component. Then, point (c) would not be applicable.

comment *230* comment by: *DSAC - FR NSA*

Only ED-153 provides a methodology to allocate SWAL and it is not sufficiently detailed and "constraining" to assure that SWAL will be allocated on the same way by all users. A more detailed GM would help to harmonize SWAL allocation.

response *Noted*

There are some particularities depending on the way that the safety (support) assessment is applied by each ANSP. It is noted that the current AMC & GM on changes to functional system does not have a reference severity classification scheme for hazard effects different from accident (catastrophic). This aspect will be considered for future rulemaking activity.

comment *262* comment by: *NATS*

Para (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." Where this is the case, appropriate partitioning needs to be demonstrated
Issue : Suggests it is OK to have components of different criticality in the same system without partitioning.
Suggestion: Reword to "The use of multiple SWALs would also allow the possibility of managing several criticalities of the different software components within the system (with appropriate partitioning) by the same set of software assurance processes."

response *Accepted*

Considering the comment, the text has been amended accordingly.

comment *274* comment by: *German NSA (BAF)*

From the industrial standards only ED-153 use the term "SOFTWARE ASSURANCE LEVELS (SWAL)". If this term is used in the NPA it should be made clear whether it is used in the meaning of ED-153 levels or as general designation.

response *Noted*

The diversity of terms used in the different software standards is acknowledged. The term 'SWAL' has been used without a particular link to ED-153.

comment *292* comment by: *ASD/Thales Air Systems*

GM2 to AM4 (b): regarding the sentence "... and the architecture and/or procedural defences identified", it appears useful to be more detailed in the guidance explaining that mitigation measures are divided into 2 classes, preventive mitigations which decrease the probability of occurence of the hazard and protective mitigations which reduce the severity of the end effect of the hazard. And that the SWAL allocation done by ATS providers should take into account existing mitigations means to allocate the appropriate SWAL to a software equipment of the the ATM system.

response *Not accepted*

Despite that, this information could be considered useful. It is preferred to keep the provision at a higher level of abstraction rather to enter in other domains safety assessment techniques.

comment *342* comment by: *UK CAA*

GM2 to AMC4 ATS.OR.205(a)(2)

Equivalent coverage in EC 2017/373 text: N/A

The ATM IR does not define assurance levels. It allows their use but points out that there can be many different types and that their use does not imply satisfaction of requirement …
See GM2 ATS.OR.205(a)(2)

Comments:

	Not specific to software. Removal of the SW related terms would have no effect on the meaning of the text and would broaden it to include PPE. Assurance levels can be used in other fields as well e.g. DALs, HWALs The relationship between confidence and SWALs is not defined and so introducing SWALs should not be done until there is some solid underpinning evidence for such a relationship
response	*Noted* An analysis of the requirements has shown that there is no overlap. The commented GM is introduced to illustrate the intent of AMC4 ATS.OR.205(a)(2).

comment	*343* comment by: *UK CAA* **GM2 to AMC4 ATS.OR.205(a)(2) point (a)** **Equivalent coverage in EC 2017/373 text: N/A**
response	*Noted* An analysis of the requirements has shown that there is no overlap. The commented GM is introduced to illustrate the intent of AMC4 ATS.OR.205(a)(2).

comment	*344* comment by: *UK CAA* **GM2 to AMC4 ATS.OR.205(a)(2) point (b)** **Equivalent coverage in EC 2017/373 text: N/A**
response	*Noted* An analysis of the requirements has shown that there is no overlap. The commented GM is introduced to illustrate the intent of AMC4 ATS.OR.205(a)(2).

comment	*345* comment by: *UK CAA* **GM2 to AMC4 ATS.OR.205(a)(2) point (c)** **Equivalent coverage in EC 2017/373 text: N/A**
response	*Noted* An analysis of the requirements has shown that there is no overlap. The commented GM is introduced to illustrate the intent of AMC4 ATS.OR.205(a)(2).

comment	*346* comment by: *UK CAA* **GM2 to AMC4 ATS.OR.205(a)(2) point (d)** **Equivalent coverage in EC 2017/373 text: None**

Comments: Out of scope/context. This section deals with ATSPs only.

response *Noted*

An analysis of the requirements has shown that the commented provision is relevant. The commented GM is introduced to illustrate the intent of AMC4 ATS.OR.205(a)(2).

GM3 to AMC4 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system p. 17-18

comment *25* comment by: *D Winship*

para (c)
"The definition of the software assurance processes may be based on one of these industrial standards without…."

The intent of this statement requires consideration – there is no reason why the service provider can't utilise best practices from a number of the relevant standards. The sentence as currently written could be interpreted as stating they can only select one due to the use of "without combining provisions for different standards". Please clarify intent of this paragraph and consider revision.

response *Partially accepted*

It would not be considered as a good practice to combine objectives from different standards as they were developed separately under different considerations and there could be some internal compensation means (one objective is less demanding in a particular standard because another objective is more demanding). On the other hand, the use of the verb 'may' allows the service provider to use the best practices to complement one of the standards or to define the full set of software assurance processes. No change is derived from this comment.

However, considering the comment, the text has been amend to promote clarity.

comment *174* comment by: *DSNA*

Even if the service provider may be able to validate pre-defined/standard additional software assurance processes, it may not be always able to define them because it requires a high level of expertise on the subject which may not be its core business.

response *Noted*

It should be highlighted that Regulation (EC) No 482/2008 is currently applicable and the ANSPs are required to implement a software assurance system.

comment *175* comment by: *DSNA*

In item (b), the ED-12C/DO-178C should be removed too due to the fact that the ED-109A/DO-278A already covers same assumptions for ATM context.

Note also that DO-278B doesn't exist yet, and should be replaced by DO-278A. Finally, ED109 should be considered as it is a standard currently used in industry right now (not all software development have switched from ed109 to ed109A).

response *Partially accepted*

The comments are duly considered.

It should be acknowledged that still some European ANSPs are making use of ED-12C/DO-178C to facilitate the software assurance process. Considering the nature of the commented GM, the referenced standard remains.

comment *231* comment by: *DSAC - FR NSA*

The same reference as in the array "RTCA DO-178C" and "RTCA DO-278B" should be used.

response *Accepted*

comment *263* comment by: *NATS*

Para (b) "When tools are used during the software development lifecycle". It is difficult to imagine a software development lifecycle that does not include at least one tool (such as a compiler or development environment). In those terms "Tool Qualification" always exists for a software development lifecycle.
Issue: Clarify that tool qualification it not 'optional' as implied by the statement.
Suggestion: Add ED-215 to the list of ED-109A related supplements

response *Accepted*

As regards the tools qualification, EASA agrees that tools are widely used for software development and verification. Nevertheless, it might be possible that the tools do not require qualification because the output is verified independently. It is preferred to keep the proposed text.

comment *269* ❖ comment by: *ASD/Thales Air Systems*

To not create confusion, it is very important to not mix standards for airborne systems like DO-178C and standards for ground systems like ED-109A. A unique list may be confusing for a Service Provider that is not aware about the techncal content of those standards and may require the compliance to DO-178C to ground systems manufacturers. This confusion between standards could create a climate of incomprehension that could hinder functional improvement initiatives in ATM systems. Moreover, safety management systems put in place by ATM ground manufacturers are based on ATM standards (e.g. ED-109A, ED-153), and it will represent a blocking industrial issue to comply with standards, such as DO-178C, not adapted to ATM ground systems.

That is the reason why i**t appears necessary to separate these 2 different categories of standards** (airborne standards vs ground standards).

response | *Not accepted*

It should be acknowledged that the scope of each document, i.e. standard, indicates the intended domain of applicability. This is especially relevant taking into account the possibility of identifying ATM/ANS systems with ground and space components.

comment | *283* ❖ comment by: *ASD/Thales Air Systems*

In the item (c), it is written that "The definition of the software assurance processes **may be** based on one of these industrial standards ...". From an industrial point of view, we know very well the technical content of these standards and we also know that requiring a compliance to provisions/requirements coming from different standards is a strong source of confusion. This is the reason why it appears useful to be more strict on this topic by writting for example: "The definition of the software assurance processes **should be** based on one of these industrial standards ...".

response | *Not accepted*

Being guidance material and providing a non-exhaustive list of standards, the current wording is considered more suitable. It is acknowledged that there are other ANSPs that base the software assurance process on other standards (CMMI).

comment | *347* comment by: *UK CAA*

GM3 to AMC4 ATS.OR.205(a)(2) point (a)

Equivalent coverage in EC 2017/373 text: N/A

Comments:
Not specific to software. Removal of the SW related terms would have no effect on the meaning of the text and would broaden it to include PPE.
This section is out of context. The approval of processes is covered in ATM/ANS.OR.B.10 and its associated AMC/GM

response | *Noted*

comment | *348* comment by: *UK CAA*

GM3 to AMC4 ATS.OR.205(a)(2) point (c)

Equivalent coverage in EC 2017/373 text: N/A

Comments:
Not specific to software. Removal of the SW related terms would have no effect on the meaning of the text and would broaden it to include PPE.
This section is out of context. The approval of processes is covered in ATM/ANS.OR.B.10 and its associated AMC/GM

response | *Noted*

GM4 to AMC4 ATS.OR.205(a)(2) Safety assessment and assurance of changes to the functional system p. 18-19

comment *8* comment by: *DFS Deutsche Flugsicherung GmbH*

(a)
The second sentence is not clear: “This requirement applies also to software assurances” – The whole subject is on software assurance, so please be more concrete which requirement is meant ??

Better, we suggest to remove the second sentence. (It also contradicts e.g. the next paragraph where it says that non-ATS-providers may have different software assurance processes.)

response *Partially accepted*

Considering the comment, the text has been amended to promote clarity.

comment *26* comment by: *D Winship*

para (a)
“applies also to software assurances ….as mitigation means against software design failures”
Consideration should be given to rewording this sentence re “software assurances”. Also scope for mitigations may not only be limited to “software **design** failures”.

Suggested revision
“This requirement is also applicable to software assurance evidence which may include information on the mitigation measures established to address software failures or unintended behaviours.”

response *Accepted*

Considering the comment, the text has been amended.

comment *46* comment by: *CANSO*

(a)
The second sentence is not clear: “This requirement applies also to software assurances” – The whole subject is on software assurance, so please be more concrete which requirement is meant ??

Better, we suggest to remove the second sentence. (It also contradicts e.g. the next paragraph where it says that non-ATS-providers may have different software assurance processes.)

response *Partially accepted*

Considering the comment, the text has been amended to promote clarity.

comment

78 comment by: *Swedish Transport Agency, Civil Aviation Department (Transportstyrelsen, Luftfartsavdelningen)*

part a

The responsability is clear, avoids the current practice to rely on industry.

response

Noted

The comment is duly noted.

comment

123 comment by: *ENAV*

(a)
The second sentence is not clear: "This requirement applies also to software assurances" – The whole subject is on software assurance, so please be more concrete which requirement is meant ??

Better, we suggest to remove the second sentence. (It also contradicts e.g. the next paragraph where it says that non-ATS-providers may have different software assurance processes.)

response

Partially accepted

Considering the comment, the text has been amended to promote clarity.

comment

264 comment by: *NATS*

Para (b)
This bullet implies that a non-ATS provider may have an equivalent SWAL scheme (especially if the ATS provider is using SWAL allocation).
Impact: Implication that the non-ATS provider may require a SWAL scheme.
Suggestion: Modify statement to "ATS and non-ATS providers may rely on different sets of software assurance processes and if applicable, different sets of SWALs."

response

Accepted

Considering the comment, the text has been amended accordingly.

comment

265 comment by: *NATS*

Para (d)
This bullet implies that a non-ATS provider may have an equivalent SWAL scheme (especially if the ATS provider is using SWAL allocation).
Issue: Implication that the non-ATS provider may require a SWAL scheme.
Suggestion: Modify statement to "If SWALs are used, the ATS provider should….."

response | *Accepted*

Considering the comment, the text has been amended accordingly.

comment | *293* comment by: *ASD/Thales Air Systems*

GM4 to AMC4 (a): in practice there are many cases where ATS providers rely on non-ATS providers expertise to define an appropriate mitigation strategy to solve bloking issues. For example, based on the safety objectives allocated by the ATS provider, an equipement provider may recommend to a ATS provider to implement specific procedures to manage a specific risk identified during the training phase.
Regarding software assurance, it is important to distinguish the target SWAL allocation done by ATS provider and the implemented SWAL which depends on the design of the software and the architecture of the system where this software is integrated (e.g. software implemented using diversification or using a fallback solution, etc.).

response | *Noted*

It should be pointed out that the comment addresses the necessary interactions between ATS and non-ATS provider in order to ensure that the non-ATS service is consistent with the intended use. This coordination is also necessary for the safety and safety support assessments.

Considering the comment, the commented GM will remain as initially proposed without modifications.

comment | *349* comment by: *UK CAA*

GM4 to AMC4 ATS.OR.205(a)(2)

Equivalent coverage in EC 2017/373 text: General GM Section 2.4 & 3.3

Comments:
Not specific to software. Removal of the SW related terms would have no effect on the meaning of the text and would broaden it to include PPE.
All of this is covered to a greater depth in the general GM- on multi actor changes – Section 2.4 and Service provider centric view – Section 3.3

response | *Noted*

The comment is duly noted.

6. Appendix p. 22-23

comment | *74* comment by: *CANSO*

Page 23
Remark:

	Cross reference table seems to give some wrong references and needs to be corrected as this gives troubles in comparing with EC 482/2002 E;g AMC6 ATM/ANS.OR.C.005(a)(2), point (1)(a) refers to (a)(1) , etc (letters and figures seem inverted in the NPA referenced points) => References shall be updated.
response	*Accepted*

comment	*75* comment by: *CANSO* Remark: There are some differences between NPA and current regulation (e.g consideration about derived requirements, safety requirements vs requirements etc.), so a transition period for projects that have started before the entry into force of the regulation needs to be addressed. *=> EC 482/2002 - Article 7 " Entry into force " can't be to N/A and because it should be considered for projects which have already started software developments or under call for tender process*
response	*Noted* It should be noted that Regulation (EC) No 482/2008 entered into force in 2010 and, hence, after several years of application, it is understood that the concept of software legacy does not require a particular treatment. Consequently, any new software or modifications to existing software should follow the software assurance processes.

comment	*124* comment by: *ENAV* Page 23 Remark: Cross reference table seems to give some wrong references and needs to be corrected as this gives troubles in comparing with EC 482/2002 E;g AMC6 ATM/ANS.OR.C.005(a)(2), point (1)(a) refers to (a)(1) , etc (letters and figures seem inverted in the NPA referenced points) => References shall be updated.
response	*Accepted*

comment	*125* comment by: *ENAV* Remark: There are some differences between NPA and current regulation (e.g consideration about derived requirements, safety requirements vs requirements etc.), so a transition period for projects that have started before the entry into force of the regulation needs to be addressed. *=> EC 482/2002 - Article 7 " Entry into force " can't be to N/A and because it should be considered for projects which have already started software developments or under call for tender process*
response	*Noted*

It should be noted that Regulation (EC) No 482/2008 entered into force in 2010 and, hence, after several years of application, it is understood that the concept of software legacy does not require a particular treatment. Consequently, any new software or modifications to existing software should follow the software assurance processes.

comment *171* comment by: *DSNA*

There are some differences between NPA and current regulation (e.g consideration about derived requirements, safety requirements vs requirements etc.), so a transition period for projects that have started before the entry into force of the regulation needs to be adressed.
=> EC 482/2002 - Article 7 " Entry into force " can't be to N/A and because it should be considered for projects which have already started software developments or under call for tender process

response *Noted*

It should be noted that Regulation (EC) No 482/2008 entered into force in 2010 and, hence, after several years of application, it is understood that the concept of software legacy does not require a particular treatment. Consequently, any new software or modifications to existing software should follow the software assurance processes.

comment *203* comment by: *AESA/DSANA*

Errata in number of NPA references.
Please consider to review the following NPA references in the cross reference table Regulation (EC) No 482/2008 and this NPA:

Article 3.1 is missing. In the reference table it should say **Article 3(1) > N/A**
Article 4 >ATM/ANS.OR.B.010(a)(a) instead of ATM/ANS.OR.B.010(a)(1)
Article 4(1) > AMC5 ATM/ANS.OR.C.005(a)(2), point (a) and AMC3 ATS.OR.205(a)(2), point (a) instead of AMC5 ATM/ANS.OR.C.005(a)(2), point (1) and AMC3 ATS.OR.205(a)(2), point (1)
Art. 3(2)(a) > AMC6 ATM/ANS.OR.C.005(a)(2), point (a)(1) and AMC4 ATS.OR.205(a)(2), point (a) (1) instead of AMC6 ATM/ANS.OR.C.005(a)(2), point (1)(a) and AMC4 ATS.OR.205(a)(2), point (1)(a)
Article 3(2)(b) > AMC6 ATM/ANS.OR.C.005(a)(2), point (a) (2) and AMC4 ATS.OR.205(a)(2), point (a)(2) instead of AMC6 ATM/ANS.OR.C.005(a)(2), point (1)(b) and
AMC4 ATS.OR.205(a)(2), point (1)(b)
Article 3(2)(c) > AMC6 ATM/ANS.OR.C.005(a)(2), point (a)(3) and AMC4 ATS.OR.205(a)(2), point (a)(3) instead of AMC6 ATM/ANS.OR.C.005(a)(2), point (1)(c) and AMC4 ATS.OR.205(a)(2), point (1)(c)
Article 3(2)(d) > AMC5 ATM/ANS.OR.C.005(a)(2), point (a) and AMC3 ATS.OR.205(a)(2), point (a) instead of AMC5 ATM/ANS.OR.C.005(a)(2), point (1) and AMC3 ATS.OR.205(a)(2), point (1)

	Article 3(2)(e) > AMC6 ATM/ANS.OR.C.005(a)(2), point (b) and AMC4 ATS.OR.205(a)(2), point (b) instead of AMC6 ATM/ANS.OR.C.005(a)(2), point (2) and AMC4 ATS.OR.205(a)(2), point (2) **Art. 4(3)(a) Annex II — Part A > AMC6 ATM/ANS.OR.C.005(a)(2), points (a)(1)(i) and (ii) AMC4 ATS.OR.205(a)(2), points (a)(1)(i) and (ii)** instead of AMC6 ATM/ANS.OR.C.005(a)(2), points (1)(a)(i) and (ii) and AMC4 ATS.OR.205(a)(2), points (1)(a)(i) and (ii) **Art. 4(3)(b) Annex II — Part B > AMC6 ATM/ANS.OR.C.005(a)(2), points (a)(4) and (5) and AMC4 ATS.OR.205(a)(2), points (a)(4) and (5)** instead of AMC6 ATM/ANS.OR.C.005(a)(2), points (1)(d) and (e) and AMC4 ATS.OR.205(a)(2), points (1)(d) and (e) **Art. 4(3)(c) Annex II — Part C > AMC6 ATM/ANS.OR.C.005(a)(2), point (d) and AMC4 ATS.OR.205(a)(2), point (d**) instead of AMC6 ATM/ANS.OR.C.005(a)(2), point (4) and AMC4 ATS.OR.205(a)(2), point (4) **Art. 4(3)(d) Annex II — Part D > AMC6 ATM/ANS.OR.C.005(a)(2), points (a)(1)((i) and (ii) and AMC4 ATS.OR.205(a)(2), points (a)(2) (i) and (ii**) instead of AMC6 ATM/ANS.OR.C.005(a)(2), points (1)(b)(i) and (ii) and AMC4 ATS.OR.205(a)(2), points (1)(b)(i) and (ii) **Art. 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 (c)** instead of : 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) and AMC4 ATS.OR.205(a)(2), point (3) **Article 4(5)> AMC5 ATM/ANS.OR.C.005(a)(2), point (b) AMC3 ATS.OR.205(a)(2), point (b)** instead of:AMC5 ATM/ANS.OR.C.005(a)(2), point (2) and AMC3 ATS.OR.205(a)(2), point (2) **Art. 5 > Mainly addressed in NPA 2014-13; In this NPA the software elements are: AMC6 ATM/ANS.OR.C.005(a)(2), point (e) and AMC4 ATS.OR.205(a)(2), point (e)** instead of Mainly addressed in NPA 2014-13; In this NPA the software elements are: AMC6 ATM/ANS.OR.C.005(a)(2), point (5) and AMC4 ATS.OR.205(a)(2), point (5)
response	*Accepted*

3. Attachments

20171207CommentFormExternal.pdf
Attachment #1 to comment #350

20171117UK CAA Table of Detailed Comments for Comment No 1 on NPA 2017-10.pdf
Attachment #2 to comment #350

20171117UK CAA Table of Detailed Comments for Comment No 1 on NPA 2017-10.pdf
Attachment #3 to comment #236
