AMC-20 AMENDMENT 19 — CHANGE INFORMATION

EASA publishes amendments to the General Acceptable Means of Compliance for Airworthiness of Products, Parts and Appliances (AMC-20) as consolidated documents. These documents are used for establishing the certification basis for applications made after the date of entry into force of the applicable amendment.

Consequently, except for a note '[Amdt 20/19]' under the amended paragraph, the consolidated text of the AMC does not allow readers to see the detailed changes compared to the previous amendment. To allow readers to see these detailed changes, this document has been created. The same format as for the publication of notices of proposed amendments (NPAs) is used to show the changes:

— deleted text is ~~struck through~~;

— new or amended text is highlighted in blue;

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

Preamble

ED Decision 2020/010/R

Amendment 19

The following is a list of paragraphs affected by this Amendment:

SUBPART A — GENERAL	Created
AMC 20-1	Amended (NPA 2017-09)
AMC 20-2	Amended (NPA 2017-09)
AMC 20-3	Amended (NPA 2017-09)
AMC 20-8	Amended (NPA 2016-19)
AMC 20-19	Created (NPA 2017-09)
AMC 20-152A	Created (NPA 2018-09)
AMC 20-189	Created (NPA 2018-09)
SUBPART B — LIST OF AMC-20 ITEMS	Created

AMC-20

1. The following SUBPART A is inserted:

SUBPART A — GENERAL

2. AMC 20-1 is amended as follows:

AMC 20-1A Certification of Aircraft Propulsion Systems Equipped with Electronic Control Systems

1 GENERAL

The existing certification specifications (CSs) ~~specific regulations~~ for Engine, Propeller and aircraft certification may require special interpretation for Engines and Propellers equipped with electronic control systems. Because of the nature of this technology and because of the greater interdependence of ~~e~~Engine, ~~p~~Propeller and aircraft systems, it has been found necessary to prepare acceptable means of compliance (AMC) specifically addressing the certification of these electronic control systems.

~~This~~ AMC 20-1( ) addresses the compliance tasks relating to the certification of the installation of propulsion systems equipped with electronic control systems. AMC 20-3( ) is dedicated to the certification of Engine ~~C~~control ~~S~~systems but identifies some ~~e~~Engine-installation-related issues~~,~~ that should be read in conjunction with ~~this~~ AMC 20-1( ).

Like any AMC~~acceptable means of compliance~~, it is issued to outline issues to be considered during demonstration of compliance with the ~~certification specifications~~CSs.

2 RELEVANT SPECIFICATIONS

For aircraft certification, some of the ~~main~~related CSs~~certification specifications~~ are:

— ~~F~~for aeroplanes in CS-25 (and, where applicable, CS-23):

  — ~~P~~paragraphs~~,~~ 33, 581, 631, 899, 901, 903, 905, 933, 937, 939, 961, 994, 995, 1103(d), 1143 (except (d)), 1149, 1153, 1155, 1163, 1181, 1183, 1189, 1301, 1305, 1307(c), 1309, 1337, 1351(b) and (d), 1353(a) and (b), 1355(c), 1357, 1431, 1461, 1521(a), 1527~~;~~.

— ~~F~~for rotorcraft: equivalent specifications in CS-27 and CS-29.

3 SCOPE

This AMC ~~acceptable means of compliance~~ is relevant to the CSs~~certification specifications~~ for aircraft installation of Engines or Propellers with electronic control systems, whether using electrical or electronic (analogue or digital) technology.

It gives guidance on the precautions to be taken for the use of electrical and electronic technology for Engine and Propeller control, protection and monitoring, and, where applicable, for integration of functions specific to the aircraft.

Precautions have to be adapted to the criticality of the functions. These precautions may be affected by the degree of authority of the system, the phase of flight, and the availability of a ~~back-up~~backup system.

This document also discusses the division of compliance tasks between the applicants for Engine, Propeller (when applicable), and aircraft type certificates. This guidance relates to issues to be considered during aircraft certification.

It does not cover APU control systems; APUs, which are not used as "'propulsion systems'", are addressed in the dedicated AMC 20-2( ).

4 PRECAUTIONS

(a) General

The introduction of electrical and electronic technology can entail the following:

— A greater interdependence of the Engine or Propeller and on the aircraft owing to the useexchange of electrical power and/or data between themsupplied from the Aircraft.;

— an increased integration of the control and the related indication functions,;

— an increased risk of significant fFailures that are common to more than one Engine or Propeller of the aircraft which might, for example, occur as a result of:–

— iInsufficient protection from electromagnetic disturbance (e.g. lightning, internal or external radiation effects),;

— iInsufficient integrity of the aircraft electrical power supply,;

— iInsufficient integrity of data supplied from the aircraft,;

— Hhidden design faults or discrepancies contained within the design of the propulsion system control software or complexairborne electronic hardware (AEH),; or

— Oomissions or errors in the system/software/AEH specification.

SpecialAppropriate design and integration precautions should therefore be taken to minimise these risks.

(b) Objective

The introduction of electronic control systems should provide for the aircraft at least the equivalent level of safety, and the related reliability level, as achieved in aircraft equipped with Engine and Propellers using hydromechanical control and protection systems.

When possible, early co-ordination coordination between the Engine, Propeller and aircraft applicants is recommended in association with the AgencyEASA as discussed in under paragraphSection (5) of this AMC.

(c) Precautions relating to electrical power supply and data from the aircraft

When considering the objectives of paragraphSection 4(a) or (b), due consideration should be given to the reliability of electrical power and data supplied to the electronic control systems and peripheral components. The potential adverse effects on Engine and Propeller operation of any loss of electrical power supply from the aircraft or failure of data coming from the aircraft are assessed during the Engine and Propeller certification.

During aircraft certification, the assumptions made as part of the Engine and Propeller certification on reliability of aircraft power and data should be checked for consistency with the actual aircraft design.

Aircraft should be protected from unacceptable effects of faults due to a single cause, simultaneously affecting more than one Engine or Propeller. In particular, the following cases should be considered:

— ~~E~~erroneous data received from the aircraft by the Engine/Propeller control system if the data source is common to more than one Engine/Propeller (e.g. air data sources, autothrottle synchronising)~~,~~; and

— ~~C~~control system operating faults propagating via data links between Engine/Propellers (e.g. maintenance recording, common bus, cross-talk, autofeathering, automatic reserve power system).

Any precautions needed may be taken either through the aircraft system architecture or by logic internal to the electronic control system.

(d) Local events

For Engine and Propeller certification, effects of local events should be assessed.

Whatever the local event, the behaviour of the electronic control system should not cause a hazard to the aircraft. This will require consideration of effects such as the control of the thrust reverser deployment, the ~~over-speed~~ overspeed of the Engine, transient~~s~~ effects or inadvertent Propeller pitch change under any flight condition.

When the demonstration that there is no hazard to the aircraft is based on the assumption that there exists another function to afford the necessary protection, it should be shown that this function is not rendered inoperative by the same local event (including destruction of wires, ducts, power supplies).

Such assessment should be reviewed during aircraft certification.

(e) Software and ~~Programmable Logic Devices~~airborne electronic hardware (AEH)

The acceptability of the criticality levels and methods used for the development and verification of software and ~~Programmable Logic Devices~~AEH which are part of the Engine and Propeller type designs should have been agreed between the aircraft, Engine and Propeller designers prior to the certification activity.

Note: In this AMC, the ‘criticality level’ is used to reflect either the software level of a software item or the AEH design assurance level (or DAL) of an AEH item.

(f) Environmental effects

The validated protection levels for the Engine and Propeller electronic control systems, as well as their emissions of radio frequency energy, are established during the Engine and Propeller certification and are contained in the instructions for installation. For the aircraft certification, it should be substantiated that these levels are appropriate~~adequate~~.

5 ~~INTER-RELATION~~INTERRELATION BETWEEN ENGINE, PROPELLER AND AIRCRAFT CERTIFICATION

(a) Objective

To satisfy the aircraft certification specifications, such as CS 25.901, CS 25.903 and CS 25.1309, an analysis of the consequences of failures of the system on the aircraft has to

be made. It should be ensured that the software ~~levels~~/AEH criticality levels and the safety and reliability objectives for the electronic control system are consistent with these requirements.

(b) Interface Definition

The interface has to be identified for the ~~hardware~~AEH and software aspects between the Engine, Propeller and the aircraft systems in the appropriate documents.

The Engine/Propeller/aircraft documents should cover in particular: ~~:~~

— ~~T~~the software ~~quality level~~/AEH criticality level (per function if necessary)~~;~~,

— ~~T~~the reliability objectives for a loss of Engine/Propeller control or a significant change in thrust~~,~~ (including an IFSD due to a control system malfunction), or for the transmission of faulty parameters~~;~~,

— ~~T~~the degree of protection against lightning or other electromagnetic effects (e.g. the level of induced voltages that can be supported at the interfaces)~~;~~,

— Engine, Propeller and aircraft interface data and characteristics~~;~~, and

— the ~~A~~aircraft power supply and its characteristics (if relevant).

(c) Distribution of Compliance Demonstration

The certification tasks of the aircraft propulsion system equipped with electronic control systems may be shared between the Engine, Propeller and aircraft certification. The distribution between the different certification activities should be identified and agreed with ~~the Agency~~EASA and/or the appropriate Engine and aircraft ~~A~~authorities~~:~~ (an example is given in ~~paragraph~~Section ~~(~~6~~)~~ 'TABLE').

Appropriate evidence provided for Engine and Propeller certification should be used for aircraft certification. For example, the quality of any aircraft function software/AEH and aircraft/Engine/Propeller interface logic already demonstrated for Engine or Propeller certification should need no additional substantiation for aircraft certification.

Aircraft certification should deal with the specific precautions taken in respect of the physical and functional interfaces with the Engine/Propeller.

6. TABLE

The following is ~~A~~an example of the distribution of the tasks between the Engine certification and the aircraft certification. (When necessary, a similar approach should be taken for Propeller applications.)~~.~~

TASK	SUBSTANTIATION UNDER CS-E	SUBSTANTIATION UNDER CS-25	
		with ~~e~~Engine data	with aircraft data
ENGINE CONTROL AND PROTECTION	— Safety objective — Software ~~level~~/AEH criticality level	— Consideration of common mode effects (including software and AEH) — Reliability — Software ~~level~~/AEH criticality level	
MONITORING	— Independence of control and monitoring parameters	— Monitoring parameter reliability	— Indication system reliability — Independence ~~e~~Engine/~~e~~Engine
AIRCRAFT DATA	— Protection of ~~e~~Engine from aircraft data failures — Software ~~level~~/AEH criticality level		— Aircraft data reliability — Independence ~~e~~Engine/~~e~~Engine
THRUST REVERSER CONTROL/ MONITORING	— Software ~~level~~/AEH criticality level	— System reliability — Architecture — Consideration of common mode effects (including software and AEH)	— Safety objectives
CONTROL SYSTEM ELECTRICAL SUPPLY	— Reliability or quality Requirement of aircraft supply, if used		— Reliability of quality of aircraft supply, if used — Independence ~~e~~Engine/~~e~~Engine
ENVIRONMENTAL CONDITIONS	— Equipment protection	— Declared capability	— Aircraft design
LIGHTNING AND OTHER ELECTROMAGNETIC EFFECTS	— Equipment protection — Electromagnetic emissions	— Declared capability — Declared emissions	— Aircraft wiring protection and electromagnetic compatibility
FIRE PROTECTION	— Equipment protection	— Declared capability	— Aircraft design

3. AMC 20-2A is amended as follows:

AMC 20-2~~A~~B Certification of Essential Auxiliary Power Units (APUs) Equipped with Electronic Controls

1 GENERAL

The existing certification specifications (CSs) ~~regulations~~ for APU and aircraft certification may require special interpretation for essential APUs equipped with electronic control systems. Because of the nature of this technology, it has been found necessary to prepare acceptable means of compliance (AMC) specifically addressing the certification of these electronic control systems.

Like any AMC~~acceptable means of compliance~~, the content of this document is not mandatory. It is issued for guidance purposes, and to outline a method of compliance with the CSs~~airworthiness code~~. In lieu of following this method, an alternative method may be followed, provided that this is agreed by ~~the Agency~~EASA as an acceptable method of compliance with the CSs~~airworthiness code~~.

This document discusses the compliance tasks relating to both the APU and the aircraft certification.

2 RELEVANT~~REFERENCE~~ SPECIFICATIONS

2.1 APU ~~C~~certification

CS-APU

— Book 1, paragraph 2(c);

— Book 1, Section A, paragraphs 10(b), 20, 80, 90, 210, 220, 280 and 530;

— Book 2, Section A, AMC CS-APU 20.

2.2 Aircraft ~~C~~certification

Aeroplanes: CS-25

— ~~P~~paragraphs 581, 899, 901, 903, 939, 1141, 1163, 1181, 1183, 1189, 1301, 1305, 1307(c), 1309, 1337, 1351(b) and (d), 1353(a) and (b), 1355(c), 1357, 1431, 1461, 1521, 1524, 1527

3 SCOPE This AMC~~acceptable means of compliance~~ provides guidance ~~for~~ on electronic (analogue and digital) essential APU control systems, and on the interpretation and means of compliance with the relevant APU and aircraft certification requirements.

It gives guidance on the precautions to be taken for the use of electronic technology for APU control, protection and monitoring and, where applicable, for integration of functions specific to the aircraft.

Precautions have to be adapted to the criticality of the functions. These precautions may be affected by: ~~–~~

— ~~D~~degree of authority of the system;~~,~~

— ~~P~~phase of flight;~~,~~

— ~~A~~availability of ~~back-up~~backup system.

This document also discusses the division of compliance tasks between the APU and the aircraft certification.

4 PRECAUTIONS

4.1 General

The introduction of electronic technology can entail the following:

(a) ~~A~~ greater interdependence of the APU and ~~on~~ the aircraft owing to the ~~use~~exchange of electrical power and/or data between them ~~supplied from the aircraft,~~;

(b) a ~~R~~risk of significant failures which might, for example, occur as a result of~~;~~ ~~–~~

(i) ~~I~~insufficient protection from electromagnetic disturbance (e.g. lightning, internal or external radiation effects)~~;~~;

(ii) ~~I~~insufficient integrity of the aircraft electrical power supply~~;~~;

(iii) ~~I~~insufficient integrity of data supplied from the aircraft~~;~~;

(iv) ~~H~~hidden design faults or discrepancies contained within the design of the APU control software/airborne electronic hardware (AEH)~~;~~ or

(v) ~~O~~omissions or errors in the system specification.

~~Special~~Appropriate design and integration precautions must therefore be taken to minimise these risks.

4.2 Objective

The introduction of electronic control systems should provide for the aircraft at least the equivalent level of safety, and the related reliability level, as achieved by an essential APU equipped with hydromechanical control and protection systems.

This objective, when defined during the aircraft/APU certification for a specific application, will be agreed with EASA~~the Agency~~.

4.3 Precautions related~~ing~~ to APU control, protection and monitoring

The software and AEH associated with the APU control, protection and monitoring functions must have a ~~software~~criticality level and architecture appropriate to the~~ir~~ criticality of the functions performed ~~(see paragraph 4.2)~~.

For digital systems, any residual errors not activated during the software/AEH development and certification process could cause an unacceptable failure. The latest edition of AMC 20-115/AMC 20-152 constitutes an acceptable means of compliance for software/AEH development, verification and software/AEH aspects of certification. The APU software/AEH criticality level should be determined by the APU and aircraft/system safety assessment process; ED-79A/ARP4754A and ARP4761 provide guidelines on how to conduct an aircraft/APU/system safety assessment process.~~at least level B according to the industry documents referred in the latest edition of AMC 20-115. In some specific cases, level A may be more appropriate.~~

It should be noted that the software/AEH development assurance methods and disciplines described in the latest edition of AMC 20-115/AMC 20-152 may not, in themselves, be sufficient to ensure that the overall system safety and reliability targets have been achieved. This is particularly true for certain critical systems, such as full~~y~~ authority digital engine control (FADEC) systems. In such cases, it is accepted that other measures, usually within the system, in addition to a high level of software/AEH development assurance, ~~discipline~~ may be necessary to achieve these safety objectives and demonstrate that they have been met.

It is outside the scope of the latest edition of AMC 20-115/AMC 20-152 to suggest or specify these measures, but in accepting that they may be necessary, it is also the intention to encourage the development of software/AEH techniques which could support meeting the overall system safety objectives."

Note: In this AMC, the 'criticality level' is used to reflect either the software level of a software item and the AEH design assurance level (or DAL) of an AEH item.

4.4 Precautions related~~ing~~ to APU independence from the aircraft

4.4.1 Precautions related~~ing~~ to electrical power supply and data from the aircraft

When considering the objectives of ~~paragraph~~Section 4.2, due consideration must be given to the reliability of electrical power and data supplied to the electronic controls and peripheral components. Therefore, the potential adverse effects on APU operation of any loss of electrical power supply from the aircraft or failure of data coming from the aircraft must be assessed during the APU certification.

(a) Electrical power

The use of either the aircraft electrical power network or electrical power sources specific to the APU, or the combination of both, may meet the objectives.

If the aircraft electrical system supplies power to the APU control system at any time, the power supply quality, including transients or failures, must not lead to a situation identified during the APU certification which is considered during the aircraft certification to be a hazard to the aircraft.

(b) Data

The following cases should be considered:

(i) ~~E~~erroneous data received from the aircraft by the APU control system~~;~~ and

(ii) ~~C~~control system operating faults propagating via data links.

In certain cases, defects of aircraft input data may be overcome by other data references specific to the APU in order to meet the objectives.

4.4.2 Local ~~E~~events

(a) In designing an electronic control system to meet the objectives of ~~paragraph~~Section 4.2, special consideration needs to be given to local events.

Examples of local events include fluid leaks, mechanical disruptions, electrical problems, fires or overheat conditions. An overheat condition results when the temperature of the electronic control unit is greater than the maximum safe design operating temperature declared during the APU certification. This situation can increase the failure rate of the electronic control system.

(b) Whatever the local event, the behaviour of the electronic control system must not cause a hazard to the aircraft. This will require consideration of effects such as the overspeed of the APU.

When the demonstration that there is no hazard to the aircraft is based on the assumption that there exists another function to afford the necessary protection, it must be shown that this function is not rendered inoperative by the same local event (including destruction of wires, ducts, power supplies).

(c) Specific design features or analysis methods may be used to show compliance with respect to hazardous effects. Where this is not possible, for example due to the variability

or the complexity of the failure sequence, then testing may be required. These tests must be agreed with EASA~~the Agency~~.

4.4.3 Lightning and other electromagnetic effects

Electronic control systems are sensitive to lightning and other electromagnetic interference. The system design must incorporate sufficient protection in order to ensure the functional integrity of the control system when subjected to designated levels of electric or electromagnetic inductions, including external radiation effects.

The validated protection levels for the APU electronic control system must be detailed during the APU certification in an approved document. For aircraft certification, it must be substantiated that these levels are adequate.

4.5 Other functions integrated into the electronic control system

If functions other than those directly associated with the control of the APU are integrated into the electronic control system, the APU certification should take into account the applicable aircraft requirements.

5 ~~INTER-RELATION~~INTERRELATION BETWEEN APU CERTIFICATION AND AIRCRAFT CERTIFICATION

5.1 Objective

To satisfy the certification~~CS aircraft~~ requirements, such as CS 25.901~~A901~~, CS 25.903~~A903~~ and CS 25.1309, an analysis of the consequences of failures of the system on the aircraft has to be made. It should be ensured that the software/AEH criticality levels and the safety and reliability objectives for the electronic control system are consistent with these requirements.

5.2 Interface definition

The interface has to be identified for the ~~hardware~~AEH and software aspects between the APU and the aircraft systems in the appropriate documents.

The APU documents should cover in particular:~~–~~

(a) ~~T~~the software/AEH criticality ~~quality~~ level (per function if necessary);~~,~~

(b) ~~T~~the reliability objectives for:~~–~~

an APU ~~shut-down~~shutdown in flight;~~,~~

~~A~~a ~~L~~loss of APU control or a significant change in performance;~~,~~ and

the transmission of faulty parameters;~~,~~

(c) ~~T~~the degree of protection against lightning or other electromagnetic effects (e.g. the level of induced voltages that can be supported at the interfaces);~~,~~

(d) the APU and aircraft interface data and its characteristics;~~,~~ and

(e) the ~~A~~aircraft power supply and its characteristics (if relevant).

5.3 Distribution of compliance demonstrations

The certification of the APU equipped with electronic controls and of the aircraft may be shared between the APU certification and the aircraft certification. The distribution between the APU certification and the aircraft certification must be identified and agreed with EASA~~the Agency~~ and/or the appropriate APU and aircraft ~~A~~authorities (an example is given in the appendix).

Appropriate evidence provided for the APU certification should be used for the aircraft certification. For example, the quality of any aircraft function software/AEH and aircraft/APU interface logic already demonstrated for the APU certification should need no additional substantiation for the aircraft certification.

Aircraft certification must deal with the specific precautions taken in respect of the physical and functional interfaces with the APU.

Appendix to AMC 20-2B

The following is ~~A~~an example of ~~tasks~~the distribution of the tasks between the APU certification and the aircraft certification.

FUNCTIONS OR INSTALLATION CONDITIONS	SUBSTANTIATION UNDER CS-APU	SUBSTANTIATION UNDER CS-25	
APU CONTROL AND PROTECTION	— Safety objective — Software/AEH criticality level	— Reliability — Software/AEH criticality level	
MONITORING	— Independence of control and monitoring parameters	— Monitoring parameter reliability	— Indication system reliability
AIRCRAFT DATA	— Protection of APU from aircraft data failures — Software/AEH criticality level		— Aircraft data reliability
CONTROL SYSTEM ELECTRICAL SUPPLY			— Reliability and quality of aircraft supply if used
ENVIRONMENTAL CONDITIONS, LIGHTNING AND OTHER ~~ELECTRO-MAGNETIC~~ ELECTROMAGNETIC EFFECTS	— Equipment protection	— Declared capability	— Aircraft design — Aircraft wiring protection

4. AMC 20-3A is amended as follows:

AMC 20-3~~A~~B Certification of Engines Equipped with Electronic Engine Control Systems

(1) PURPOSE

The existing certification specifications of CS-E for Engine certification may require specific interpretation for Engines equipped with Electronic Engine Control Systems (EECS), with special regard to interface with the certification of the aircraft and/or Propeller when applicable. Because of the nature of this technology, it has been considered useful to prepare acceptable means of compliance (AMC) specifically addressing the certification of these control systems.

Like any AMC~~acceptable means of compliance~~, it is issued to outline issues to be considered during the demonstration of compliance with CS-E~~the Engine certification specifications~~.

(2) SCOPE

This AMC~~acceptable means of compliance~~ is relevant to Engine certification specifications for EECS, whether they use~~using~~ electrical or electronic (analogue or digital) technology. This is in addition to other AMC~~acceptable means of compliance~~ such as AMC E 50 or AMC E 80.

It gives guidance on the precautions to be taken for the use of electrical and electronic technology for Engine control, protection, limiting and monitoring functions, and, where applicable, for the integration of aircraft or Propeller functions. In the~~se~~ latter case~~s~~, this document is applicable to such functions integrated into the EECS, but only to the extent that these functions affect compliance with CS-E specifications.

The text deals mainly with the thrust and power functions of an EECS, since this is the prime function of the Engine. However, there are many other functions, such as bleed valve control, that may be integrated into the system for operability reasons. The principles outlined in this AMC apply to the whole EECS~~system~~.

This document also discusses the division of compliance tasks for certification between the applicants for Engine, Propeller (when applicable), and aircraft type certificates. This guidance relates to issues to be considered during ~~e~~Engine certification. AMC 20-1( )addresses issues associated with the ~~e~~Engine installation in the aircraft.

The introduction of electrical and electronic technology can entail the following:

— ~~a~~ greater dependence of the Engine on the aircraft owing to the increased use of electrical power or data supplied from the aircraft;~~,~~

— ~~an~~ increased integration of control and related indication functions;~~,~~

— ~~an~~ increased risk of significant Failures that are common to more than one Engine of the aircraft which might, for example, occur as a result of:

  — ~~i~~nsufficient protection from electromagnetic disturbance (e.g. lightning, internal or external radiation effects) (see CS-E 50(a)(1), CS E-80 and CS-E 170);~~,~~

  — ~~i~~nsufficient integrity of the aircraft electrical power supply (see CS-E 50 (h));~~,~~

— ~~I~~insufficient integrity of data supplied from the aircraft (see CS-E 50(g)); ~~,~~

— ~~H~~hidden design Faults or discrepancies contained within the design of the propulsion system control software or ~~complex~~airborne electronic hardware (AEH) (see CS-E 50(f)); ~~,~~ or

— ~~O~~omissions or errors in the system/software/AEH specification (see CS-E 50(f)).

~~Special~~Appropriate design and integration precautions should therefore be taken to minimise any adverse effects from the above.

(3) RELEVANT SPECIFICATIONS AND REFERENCE DOCUMENTS

Although compliance with many CS-E specifications might be affected by the Engine Control System, the main paragraphs relevant to the certification of the Engine Control System itself are the following:

CS-E Specification	Turbine Engines	Piston Engines
CS-E 20 (Engine configuration and interfaces)	✓	✓
CS-E 25 (Instructions for Continued Airworthiness)~~,~~	✓	✓
CS-E 30 (Assumptions)~~,~~	✓	✓
CS-E 50 (Engine Control System)	✓	✓
CS-E 60 (Provision for instruments)	✓	✓
CS-E 80 (Equipment)	✓	✓
CS-E 110 (Drawing and marking of parts ~~-~~— Assembly of parts)	✓	✓
CS-E 130 (Fire prevention)	✓	✓
CS-E 140 (Tests-Engine configuration)	✓	✓
CS-E 170 (Engine systems and component verification)	✓	✓
CS-E 210 (Failure analysis)		✓
CS-E 250 (Fuel System)		✓
CS-E 390 (Acceleration tests)		✓
CS-E 500 (Functioning)	✓	
CS-E-510 (Safety analysis)	✓	
CS-E 560 (Fuel system)	✓	
CS-E 745 (Engine Acceleration)	✓	
CS-E 1030 (Time-limited dispatch)	✓	✓

The following documents are referenced in ~~this~~ AMC 20-3B:

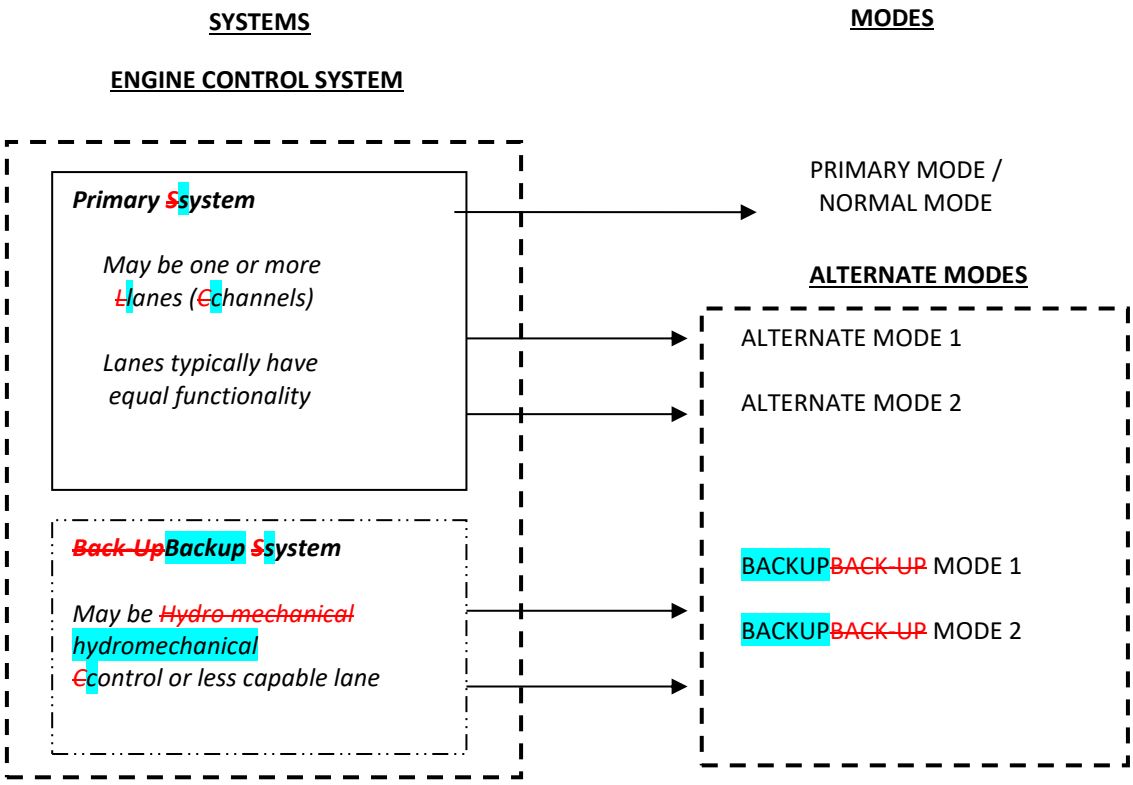
[…]

(4) DEFINITIONS

The words defined in CS-Definitions and in CS-E 15 are identified by capital letters.

The following figure and associated definitions are provided to facilitate a clear understanding of the terms used in this AMC.

DEFINITIONS VISUALISED



(5) GENERAL

It is recognised that the determination of compliance of the Engine Control System with the applicable aircraft certification specifications will only be made during the aircraft certification.

In the case where the installation is unknown at the time of Engine certification, the applicant for Engine certification should make reasonable installation and operational assumptions for the target installation. Any installation limitations or operational issues will be noted in the instructions for installation or operation, and/or the Type Certificate Data Sheet (TCDS) (see CS-E 30 Assumptions).

When possible, early ~~co-ordination~~coordination between the Engine and the aircraft applicants is recommended in association with the relevant authorities as discussed under ~~paragraph~~Section ~~(~~15~~)~~ of this AMC.

(6) SYSTEM DESIGN AND VALIDATION

(a) Control Modes ~~-~~— General

Under CS-E 50(a), the applicant should perform all necessary testing and analysis to ensure that all Control Modes, including those which occur as a result of control Fault Accommodation strategies, are implemented as required.

The need to provide protective functions, such as ~~over-speed~~overspeed protection, for all Control Modes, including any Alternate Modes, should be reviewed under the specifications of CS-E 50~~-~~(c), (d) and (e), and CS-E 210 or CS-E 510.

Any limitations on operations in Alternate Modes should be clearly stated in the Engine instructions for installation and operation.

Descriptions of the functioning of the Engine Control System operating in its Primary and any Alternate Modes should be provided in the Engine instructions for installation and operation.

Analyses and/or testing are necessary to substantiate that operating in the Alternate Modes has no unacceptable effect on Engine durability or endurance. Demonstration of the durability and reliability of the control system in all modes is primarily addressed by the component testing of CS-E 170. Performing some portion of the Engine certification testing in the Alternate Mode(s) and during transition between modes can be used as part of the system validation required under CS-E 50-(a).

(i) Engine Test Considerations

If the Engine certification tests defined in CS-E are performed using only the Engine Control System's Primary Mode in the Full-up Configuration and if approval for dispatch in the Alternate Mode is requested by the applicant under CS-E 1030, it should be demonstrated, by analysis and/or test, that the Engine can meet the defined test-success criteria when operating in any Alternate ~~m~~Mode that is proposed as a dispatchable configuration as required by CS-E- 1030.

Some capabilities, such as operability, blade-off, rain, hail, bird ingestion, etc., may be lost in some control modes that are not dispatchable. These modes do not require engine test demonstration as long as the installation and operating instructions reflect this loss of capability.

(ii) Availability

Availability of any Back-up Mode should be established by routine testing or monitoring to ensure that the Back-up Mode will be available when needed. The frequency of establishing its availability should be documented in the ~~i~~Instructions for ~~c~~Continued ~~a~~Airworthiness (ICA).

(b) Crew Training Modes

This AMC~~acceptable means of compliance~~ is not specifically intended to apply to any crew training modes. These modes are usually installation-, and possibly operator-, specific and need to be negotiated on a case-by-case basis. As an example, one common application of crew training modes is for simulation of the 'failed-fixed' mode on a twin-engine rotorcraft. Training modes should be described in the Engine instructions for installation and operation as appropriate. Also, precautions should be taken in the design of the Engine Control System and its crew interfaces to prevent inadvertent entry into any training modes. Crew training modes, including lock-out systems, should be assessed as part of the System Safety Analysis (SSA) of CS-E 50-(d).

(c) Non-Dispatchable Configurations and Modes

For control configurations which are not dispatchable, but for which the applicant seeks to take credit in the system Loss of Thrust (or Power) Control (LOTC/LOPC) analysis, it may be acceptable to have specific operating limitations. In addition, compliance with CS-E 50-(a) does not imply strict compliance with the operability specifications of CS-E 390, CS-E 500 and CS-E 745 in these non-dispatchable configurations, if it can be demonstrated that, in the intended installation, no likely pilot control system inputs will result in Engine surge, stall, flame-out or unmanageable delay in power recovery. For example, in a twin-engine rotorcraft, a rudimentary Back-up System may be adequate since frequent and rapid changes in power setting with the Back-up System may not be necessary.

In addition to these operability considerations, other factors which should be considered in assessing the acceptability of such reduced-capability Back-up Modes include:

— ~~I~~the installed operating characteristics of the Back-up Mode and the differences from the Primary Mode;~~.~~

— ~~I~~the likely impact of the Back-up Mode operations on pilot workload, if the aircraft installation is known;~~.~~

— ~~I~~the frequency of transfer from the Primary Mode to the Back-up Mode (i.e. the reliability of the Primary Mode);~~.~~ ~~F~~frequencies of transfer of less than 1 per 20 000 engine flight hours have been considered acceptable.

(d) Control Transitions

The intent of CS-E 50(b) is to ensure that any control transitions, which occur as a result of Fault Accommodation, occur in an acceptable manner.

In general, transition to Alternate Modes should be accomplished automatically by the Engine Control System. However, systems for which~~wherein~~ pilot action is required to engage the Back-up Mode may also be acceptable. For instance, a Fault in the Primary System may result in a ~~"~~'failed-fixed'~~"~~ fuel flow and some action is required by the pilot to engage the Back-up System in order to modulate Engine power. Care should be taken to ensure that any reliance on manual transition is not expected to pose an unacceptable operating characteristic, unacceptable crew workload or require exceptional skill.

The transient change in power or thrust associated with transfer to Alternate Modes should be reviewed for compliance with CS-E 50(b). If available, input from the installer should be considered. Although this is not to be considered a complete list, some of the items that should be considered when reviewing the acceptability of Control Mode transitions are:

— The frequency of occurrence of transfers to any Alternate Mode and the capability of the Alternate Mode. Computed frequency-of-transfer rates should be supported with data from endurance or reliability testing, in-service experience on similar equipment, or other appropriate data.

— The magnitude of the power, thrust, rotor or Propeller speed transients.

— Successful demonstration, by simulation or other means, of the ability of the Engine Control System to control the Engine safely during the transition. In some cases, particularly those involving rotorcraft, it may not be possible to make a determination that the mode transition provides a safe system based solely on analytical or simulation data. Therefore, a flight test programme to support this data will normally be expected.

— An analysis should be provided to identify those Faults that cause Control Mode transitions either automatically or through pilot action.

— For turboprop or turboshaft engines, the transition should not result in excessive overspeed~~over-speed~~ or underspeed~~under-speed~~ of the rotor or Propeller which could cause emergency shutdown, loss of electrical generator power or the setting-off of warning devices.

The thrust or power ~~or thrust~~ change associated with the transition should be declared in the instructions for installing the Engine.

(i) Time Delays

Any observable time delays associated with Control Mode, channel or system transitions or in re-establishing the pilot's ability to modulate Engine thrust or

power should be identified in the Engine instructions for installation and operation (see CS-E 50(b)). These delays should be assessed during aircraft certification.

(ii) Annunciation to the Flight Crew

If annunciation is necessary to comply with CS-E 50(b)(3), the type of annunciation to the flight crew should be commensurate with the nature of the transition. For instance, reversion to an Alternate Mode of control where the transition is automatic and the only observable changes in operation of the Engine are different thrust control schedules, would require a very different form of annunciation to that required if timely action by the pilot is required in order to maintain control of the aircraft.

The intent and purpose of the cockpit annunciation should be clearly stated in the Engine instructions for installation and operation, as appropriate.

(e) Environmental conditions

Environmental conditions include electromagnetic interference (EMI), high-intensity radiated fields (HIRF) and lightning. The environmental conditions are addressed under CS-E- 80 and CS-E 170. The following provides additional guidance for EMI, HIRF and lightning.

(i) Declared levels

When the installation is known during the Engine type-certification programme, the Engine Control System should be tested at levels that have been determined and agreed by the Engine and aircraft applicants. It is assumed that, by this agreement, the installation can meet the aircraft certification specifications. Successful completion of the testing to the agreed levels would be accepted for Engine type certification. This, however, may make the possibility of installing the Engine dependent on a specific aircraft.

If the aircraft installation is not known or defined at the time of the Engine certification, in order to determine the levels to be declared for the Engine certification, the Engine applicant may use the external threat level defined at the aircraft level and use assumptions on installation attenuation effects.

If none of the options defined above are available, it is recommended that the procedures and minimum default levels for HIRF testing should be ~~are~~ agreed with EASA~~the Agency~~.

(ii) Test procedures

(A) General

The installed Engine Control System, including representative Engine–~~–~~aircraft interface cables, should be the basis for certification testing.

~~Electro-Magnetic Interference (~~EMI~~)~~ test procedures and test levels conducted in accordance with MIL-STD-461 or EUROCAE ED 14/DO-160 have been considered acceptable.

The applicant should use the HIRF test guidelines provided in EUROCAE ED 14/RTCA DO-160 or equivalent. However, it should be recognised that the tests

defined in EUROCAE ED 14/RTCA DO-160 are applicable at a component test level, requiring the applicant to adapt these test procedures to a system level HIRF test to demonstrate compliance with CS-E 80 and CS-E 170.

For lightning tests, the guidelines of SAE ARP5412, 5413, 5414~~,~~ and 5416, and EUROCAE ED 14/RTCA DO-160 would be applicable.

Pin Injection Tests (PIT) are normally conducted as component tests on the EECS unit and other system components as required. PIT levels are selected as appropriate from the tables of EUROCAE ED 14/DO-160.

Environmental tests, such as MIL-STD-810, may be accepted in lieu of EUROCAE ED-14/DO-160 tests where these tests are equal to or more rigorous than those defined in EUROCAE ED 14/DO-160.

(B) Open-loop and Closed-loop Testing

HIRF and lightning tests should be conducted as system tests on closed-loop or open-loop laboratory set-ups.

The closed-loop set-up is usually provided with hydraulic pressure to move actuators to close the inner actuating loops. A simplified Engine simulation may be used to close the outer Engine loop.

Testing should be conducted with the Engine Control System controlling at the most sensitive operating point, as selected and detailed in the test plans by the applicant. The system should be exposed to the HIRF and lightning environmental threats while operating at the selected condition. There may be a different operating point for HIRF and lightning environmental threats.

For tests in open- and closed-loop set-ups, the following factors should also be considered:

— If a special EECS test software is used, that software should be developed at the criticality level determined by the Engine safety assessment process ~~and implemented by guidelines defined for software levels of at least software level C as defined in the industry documents referred in the latest edition of AMC 20-115~~.

— The Engine Control System should be tested at the criticality levels that have been determined and agreed by the Engine and aircraft applicants. It is assumed that by this agreement, the installation meets the aircraft certification specifications. In some cases, the application code is modified to include the required test code features.

— The system test set-up should be capable of monitoring both the output ~~drive~~ signals and the input signals.

— Anomalies observed during open-loop testing on inputs or outputs should be duplicated on the Engine simulation to determine whether the resulting power or thrust perturbations comply with the ~~pass/fail~~pass–fail criteria.

(iii) ~~Pass/Fail~~Pass–Fail Criteria

The ~~pass/fail~~pass–fail criteria of CS-E 170 for HIRF and lightning should be interpreted as "~~'~~no adverse effect~~'~~" on the functionality of the system.

The following are considered adverse effects:

— ~~A~~a greater than 3 % change of Take-off Power or Thrust for a period of more than 2~~two~~ seconds;~~.~~

— ~~T~~transfers to ~~a~~Alternate ~~c~~Channels, Back~~-~~up Systems, or Alternate Modes;~~.~~

— ~~C~~component damage;~~.~~

— ~~F~~false annunciation to the flight crew, which could cause unnecessary or inappropriate flight crew action;~~.~~

— ~~E~~erroneous operation of protection systems, such as overspeed~~over-speed~~ or thrust reverser circuits.

~~Hardware~~AEH or ~~S~~software design changes implemented after the initial environmental testing should be evaluated for their effects with respect to the EMI, HIRF and lightning environment.

(iv) Maintenance Actions

CS-E 25 requires that the applicant prepare Instructions for Continued Airworthiness (ICA). These include~~This includes~~ a maintenance plan. Therefore, for any protection system that is part of the type design of the Engine Control System and is required by the system to meet the qualified levels of EMI, HIRF and lightning, a maintenance plan should be provided to ensure the continued airworthiness for the parts of the installed system which are supplied by the Engine type~~-~~certificate holder.

~~.~~The maintenance actions to be considered include periodic inspections or tests for required structural shielding, wire shields, connectors, and equipment protection components. Inspections or tests when the part is exposed may also be considered. The applicant should provide the engineering validation and substantiation of these maintenance actions.

(v) Time~~-~~Limited Dispatch (TLD) Environmental Tests

Although TLD is only an optional requirement for certification (see CS-E 1000 and CS-E 1030), EMI, HIRF and lightning tests for TLD are usually conducted together with tests conducted for certification. Acceptable means of compliance are provided in AMC E 1030.

[…]

(10) SOFTWARE AND AIRBORNE ELECTRONIC HARDWARE (AEH) DESIGN AND IMPLEMENTATION

(a) Objective

For Engine Control Systems that use software/AEH, the objective of CS-E 50(f) is to prevent as far as possible software/AEH errors that would result in an unacceptable effect on power or thrust, or any unsafe condition.

~~It is understood that it may be impossible to establish with certainty that the software has been designed without errors. However, if the applicant uses the software level appropriate for the criticality of the performed functions and uses approved software development and verification processes, the Agency would consider the software to be compliant with the requirement to minimise errors.~~ In multiple Engine installations, the possibility of software/AEH errors that are common to more than one Engine Control System may determine the criticality level of the software/AEH.

(b) Approved Methods

Methods for developing software/AEH~~,~~ that are compliant with the guidelines contained in the latest edition of AMC 20-115/AMC 20-152 are acceptable methods. Alternative methods for developing software/AEH may be proposed by the applicant and are subject to approval by EASA~~the Agency~~.

Software/AEH which was not developed using the versions of ED-12/ED-80 referenced in the latest edition of AMC 20-115/AMC 20-152 is referred to as legacy software/AEH. In general, changes made to legacy software/AEH applicable to its original installation are assured in the same manner as the original certification. When legacy software/AEH is used in a new aircraft installation that requires the latest edition of AMC 20-115/AMC 20-152, the original approval of the legacy software/AEH is still valid, assuming that equivalence to the required software/AEH criticality level can be ascertained. If the software/AEH development method equivalence is acceptable to EASA~~the Agency~~, taking into account the conditions defined in the latest edition of AMC 20-115/AMC 20-152, the legacy software/AEH can be used in the new installation ~~that requires AMC 20-115 software~~. If equivalence cannot be substantiated, all the software changes should be assured through the use of the latest edition of AMC 20-115 for software or of AMC 20-152 for AEH.

Note: In this AMC, the 'criticality level' is used to reflect either the software level of a software item or the AEH design assurance level (or DAL) of an AEH item.

(c) Software/AEH criticality ~~L~~level ~~of software design assurance~~

~~In multiple Engine installations, the design, implementation and verification of the software in accordance with Level A (as defined in the industry documents referred in the latest edition of AMC 20-115) is normally needed to achieve the certification objectives for aircraft to be type certificated under CS-25, CS-27 Category A and CS-29 Category A.~~

~~The criticality of functions on other aircraft may be different, and therefore, a different level of software development assurance may be acceptable. For example, in the case of a piston engine in a single engine aircraft, level C (as defined in the industry documents referred in the latest edition of AMC 20-115) software has been found to be acceptable.~~

The software/AEH criticality level is determined by the Engine safety assessment process. ED-79A/ARP4754A and ARP4761 provide guidelines on how to conduct an aircraft/Engine/system safety assessment process. The Engine software/AEH should be developed at the criticality levels that have been determined and agreed by the Engine and aircraft applicants. It is assumed that by this agreement, the aircraft certification specifications are met.

Determination of the appropriate software/AEH criticality level may depend on the Failure modes and consequences of those Failures. For example, it is possible that Failures resulting in significant thrust or power increases or oscillations may be more severe than an Engine shutdown~~,~~ and, therefore, the possibility of these types of Failures should be considered when selecting a given software/AEH criticality level.

~~It may be possible to partition non-critical software from the critical software and design and implement the non-critical software to a lower level as defined by the industry documents referred in the latest edition of AMC 20-115. The adequacy of the partitioning method should be demonstrated. This demonstration should consider whether the partitioned lower software levels are appropriate for any anticipated installations. Should the criticality level be higher in subsequent installations, it would be difficult to raise the software level.~~

[…]

(11) RESERVED~~PROGRAMMABLE LOGIC DEVICES~~

~~CS E 50 (f) applies to devices referred to as Progammable Logic Devices.~~

~~Because of the nature and complexity of systems containing digital logic, the Programmable Logic Devices should be developed using a structured development approach, commensurate with the hazard associated with Failure or malfunction of the system in which the device is contained.~~

~~RTCA DO-254/ EUROCAE ED-80 which describes the standards for the criticality and design assurance levels associated with Programmable Logic Devices development, is an acceptable means, but not the only means, for showing compliance with CS E 50 (f).~~

~~For off the shelf equipment or modified equipment, service experience may be used in showing compliance to these standards. This should be acceptable provided the worst case Failure or malfunction of the device for the new installation is no more severe than that for original installation of the same equipment on another installation. Consideration should also be given to any significant differences related to environmental, operational or the category of the aircraft where the original system was installed and certified.~~

[…]

(15) ENGINE, PROPELLER AND AIRCRAFT SYSTEMS INTEGRATION AND THE INTERRELATION~~INTER-RELATION~~ BETWEEN ENGINE, PROPELLER AND AIRCRAFT CERTIFICATION ACTIVITIES

[…]

(c) Certification activities

(i) Objective

To satisfy the aircraft specifications, such as CS 25.901, CS 25.903 and CS 25.1309, an analysis of the consequences of Failures of the Engine Control System on the aircraft has to be made. The Engine applicant should, together with the aircraft applicant, ensure that the software/AEH criticality levels and the safety and reliability objectives for the Engine electronic control system are consistent with these specifications.

(ii) Interface Definition and System Responsibilities

System responsibilities as well as interface definitions should be identified for the functional as well as~~and~~ hardware and software aspects between the Engine, Propeller and the aircraft systems in the appropriate documents.

The Engine/Propeller/aircraft documents should cover in particular:

— Functional requirements and criticality (which may be based on Engine, Propeller and aircraft considerations);

— Fault Accommodation strategies;

— Maintenance strategies;

— The software/AEH criticality level (per function if necessary);~~,~~

— The reliability objectives for:

— LOTC/LOPC events,

— Transmission of faulty parameters;

— The environmental requirements including the degree of protection against lightning or other electromagnetic effects (e.g. level of induced voltages that can be supported at the interfaces);

— Engine, Propeller and aircraft interface data and characteristics;

— Aircraft power supply requirements and characteristics (if relevant).

(iii) Distribution of Compliance Tasks

The tasks for the certification of the aircraft propulsion system equipped with Electronic Engine Control Systems (EECSs) may be shared between the Engine, Propeller and aircraft applicants. The distribution of these tasks between the applicants should be identified and agreed with the appropriate Engine, Propeller and aircraft authorities. For further information, refer to AMC 20-1( ).

The aircraft certification should deal with the overall integration of the Engine and Propeller in compliance with the applicable aircraft specifications.

The Engine certification will address the functional aspects of the Engine Control System in compliance with the applicable Engine specifications.

Appropriate evidence provided for Engine certification should be used for aircraft certification. For example, the quality of any aircraft function software/AEH and aircraft~~/~~ – Engine interface logic already demonstrated for Engine certification should need no additional substantiation for aircraft certification.

Two examples are given below to illustrate this principle.

(A) Case of an EECS performing the functions for the control of the Engine and the functions for the control of the Propeller.

The Engine certification would address all general requirements such as software/AEH development ~~quality~~ assurance procedures, EMI, HIRF and lightning protection levels, effects of loss of aircraft-supplied power.

The Engine certification would address the functional aspects for the Engine functions (safety analysis, rate of~~for~~ LOTC/LOPC events, effect of loss of ~~A~~aircraft-~~S~~supplied ~~D~~data, etc.). The Fault Accommodation logic affecting the control of the Engine, for example, will be reviewed at that time.

The Propeller certification will similarly address the functional aspects for the Propeller functions. The Fault Accommodation logic affecting the control of the Propeller, for example, will be reviewed at that time.

In this example, the Propeller functions and characteristics defined by the Propeller applicant, ~~that~~which are to be provided by the Engine Control System, would normally need to be refined by flight test. The Propeller applicant is responsible for ensuring that these functions and characteristics, ~~that~~which are provided for use during the Engine certification programme, define an airworthy Propeller configuration, even if they have not yet been refined by flight test.

With regard to changes in design, agreement by all parties involved should be reached so that changes to the Engine Control System that affect the Propeller system, or vice versa, do not lead to any inadvertent effects on the other system.

(B) Case of an aircraft computer performing the functions for the control of the Engine.

The aircraft certification will address all general requirements such as software/AEH development ~~quality~~ assurance procedures, EMI, HIRF and lightning protection levels.

The aircraft certification will address the functional aspects for the aircraft functions.

The Engine certification will address the functional aspects for the Engine functions (safety analysis, rate of~~for~~ LOTC/LOPC events, effect of loss of ~~A~~aircraft-~~S~~supplied ~~D~~data, etc.) The Fault Accommodation logic affecting the control of the Engine, for example, will be reviewed at that time.

5. AMC 20-8 is amended as follows:

AMC 20-8A Occurrence Reporting

1. INTENT

This AMC is interpretative material and provides guidance in order to determine when which occurrences should be reported to EASA the Agency, competent national authorities and to other organisations., and it provides guidance on the timescale for submission of such reports.

It also describes the objective of the overall occurrence-reporting system, including internal and external functions.

2. APPLICABILITY

(a) This AMC only applies to occurrence reporting by persons or/ organisations regulated by that are subject to Regulation (EC) No 1592/2002(EU) No 748/2012 and Regulation (EU) No 1321/2014 of the European Parliament and of the Council. It does not address reporting by aerodrome organisations, air navigation service providers and authorities themselves.

(b) In most cases, the obligation to report is on the holders of a certificate or approval, which in most cases are organisations, but in some cases can be a naturalsingle person. In addition, some reporting requirements are directed to persons. However, in order not to complicate the text, only the term 'organisation' is used.

(c) The AMC also does not apply to specifically address dangerous goods reporting. The definition of reportable dangerous goods occurrences is different from the other occurrences and the reporting system is also separate. This subject is covered in specific operationaloperating requirements and guidance, and in European Union regulations and ICAO Ddocuments, namely:

(i) ICAO Annex 18, The safe Transport of Dangerous Goods by Air, Chapter 12

(ii) ICAO Doc 9284-AN/905, Technical Instructions for the Safe Transport of Dangerous Goods by Air

(i) Commission Regulation (EU) No 965/2012 of 5 October 2012 laying down technical requirements and administrative procedures related to air operations pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council;

(ii) ICAO Annex 18 'Safe Transport of Dangerous Goods by Air'; and

(iii) ICAO Doc 9284-AN/905 'Technical Instructions for the Safe Transport of Dangerous Goods by Air'.

3. OBJECTIVE OF OCCURRENCE REPORTING

(a) The occurrence-reporting system is an essential part of the overall monitoring function. The objective of the occurrence-reporting, collection, investigation and analysis systems described in the applicable requirements of Regulation (EU) 2018/1139, as well as of Regulation (EU) No 376/2014 and the delegated and implementing acts adopted on the basis thereof the operating rules, and the airworthiness rules is to use the reported information to contribute to the

improvement of aviation safety~~,~~ and it should not be used to attribute blame or liability or to establish benchmarks for safety performance. ~~and not to attribute blame, impose fines or take other enforcement actions.~~

(b) The detailed objectives of the occurrence-reporting systems are to:

(i) ~~To~~ enable the assessment of the safety implications of each occurrence to be made, including previous similar occurrences, so that any necessary action can be initiated; ~~.~~ ~~T~~this includes determining what ~~and why it~~ had occurred and why, and what might prevent a similar occurrence from happening in the future; ~~.~~

(ii) ~~To~~ ensure that knowledge of occurrences is disseminated so that other persons and organisations may learn from them.

(c) The occurrence-reporting system is complementary to the normal day-to-day procedures and ~~'~~'control'~~'~~ systems and is not intended to duplicate or supersede any of them. The occurrence-reporting system is a tool to identify those occasions where routine procedures have failed.

(d) Occurrences should remain in the database when judged reportable by the person submitting the report as the significance of such reports may only become obvious at a later date.

4. REPORTING TO EASA~~THE AGENCY~~ AND COMPETENT~~NATIONAL~~ AUTHORITIES

(a) ~~Requirements~~For organisations that have their principal place of business in a Member State, Commission Implementing Regulation (EU) 2015/1018 provides a classification of the occurrences in civil aviation for which reporting is mandatory. This list should not be understood as being an exhaustive collection of all the issues that may pose a significant risk to aviation safety, and therefore reporting should not be limited to the items listed therein and the additional items identified in points 21.A.129(f) and 21.A.165(f) of Part 21.

For organisations that do not have their principal place of business in a Member State, such a list is provided in Section ~~8~~9.

(b) These lists are based on the following general airworthiness requirements:

~~(i) As detailed in the operating rules, occurrences defined as an incident, malfunction, defect, to prevent similar occurrences in the future. Known and planned preventive actions should be included within the report.~~

(i)~~(ii)~~ The design rules for products, ~~and~~ parts and appliances ~~design rules~~ prescribe that an occurrence~~s~~ that is defined as a failure, malfunction, defect or other occurrence related to a product or part, ~~or appliance~~ which has resulted ~~in~~ or may result in an unsafe condition, must be reported to EASA~~the Agency~~.

~~(iii) According to the product and part and appliances production rules occurrences defined as a deviation which could lead to an unsafe condition must be reported to the Agency and the national authority.~~

(ii) The product and part production rules prescribe that products or parts released from the production organisation with deviations from the applicable design data that could lead to a potential unsafe condition, as identified with the holder of the type certificate (TC) or

design approval holder (DAH), must be reported to the ~~Agency and the national~~ competent authority.

(iii)~~(iv)~~ The continuing airworthiness ~~maintenance~~ rules stipulate that an occurrence~~s~~ that is defined as ~~any condition of the aircraft or aircraft component that has resulted or may result in an unsafe condition that could seriously hazard the aircraft~~ any safety-related event or condition of an aircraft or component identified by the organisation that endangers or, if not corrected or addressed, could endanger an aircraft, its occupants or any other person, must be reported to the ~~national~~ competent authority.

(iv) In addition, the continuing airworthiness rules prescribe that any incident, malfunction, technical defect, exceedance of technical limitations, occurrence that would highlight inaccurate, incomplete or ambiguous information, contained in the Instructions for Continued Airworthiness (ICA) established in accordance with Regulation (EU) No 748/2012, or other irregular circumstance that has or may have endangered an aircraft, its occupants or any other person, must be reported to the competent authority and to the organisation responsible for the design of the aircraft.

~~(v) Reporting does not remove the reporter's or organisation's responsibility to commence corrective actions to prevent similar occurrences in the future. Known and planned preventive actions should be included within the report.~~

~~(b) Paragraph 10.g. of this AMC provides guidance as to what should be reported by an organisation to the authority. The list of criteria provided may be used as guidance for establishing which occurrences shall be reported by which organisation. For example, the organisation responsible for the design will not need to report certain operational occurrences that it has been made aware of, if the continuing airworthiness of the product is not involved.~~

(c) Reporting does not remove the responsibility of the reporter or the organisation to initiate actions to prevent similar occurrences from happening in the future.

(d) A design or maintenance programme may include additional reporting requirements for failures or malfunctions associated with that approval or programme.

~~**5. NOTIFICATION OF ACCIDENTS AND SERIOUS INCIDENTS**~~

~~In addition to the requirement to notify the appropriate accident investigating authorities directly of any accident or serious incident, operators should also report to the national authority in charge of supervising the reporting organisation.~~

~~6~~5. REPORTING TIME — MANDATORY REPORTING — INITIAL REPORT

(a) ~~The period of 72 hours is normally understood to start from when the occurrence took place or from the time when the reporter determined that there was, or could have been, a potentially hazardous or unsafe condition.~~

The period of 72 hours is normally understood to start from when the person or organisation became aware of the occurrence. This means that there may be up to 72 hours maximum for a person to report to the organisation or to directly report to the competent authority, plus 72 hours maximum for the organisation to report to the competent authority.

~~(b) For many occurrences there is no evaluation needed; it must be reported. However, there will be occasions when, as part of a Flight Safety and Accident Prevention programme or Quality Programme, a previously non-reportable occurrence is determined to be reportable~~

(~~c~~b) Within the overall limit of 72 hours for the submission of a report, the organisation should determine the degree of urgency ~~should be determined by the level of hazard~~ based on the severity of consequence judged to have resulted from the occurrence:

(i) Where an occurrence is judged to have resulted in an immediate and particularly severe consequence ~~significant hazard~~, EASA~~the Agency~~ and/or the competent~~national~~ authority expects to be notified~~advised~~ immediately, and by the fastest possible means (e.g. telephone, fax, telex, e-mail) of whatever details are available at that time. This initial notification should then be followed up by a report within 72 hours.

A typical example of severe consequences would be an uncontained Engine failure that results in damage to the aircraft primary structure.

(ii) Where the occurrence is judged to have resulted in a less immediate and less significant risk~~hazard~~, the report submission may be delayed up to the maximum of 72 hours in order to provide more details or more reliable information.

~~7~~6. CONTENT OF INITIAL REPORTS

~~(a) Notwithstanding other required reporting means as promulgated in national requirements (e.g. AIRPROX reporting), may be transmitted in any form considered acceptable to the Agency and/or national authority. The amount of information in the report should be commensurate with the severity of the occurrence. Each report should at least contain the following elements, as applicable to each organisation:~~

~~(i) Organisation name~~

~~(ii) Approval reference (if relevant)~~

~~(iii) Information necessary to identify the aircraft or part affected.~~

~~(iv) Date and time if relevant~~

~~(v) A written summary of the occurrence~~

~~(vi) Any other specific information required~~

~~(b) For any occurrence involving a system or component, which is monitored or protected by a warning and/or protection system (for example: fire detection/extinguishing) the occurrence report should always state whether such system(s) functioned properly.~~

(a) For organisations that have their principal place of business in a Member State, the content of mandatory reports and, where possible, voluntary reports, is defined in Annex I to Regulation (EU) No 376/2014.

(b) For organisations that do not have their principal place of business in a Member State, mandatory reports and, where possible, voluntary reports, should include the information below:

(i) when: UTC date;

(ii) where: State/area of occurrence — location of occurrence;

(iii) aircraft-related information: aircraft identification, State of Registry, make-model series, aircraft category, propulsion type, mass group, aircraft serial number, and aircraft registration number;

(iv) aircraft operation and history of flight: operator, type of operation, last departure point, planned destination, flight phase;

(v) weather: the relevant weather;

(vi) where relevant, air-navigation-services-(ANS)-related information: ATM contribution, service affected, ATS unit name;

(vii) where relevant, aerodrome-related information: location indicator (ICAO airport code), location on the aerodrome; and

(viii) aircraft-damage- or personal-injury-related information: severity in terms of the highest level of damage and injury, the number and type of injuries to persons on the ground and in the aircraft).

7. REPORTING TIME — FOLLOW-UP REPORTS

(a) For organisations that have their principal place of business in a Member State, the reporting timelines for follow-up reports are those defined in Article 13 of Regulation (EU) No 376/2014.

(b) For organisations that do not have their principal place of business in a Member State, the following applies: where the organisation identifies an actual or potential aviation safety risk as a result of their analysis of occurrences or groups of occurrences reported to EASA, it should:

(i) transmit the following information to EASA within 30 days from the date of notification of the occurrence to EASA:

(1) the preliminary results of the risk assessment performed; and

(2) any preliminary mitigation action to be taken;

(ii) where required, transmit the final results of the risk analysis to EASA as soon as they are available and, in principle, no later than 3 months from the date of the initial notification of the occurrence to EASA.

~~**8. NOTIFICATION TO OTHER AGENCIES**~~

~~For approved operations organisations, in addition to reporting occurrences to the national authority, the following agencies should also be notified in specific cases:~~

~~(a) Reports relating to 'security incidents' should also be notified to the appropriate local security agency~~

~~(b) Reports relating to air traffic, aerodrome occurrences or bird strikes should also be notified to the appropriate air navigation , aerodrome or ground agency~~

~~(c) Requirements for reporting and assessment of safety occurrences in ATM within the ECAC Region are harmonised within EUROCONTROL document ESARR 2.~~

8~~9~~. REPORTING AMONG~~BETWEEN~~ ORGANISATIONS

(a) In addition to reporting occurrences to the competent authority or EASA, reporting among organisations should be considered. Such reporting will depend on the type of the organisation,

its interfaces with other organisations, and their respective safety policies and procedures, as well as the extent of contracting or subcontracting.

(b) Organisations may develop a customised list of occurrences to be reported among them, adapted to their particular aircraft, operations or products, and the organisations with which they interface. Such a customised list of occurrences to be reported among organisations is usually included or referenced in the organisation's expositions/handbooks/manuals. Any such lists should, however, not be considered to be definitive or exhaustive, and it is essential for the reporter to use their judgement of the degree of risk or potential hazard that is involved.

~~(a)~~(c) ~~Requirements exist that address the~~The following provides a non-exhaustive list of reporting lines that exist for the reporting of occurrences among organisations ~~data~~ related~~ing~~ to unsafe or ~~un~~non-airworthy conditions~~. These reporting lines are~~:

(i) ~~P~~production ~~O~~organisation to the organisation responsible for the design;

(ii) ~~M~~maintenance organisation/continuing airworthiness management organisation (CAMO) to the organisation responsible for the design;

(iii) ~~M~~maintenance organisation/CAMO to the operator;

(iv) ~~O~~operator to the organisation responsible for the design; and

(v) ~~P~~production organisation to another production organisation.~~;~~

~~(b)~~(d) The '~~Organisation responsible for the design~~design approval holder' is a general term, which can be any one or a combination of the following natural persons or organisations:

(i) ~~H~~the holder of a ~~T~~type ~~C~~certificate (TC) of an ~~A~~aircraft, Engine or Propeller;

(ii) ~~H~~the holder of a ~~S~~supplemental ~~T~~type ~~C~~certificate (STC) on an ~~A~~aircraft, Engine or Propeller;

(iii) ~~H~~the holder of a European ~~T~~technical ~~S~~standard ~~O~~order (ETSO) ~~A~~authorisation; or

~~(iv) Holder of a European Part Approval (EPA)~~

(iv) the holder of a repair design approval or a change to a type design approval.

~~(c)~~(e) If it can be determined that the occurrence has an impact on or is related to an aircraft component which is covered by a separate design approval/authorisation (TC, STC~~,~~ or ETSO ~~or EPA~~), then the holder~~s~~ of such approval/authorisation should be informed. Such information must be part of the reporting to the 'main' design approval holder. If an occurrence concerns ~~happens on~~ a component which is covered by a~~n~~ TC, STC, repair or change design approval or an ETSO authorisation ~~or EPA~~ (e.g. during maintenance), then only that TC, STC, repair or change design approval holder or ETSO ~~A~~authorisation ~~or EPA~~ holder needs to be informed by the reporting person or organisation that first determined the impact of the TC, STC, repair or change design or ETSO authorisation.

(f) Any organisation that reports to the design approval holder should actively support any investigations that may be initiated by that organisation. Support should be provided by a timely response to information requests, and by making available the affected components, parts or appliances for the purpose of the investigation, subject to an agreement with the respective

component, part or appliance owners. Design approval holders are expected to provide feedback to the reporting organisations on the results of their investigations.

~~(d)~~(g) ~~The form and timescale for reports to be exchanged between organisations is left for individual organisations to determine. What~~To ensure that there is effective reporting among organisations, it is important ~~is~~ that:

(i) ~~a relationship exists~~an interface is established between the organisations to ensure that there is an effective and timely exchange of information related~~ing~~ to occurrences;

(ii) any relevant safety issue is identified; and

(iii) it is clearly established which party is responsible for taking further action, if required.

(h) Organisations should establish procedures to be used for reporting among them, which should include as a minimum:

(i) a description of the applicable requirements for reporting;

(ii) the scope of such reporting, considering the organisation's interfaces with other organisations, including any contracting and subcontracting;

(iii) a description of the reporting mechanism, including reporting forms, means, and deadlines;

(iv) safeguards to ensure the confidentiality of the reporter and protection of personal data; and

(v) the responsibilities of the organisations and personnel involved in reporting, including for reporting to the competent authority.

Such procedures should be included in the organisation's expositions/handbooks/manuals.

~~(e) Paragraph 10.g. of this AMC provides guidance as to what should be reported by an organisation to the authority. The list of criteria provided may be used as guidance for establishing which occurrences shall be reported to which organisation. For example, certain operational occurrences will not need to be reported by an operator to the design or production organisation.~~

~~10. REPORTABLE OCCURRENCES~~

~~(a) *General*. There are different reporting requirements for operators (and/or pilots in command commanders), maintenance organisations, design organisations and production organisations. Moreover, as explained in paragraph 4. and 8. 9. above, there are not only requirements for reporting to the Agency and national authority, but also for reporting to other (private) entities. The criteria for all these different reporting lines are not the same. For example the authority will not receive the same kind of reports from a design organisation than as from an operator. This is a reflection of the different perspectives of the organisations based on their activities.~~

Figure 1 below presents a simplified scheme of the~~all~~ reporting lines.

~~**Figure 1**~~

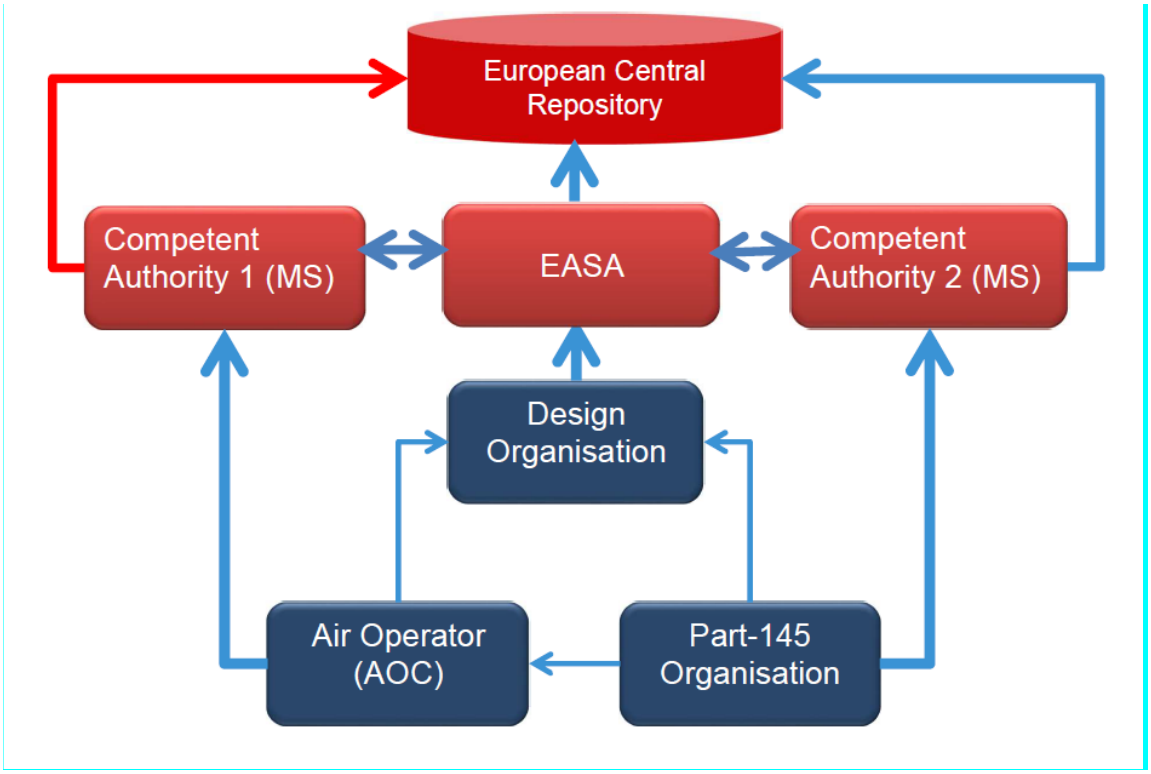

European Central Repository
Competent Authority 1 (MS)
EASA
Competent Authority 2 (MS)
Design Organisation
Air Operator (AOC)
Part-145 Organisation

Figure 1

9. REPORTABLE OCCURRENCES — MANDATORY REPORTING

For organisations that do not have their principal place of business in a Member State, the text below provides a classification of occurrences in civil aviation for which reporting is mandatory. This list should not be understood as being an exhaustive collection of all the issues that may pose a significant risk to aviation safety and, therefore, reporting should not be limited to the items listed therein and the additional items identified in points 21.A.129(f) and 21.A.165(f) of Part 21.

9.1. MANUFACTURING

Products, parts or appliances released from the production organisation with deviations from the applicable design data that could lead to a potential unsafe condition as identified by the holder of the type certificate or design approval.

9.2. DESIGN

Any failure, malfunction, defect or other occurrence related to a product, part or appliance which has resulted, or may result, in an unsafe condition.

Remark: This list is applicable to occurrences that occur on a product, part or appliance covered by the type certificate (TC), restricted type certificate (RTC), supplemental type certificate (STC), ETSO authorisation, major repair design approval or any other relevant approval deemed to have been issued in line with Commission Regulation (EU) No 748/2012.

9.3. MAINTENANCE AND CONTINUING AIRWORTHINESS MANAGEMENT

(a) Serious structural damage (for example, cracks, permanent deformation, delamination, debonding, burning, excessive wear, or corrosion) found during maintenance of the aircraft or component.

(b) Serious leakage or contamination of fluids (for example, hydraulic, fuel, oil, gas or other fluids).

(c) A failure or malfunction of any part of an Engine or power plant and/or transmission that results in either or both of the following:

(i) non-containment of components/debris;

(ii) failure of the Engine mount structure.

(d) Damage to a Propeller, or a failure or defect of a Propeller, which could lead to in-flight separation of the Propeller or any major portion of the Propeller and/or malfunctions of the Propeller control.

(e) Damage to a main rotor gearbox/attachment, or a failure or defect of a main rotor gearbox/attachment, which could lead to an in-flight separation of the rotor assembly and/or malfunctions of the rotor control.

(f) A significant malfunction of a safety-critical system or equipment, including a malfunction of an emergency system or equipment during maintenance testing, or a failure to activate these systems after maintenance.

(g) The incorrect assembly or installation of components of the aircraft found during an inspection or test procedure that was not intended for that specific purpose.

(h) An incorrect assessment of a serious defect, or a serious non-compliance with the MEL or the technical logbook procedures.

(i) Serious damage to the electrical wiring interconnection system (EWIS).

(j) Any defect in a life-controlled critical part that causes its retirement before the completion of its full service life.

(k) The use of products, components or materials from an unknown or suspect origin, or unserviceable critical components.

(l) Misleading, incorrect or insufficient applicable maintenance data or procedures, including language issues, which could lead to significant maintenance errors.

(m) The incorrect control or application of aircraft maintenance limitations or scheduled maintenance.

(n) Releasing an aircraft to service from maintenance if there remains any non-compliance which endangers flight safety.

(o) Serious damage caused to an aircraft during maintenance activities due to incorrect maintenance or the use of inappropriate or unserviceable ground support equipment that requires additional maintenance actions.

(p) Identified occurrences of burning, melting, smoke, arcing, overheating or fire.

(q) Any occurrence in which human performance, including the fatigue of the personnel, has directly contributed, or could have contributed, to an accident or a serious incident.

(r) A significant malfunction, reliability issue, or recurrent recording quality issue that affects a flight recorder system (such as a flight data recorder system, a data link recording system or a cockpit voice recorder system) or a lack of the information needed to ensure the serviceability of a flight recorder system.

~~(b) *Operations and Maintenance*. The list of examples of reportable occurrences offered below under g. is established from the perspective of primary sources of occurrence information in the operational area (operators and maintenance organisations) to provide guidance for those persons developing criteria for individual organisations on what they need to report to the Agency and/or national authority. The list is neither definitive nor exhaustive and judgement by the reporter of the degree of hazard or potential hazard involved is essential.~~

~~(c) *Design*. The list of examples will not be used by design organisations directly for the purpose of determining when a report has to be made to the authority, but it can serve as guidance for the establishment of the system for collecting data. After receipt of reports from the primary sources of information, designers will normally perform some kind of analysis to determine whether an occurrence has resulted or may result in an unsafe condition and a report to the authority should be made. An analysis method for determining when an unsafe condition exists in relation to continuing airworthiness is detailed in the AMCs regarding the issuance of Airworthiness Directives.~~

~~(d) *Production*. The list of examples is not applicable to the reporting obligation of production organisations . Their primary concern is to inform the design organisation of deviations.~~

Only in cases where an analysis in conjunction with that design organisation shows that the deviation could lead to an unsafe condition, should a report be made to the Agency and/or national authority (see also c. above).

(e) *Customised list.* Each approval, certificate, authorisation other than those mentioned in sub paragraph c and d above, should develop a customised list adapted to its aircraft, operation or product. The list of reportable occurrences applicable to an organisation is usually published within the organisation's expositions/handbooks/manuals

(f) *Internal reporting*. The perception of safety is central to occurrence reporting. It is for each organisation to determine what is safe and what is unsafe and to develop its reporting system on that basis. The organisation should establish an internal reporting system whereby reports are centrally collected and reviewed to establish which reports meet the criteria for occurrence reporting to the Agency and/or national authority and other organisations, as required.

(g) *List of examples of reportable occurrences*

The following is a generic list. Not all examples are applicable to each reporting organisation. Therefore each organisation should define and agree with the Agency and/or national authority a specific list of reportable occurrences or a list of more generic criteria, tailored to its activity and scope of work (see also 10.e above). In establishing that customised list, the organisation should take into account the following considerations:

Reportable occurrences are those where the safety of operation was or could have been endangered or which could have led to an unsafe condition. If in the view of the reporter an occurrence did not hazard the safety of the operation but if repeated in different but likely circumstances would create a hazard, then a report should be made. What is judged to be reportable on one class of product, part or appliance may not be so on another and the absence or presence of a single factor, human or technical, can transform an occurrence into a serious incident or accident.

Specific operational approvals, e.g. RVSM, ETOPS, RNAV, or a design or maintenance programme, may have specific reporting requirements for failures or malfunctions associated with that approval or programme.

A lot of the qualifying adjectives like 'significant' have been deleted from the list. Instead it is expected that all examples are qualified by the reporter using the general criteria that are applicable in his field, and specified in the requirement. (e.g. for operators: 'hazards or could have hazarded the operation')

CONTENTS:

I. AIRCRAFT FLIGHT OPERATIONS

~~A. Operation of the Aircraft~~

~~(1) (a) Risk of collision with an aircraft, terrain or other object or an unsafe situation when avoidance action would have been appropriate.~~

~~(b) An avoidance manoeuvre required to avoid a collision with an aircraft, terrain or other object.~~

~~(c) An avoidance manoeuvre to avoid other unsafe situations.~~

~~(2) Take-off or landing incidents, including precautionary or forced landings. Incidents such as under-shooting, overrunning or running off the side of runways. Take-offs, rejected take-offs, landings or attempted landings on a closed, occupied or incorrect runway. Runway incursions.~~

~~(3) Inability to achieve predicted performance during take-off or initial climb.~~

~~(4) Critically low fuel quantity or inability to transfer fuel or use total quantity of usable fuel.~~

~~(5) Loss of control (including partial or temporary loss of control) from any cause.~~

~~(6) Occurrences close to or above V_1 resulting from or producing a hazardous or potentially hazardous situation (e.g. rejected take-off, tail strike, engine power loss etc.).~~

~~(7) Go-around producing a hazardous or potentially hazardous situation.~~

~~(8) Unintentional significant deviation from airspeed, intended track or altitude. (more than 91 m (300 ft)) from any cause.~~

~~(9) Descent below decision height/altitude or minimum descent height/altitude without the required visual reference.~~

~~(10) Loss of position awareness relative to actual position or to other aircraft.~~

~~(11) Breakdown in communication between flight crew (CRM) or between Flight crew and other parties (cabin crew, ATC, engineering).~~

~~(12) Heavy landing - a landing deemed to require a 'heavy landing check'.~~

~~(13) Exceedance of fuel imbalance limits.~~

~~(14) Incorrect setting of an SSR code or of an altimeter subscale.~~

~~(15) Incorrect programming of, or erroneous entries into, equipment used for navigation or performance calculations, or use of incorrect data.~~

~~(16) Incorrect receipt or interpretation of radiotelephony messages.~~

~~(17) Fuel system malfunctions or defects, which had an effect on fuel supply and/or distribution.~~

~~(18) Aircraft unintentionally departing a paved surface.~~

~~(19) Collision between an aircraft and any other aircraft, vehicle or other ground object.~~

(20) Inadvertent and/or incorrect operation of any controls.

(21) Inability to achieve the intended aircraft configuration for any flight phase (e.g. landing gear and doors, flaps, stabilisers, slats etc).

(22) A hazard or potential hazard which arises as a consequence of any deliberate simulation of failure conditions for training, system checks or training purposes.

(23) Abnormal vibration.

(24) Operation of any primary warning system associated with manoeuvring of the aircraft e.g. configuration warning, stall warning (stick shake), over speed warning etc. unless:

(a) the crew conclusively established that the indication was false. Provided that the false warning did not result in difficulty or hazard arising from the crew response to the warning; or

(b) operated for training or test purposes.

(25) GPWS/TAWS 'warning' when:

(a) the aircraft comes into closer proximity to the ground than had been planned or anticipated; or

(b) the warning is experienced in IMC or at night and is established as having been triggered by a high rate of descent (Mode 1); or

(c) the warning results from failure to select landing gear or land flap by the appropriate point on the approach (Mode 4); or

(d) any difficulty or hazard arises or might have arisen as a result of crew response to the 'warning' e.g. possible reduced separation from other traffic. This could include warning of any Mode or Type i.e. genuine, nuisance or false.

(26) GPWS/TAWS 'alert' when any difficulty or hazard arises or might have arisen as a result of crew response to the 'alert'.

(27) ACAS RAs.

(28) Jet or prop blast incidents resulting in significant damage or serious injury.

B. Emergencies

(1) Fire, explosion , smoke or toxic or noxious fumes, even though fires were extinguished.

(2) The use of any non-standard procedure by the flight or cabin crew to deal with an emergency when:

(a) the procedure exists but is not used; or

(b) a procedure does not exist; or

(c) the procedure exists but is incomplete or inappropriate; or

(d) the procedure is incorrect; or

(e) the incorrect procedure is used.

(3) Inadequacy of any procedures designed to be used in an emergency, including when being used for maintenance, training or test purposes.

(4) An event leading to an emergency evacuation.

(5) Depressurisation.

(6) The use of any emergency equipment or prescribed emergency procedures in order to deal with a situation.

(7) An event leading to the declaration of an emergency ('Mayday' or 'Pan').

(8) Failure of any emergency system or equipment, including all exit doors and lighting, to perform satisfactorily, including when being used for maintenance, training or test purposes.

(9) Events requiring any emergency use of oxygen by any crew member.

C. Crew Incapacitation

(1) Incapacitation of any member of the flight crew, including that which occurs prior to departure if it is considered that it could have resulted in incapacitation after take-off.

(2) Incapacitation of any member of the cabin crew which renders them unable to perform essential emergency duties.

D. Injury

(1) Occurrences, which have or could have led to significant injury to passengers or crew but which are not considered reportable as an accident.

E. Meteorology

(1) A lightning strike which resulted in damage to the aircraft or loss or malfunction of any essential service.

(2) A hail strike which resulted in damage to the aircraft or loss or malfunction of any essential service.

(3) Severe turbulence encounter – an encounter resulting in injury to occupants or deemed to require a 'turbulence check' of the aircraft.

(4) A windshear encounter.

(5) Icing encounter resulting in handling difficulties, damage to the aircraft or loss or malfunction of any essential service.

F. Security

(1) Unlawful interference with the aircraft including a bomb threat or hijack.

(2) Difficulty in controlling intoxicated, violent or unruly passengers.

(3) Discovery of a stowaway.

G. Other Occurrences

(1) Repetitive instances of a specific type of occurrence which in isolation would not be considered 'reportable' but which due to the frequency at which they arise, form a potential hazard.

(2) A bird strike which resulted in damage to the aircraft or loss or malfunction of any essential service.

(3) Wake turbulence encounters.

(4) Any other occurrence of any type considered to have endangered or which might have endangered the aircraft or its occupants on board the aircraft or on the ground.

II.AIRCRAFT TECHNICAL

A. Structural

Not all structural failures need to be reported. Engineering judgement is required to decide whether a failure is serious enough to be reported. The following examples can be taken into consideration:

(1) Damage to a Principal Structural Element that has not been qualified as damage tolerant (life limited element). Principal Structural Elements are those which contribute significantly to carrying flight, ground, and pressurisation loads, and whose failure could result in a catastrophic failure of the aircraft. Typical examples of such elements are listed for large aeroplanes in AC/AMC 25.571(a) "damage tolerance and fatigue evaluation of structure", and in the equivalent AMC material for rotorcraft.

(2) Defect or damage exceeding admissible damages to a Principal Structural Element that has been qualified as damage tolerant.

(3) Damage to or defect exceeding allowed tolerances of a structural element which failure could reduce the structural stiffness to such an extent that the required flutter, divergence or control reversal margins are no longer achieved.

(4) Damage to or defect of a structural element, which could result in the liberation of items of mass that may injure occupants of the aircraft.

(5) Damage to or defect of a structural element, which could jeopardise proper operation of systems. See paragraph II.B. below.

(6) Loss of any part of the aircraft structure in flight.

B. Systems

The following generic criteria applicable to all systems are proposed:

(1) Loss, significant malfunction or defect of any system, subsystem or set of equipment when standard operating procedures, drills etc. could not be satisfactorily accomplished.

(2) Inability of the crew to control the system, e.g.:

(a) uncommanded actions;

(b) incorrect and or incomplete response, including limitation of movement or stiffness;

(c) runaway;

(d) mechanical disconnection or failure.

(3) Failure or malfunction of the exclusive function(s) of the system (one system could integrate several functions).

(4) Interference within or between systems.

(5) Failure or malfunction of the protection device or emergency system associated with the system.

(6) Loss of redundancy of the system.

(7) Any occurrence resulting from unforeseen behaviour of a system.

(8) For aircraft types with single main systems, subsystems or sets of equipment: Loss, significant malfunction or defect in any main system, subsystem or set of equipment.

(9) For aircraft types with multiple independent main systems, subsystems or sets of equipment: The loss, significant malfunction or defect of more than one main system, subsystem or set of equipment

(10) Operation of any primary warning system associated with aircraft systems or equipment unless the crew conclusively established that the indication was false provided that the false warning did not result in difficulty or hazard arising from the crew response to the warning.

(11) Leakage of hydraulic fluids, fuel, oil or other fluids which resulted in a fire hazard or possible hazardous contamination of aircraft structure, systems or equipment, or risk to occupants.

(12) Malfunction or defect of any indication system when this results in the possibility of misleading indications to the crew.

(13) Any failure, malfunction or defect if it occurs at a critical phase of flight and relevant to the operation of that system.

(14) Occurrences of significant shortfall of the actual performances compared to the approved performance which resulted in a hazardous situation (taking into account the accuracy of the performance calculation method) including braking action, fuel consumption etc.

(15) Asymmetry of flight controls; e.g. flaps, slats, spoilers etc.

Annex 1 to this AMC gives a list of examples of reportable occurrences resulting from the application of these generic criteria to specific systems

~~C. Propulsion (including Engines, Propellers and Rotor Systems) and APUs~~

~~(1) Flameout, shutdown or malfunction of any engine.~~

~~(2) Overspeed or inability to control the speed of any high speed rotating component (for example: Auxiliary power unit, air starter, air cycle machine, air turbine motor, propeller or rotor).~~

~~(3) Failure or malfunction of any part of an engine or powerplant resulting in any one or more of the following:~~

~~(a) non containment of components/debris;~~

~~(b) uncontrolled internal or external fire, or hot gas breakout;~~

~~(c) thrust in a different direction from that demanded by the pilot;~~

~~(d) thrust reversing system failing to operate or operating inadvertently;~~

~~(e) inability to control power, thrust or rpm;~~

~~(f) failure of the engine mount structure;~~

~~(g) partial or complete loss of a major part of the powerplant;~~

~~(h) Dense visible fumes or concentrations of toxic products sufficient to incapacitate crew or passengers;~~

~~(i) inability, by use of normal procedures, to shutdown an engine;~~

~~(j) inability to restart a serviceable engine.~~

~~(4) An uncommanded thrust/power loss , change or oscillation which is classified as a loss of thrust or power control (LOTC) as defined in AMC 20-1:~~

~~(a) for a single engine aircraft; or~~

~~(b) where it is considered excessive for the application, or~~

~~(c) where this could affect more than one engine in a multi-engine aircraft, particularly in the case of a twin engine aircraft; or~~

~~(d) for a multi engine aircraft where the same, or similar, engine type is used in an application where the event would be considered hazardous or critical.~~

~~(5) Any defect in a life controlled part causing retirement before completion of its full life.~~

~~(6) Defects of common origin which could cause an in flight shut down rate so high that there is the possibility of more than one engine being shut down on the same flight.~~

~~(7) An engine limiter or control device failing to operate when required or operating inadvertently.~~

~~(8) exceedance of engine parameters.~~

~~(9) FOD resulting in damage.~~

~~*Propellers and transmission*~~

~~(10) Failure or malfunction of any part of a propeller or powerplant resulting in any one or more of the following:~~

~~(a) an overspeed of the propeller;~~

~~(b) the development of excessive drag;~~

~~(c) a thrust in the opposite direction to that commanded by the pilot;~~

~~(d) a release of the propeller or any major portion of the propeller;~~

~~(e) a failure that results in excessive unbalance;~~

~~(f) the unintended movement of the propeller blades below the established minimum in-flight low-pitch position;~~

~~(g) an inability to feather the propeller;~~

~~(h) an inability to command a change in propeller pitch;~~

~~(i) an uncommanded change in pitch;~~

~~(j) an uncontrollable torque or speed fluctuation;~~

~~(k) The release of low energy parts.~~

~~*Rotors and transmission*~~

~~(11) Damage or defect of main rotor gearbox / attachment which could lead to in flight separation of the rotor assembly, and /or malfunctions of the rotor control.~~

~~(12) Damage to tail rotor, transmission and equivalent systems.~~

~~*APUs*~~

~~(13) Shut down or failure when the APU is required to be available by operational requirements, e.g. ETOPS, MEL.~~

~~(14) Inability to shut down the APU.~~

~~(15) Overspeed.~~

~~(16) Inability to start the APU when needed for operational reasons.~~

~~**D. Human Factors**~~

~~(1) Any incident where any feature or inadequacy of the aircraft design could have led to an error of use that could contribute to a hazardous or catastrophic effect.~~

~~**E. Other Occurrences**~~

~~(1) Any incident where any feature or inadequacy of the aircraft design could have led to an error of use that could contribute to a hazardous or catastrophic effect.~~

~~(2) An occurrence not normally considered as reportable (for example, furnishing and cabin equipment, water systems), where the circumstances resulted in endangering of the aircraft or its occupants.~~

(3) A fire, explosion, smoke or toxic or noxious fumes.

(4) Any other event which could hazard the aircraft, or affect the safety of the occupants of the aircraft, or people or property in the vicinity of the aircraft or on the ground.

(5) Failure or defect of passenger address system resulting in loss or inaudible passenger address system.

(6) Loss of pilots seat control during flight.

III. AIRCRAFT MAINTENANCE AND REPAIR

A. Incorrect assembly of parts or components of the aircraft found during an inspection or test procedure not intended for that specific purpose.

B. Hot bleed air leak resulting in structural damage.

C. Any defect in a life controlled part causing retirement before completion of its full life.

D. Any damage or deterioration (i.e. fractures, cracks, corrosion, delamination, disbonding etc) resulting from any cause (such as flutter, loss of stiffness or structural failure) to:

(1) primary structure or a principal structural element (as defined in the manufacturers' Repair Manual) where such damage or deterioration exceeds allowable limits specified in the Repair Manual and requires a repair or complete or partial replacement of the element;

(2) secondary structure which consequently has or may have endangered the aircraft;

(3) the engine, propeller or rotorcraft rotor system.

E. Any failure, malfunction or defect of any system or equipment, or damage or deterioration found as a result of compliance with an Airworthiness Directive or other mandatory instruction issued by a Regulatory Authority, when:

(1) it is detected for the first time by the reporting organisation implementing compliance;

(2) on any subsequent compliance where it exceeds the permissible limits quoted in the instruction and/or published repair/rectification procedures are not available.

F. Failure of any emergency system or equipment, including all exit doors and lighting, to perform satisfactorily, including when being used for maintenance or test purposes.

G. Non compliance or significant errors in compliance with required maintenance procedures.

H. Products, parts, appliances and materials of unknown or suspect origin.

I. Misleading, incorrect or insufficient maintenance data or procedures that could lead to maintenance errors.

J. Failure, malfunction or defect of ground equipment used for test or checking of aircraft systems and equipment when the required routine inspection and test procedures did not clearly identify the problem when this results in a hazardous situation.

IV. AIR NAVIGATION SERVICES, FACILITIES AND GROUND SERVICES

A. Air Navigation Services

(1) Provision of significantly incorrect, inadequate or misleading information from any ground sources, e.g. Air Traffic Control (ATC), Automatic Terminal Information Service (ATIS), Meteorological Services, navigation databases, maps, charts, manuals, etc.

(2) Provision of less than prescribed terrain clearance.

(3) Provision of incorrect pressure reference data (i.e. altimeter setting).

(4) Incorrect transmission, receipt or interpretation of significant messages when this results in a hazardous situation.

(5) Separation minima infringement.

(6) Unauthorised penetration of airspace.

(7) Unlawful radio communication transmission.

(8) Failure of ANS ground or satellite facilities.

(9) Major ATC/ Air Traffic Management (ATM) failure or significant deterioration of aerodrome infrastructure.

(10) Aerodrome movement areas obstructed by aircraft, vehicles, animals or foreign objects, resulting in a hazardous or potentially hazardous situation.

(11) Errors or inadequacies in marking of obstructions or hazards on aerodrome movement areas resulting in a hazardous situation.

(12) Failure, significant malfunction or unavailability of airfield lighting.

B. Aerodrome and Aerodrome Facilities

(1) Significant spillage during fuelling operations.

(2) Loading of incorrect fuel quantities likely to have a significant effect on aircraft endurance, performance, balance or structural strength.

(3) unsatisfactory ground de-icing / anti-icing

C. Passenger Handling, Baggage and Cargo

(1) Significant contamination of aircraft structure, or systems and equipment arising from the carriage of baggage or cargo.

(2) Incorrect loading of passengers, baggage or cargo, likely to have a significant effect on aircraft mass and/or balance.

(3) Incorrect stowage of baggage or cargo (including hand baggage) likely in any way to hazard the aircraft, its equipment or occupants or to impede emergency evacuation.

(4) Inadequate stowage of cargo containers or other substantial items of cargo.

(5) Dangerous goods incidents reporting: see operating rules.

D. Aircraft Ground Handling and Servicing

(1) Failure, malfunction or defect of ground equipment used for test or checking of aircraft systems and equipment when the required routine inspection and test procedures did not clearly identify the problem when this results in a hazardous situation.

(2) Non compliance or significant errors in compliance with required servicing procedures.

(3) Loading of contaminated or incorrect type of fuel or other essential fluids (including oxygen and potable water).

Annex 1 to AMC 20-8 — Reportable occurrences to specific systems

The following subparagraphs give examples of reportable occurrences resulting from the application of the generic criteria to specific systems listed in paragraph 10.g. II.B of this AMC.

1. Air conditioning/ventilation

(a) complete loss of avionics cooling

(b) depressurisation

2. Autoflight system

(a) failure of the autoflight system to achieve the intended operation while engaged

(b) significant reported crew difficulty to control the aircraft linked to autoflight system functioning

(c) failure of any autoflight system disconnect device

(d) Uncommanded autoflight mode change

3. Communications

(a) failure or defect of passenger address system resulting in loss or inaudible passenger address

(b) total loss of communication in flight

4. Electrical system

(a) loss of one electrical system distribution system (AC or DC)

(b) total loss or loss or more than one electrical generation system

(c) failure of the back up (emergency) electrical generating system

~~5. Cockpit/Cabin/Cargo~~

~~(a) pilot seat control loss during flight~~

~~(b) failure of any emergency system or equipment, including emergency evacuation signalling system , all exit doors , emergency lighting, etc~~

~~(c) loss of retention capability of the cargo loading system~~

~~6. Fire protection system~~

~~(a) fire warnings, except those immediately confirmed as false~~

~~(b) undetected failure or defect of fire/smoke detection/protection system, which could lead to loss or reduced fire detection/protection~~

~~(c) absence of warning in case of actual fire or smoke~~

~~7. Flight controls~~

~~(a) Asymmetry of flaps, slats, spoilers etc.~~

~~(b) limitation of movement, stiffness or poor or delayed response in the operation of primary flight control systems or their associated tab and lock systems~~

~~(c) flight control surface run away~~

~~(d) flight control surface vibration felt by the crew~~

~~(e) mechanical flight control disconnection or failure~~

~~(f) significant interference with normal control of the aircraft or degradation of flying qualities~~

~~8. Fuel system~~

~~(a) fuel quantity indicating system malfunction resulting in total loss or erroneous indicated fuel quantity on board~~

~~(b) leakage of fuel which resulted in major loss, fire hazard , significant contamination~~

~~(c) malfunction or defects of the fuel jettisoning system which resulted in inadvertent loss of significant quantity, fire hazard, hazardous contamination of aircraft equipment or inability to jettison fuel~~

~~(d) fuel system malfunctions or defects which had a significant effect on fuel supply and/or distribution~~

~~(e) inability to transfer or use total quantity of usable fuel~~

~~9. Hydraulics~~

~~(a) loss of one hydraulic system (ETOPS only)~~

~~(b) failure of the isolation system to operate~~

~~(c) loss of more than one hydraulic circuits~~

~~(d) failure of the back up hydraulic system~~

~~(e) inadvertent Ram Air Turbine extension~~

~~10. Ice detection/protection system~~

~~(a) undetected loss or reduced performance of the anti-ice/de-ice system~~

~~(b) loss of more than one of the probe heating systems~~

~~(c) inability to obtain symmetrical wing de-icing~~

~~(d) abnormal ice accumulation leading to significant effects on performance or handling qualities~~

~~(e) crew vision significantly affected~~

~~11. Indicating/warning/recording systems~~

~~(a) malfunction or defect of any indicating system when the possibility of significant misleading indications to the crew could result in an inappropriate crew action on an essential system~~

~~(b) loss of a red warning function on a system~~

~~(c) for glass cockpits: loss or malfunction of more than one display unit or computer involved in the display/warning function~~

~~12. Landing gear system /brakes/tyres~~

~~(a) brake fire~~

~~(b) significant loss of braking action~~

~~(c) unsymmetrical braking leading to significant path deviation~~

~~(d) failure of the L/G free fall extension system (including during scheduled tests)~~

~~(e) unwanted gear or gear doors extension/retraction~~

~~(f) multiple tyres burst~~

~~13. Navigation systems (including precision approaches system) and air data systems~~

~~(a) total loss or multiple navigation equipment failures~~

~~(b) total failure or multiple air data system equipment failures~~

~~(c) significant misleading indication~~

~~(d) significant navigation errors attributed to incorrect data or a database coding error~~

~~(e) unexpected deviations in lateral or vertical path not caused by pilot input.~~

~~(f) problems with ground navigational facilities leading to significant navigation errors not associated with transitions from inertial navigation mode to radio navigation mode.~~

~~14. Oxygen~~

~~(a) for pressurised aircraft: loss of oxygen supply in the cockpit~~

~~(b) loss of oxygen supply to a significant number of passengers (more than 10%), including when found during maintenance or training or test purposes~~

~~15. Bleed air system~~

~~(a) hot bleed air leak resulting in fire warning or structural damage~~

~~(b) loss of all bleed air systems~~

~~(c) failure of bleed air leak detection system~~

~~INTENTIONALLY LEFT BLANK~~

6. The following AMC 20-19 is inserted:

AMC 20-19 Passenger Service and In-Flight Entertainment (IFE) Systems

0 PREAMBLE

This document provides acceptable means of compliance (AMC) to obtain approval for the installation of in-flight entertainment (IFE) systems. It has been developed on the basis of Joint Aviation Authorities Temporary Guidance Leaflet (JAA TGL) No 17, and addresses the following concerns:

(a) the increase in the complexity of the IFE systems due to the additional cables, as well as the increase in the power needed for IFE systems;

(b) the potential consequences on the aircraft or passengers of system/electrical faults, including the risks of smoke, fire or interference with aircraft systems; these concerns are validated by adverse service experience with different types of aircraft;

(c) the potential consequences for other aircraft systems due to the transmitting capability of the IFE systems; and

(d) the lack of specific guidance on the installation of IFE systems, as these systems are categorised as non-essential services, even though these systems may affect compliance with the applicable provisions for seats and emergency evacuation.

1 PURPOSE

This AMC has been created to provide guidance to aircraft installers and equipment manufacturers on the airworthiness of IFE systems and equipment installed on civil aircraft. It does not constitute a regulation. It highlights safety concerns about IFE systems, and contains acceptable means of compliance to address those concerns and obtain airworthiness approval of such systems. An applicant for such an approval may choose another means of compliance.

2 RELATED CERTIFICATION SPECIFICATIONS (CSs)

Some of the certification specifications for which this AMC can be used are listed below. This list is for reference only and should not be considered as comprehensive. Additional CS-25 provisions are referenced where applicable. Provisions with the same number (e.g. CS 25.301) are generally read across to the other CSs (e.g. 27.301 and 29.301). However, please note that in some cases, the same topic is addressed by different provisions (e.g. for a specific CS-25 provision, the corresponding CS-23 provision may have a different number):

— CS 25.301, 303, 305, 307, 333, 337, 341, 365(g), 471, 561, 562, 581, 601, 603, 605, 609, 611, 785, 787, 789, 791, 811, 831, 853, 863, 869, 899, 1301, 1309, 1319, 1327, 1351, 1353, 1357, 1360, 1423, 1431, 1441, 1703, 1705, 1707, 1709, 1715, 1719, 1721, 1723;

— for CS-23:

  — Amendments 1 to 4: CS 23.561, 562, 785, 787, 791, 811, 867,-1301, 1309, 1327, 1351, 1353, 1357, 1359, 1431, 1441;

— Amendment 5: CS 23.2265, 2270, 2315, 2320, 2325, 2330, 2335, 2500, 2505, 2510, 2525, 2605, 2615;

— CS 27.561, 562, 610, 785, 787, 807, 853, 1301, 1309, 1319, 1327, 1351, 1353, 1357, 1365; and

— CS 29.561, 562, 610, 785, 787, 807, 853, 1301, 1309, 1319, 1327, 1351, 1353, 1357, 1359, 1431.

3 REFERENCE DOCUMENTS

The documents listed below are standards and guidance that were in force when this AMC (AMC 20-19) was adopted. Later or previous amendments may apply whenever the retained certification basis allows for it.

(a) ED Decision 2017/020/R, *AMC-20 — Amendment 14, AMC 20-115D, Airborne software development assurance using EUROCAE ED-12 and RTCA DO-178*, 19 October 2017

(b) ED Decision 2020/010/R, *AMC 20 — Amendment 19, AMC 20-152A, Development Assurance for Airborne Electronic Hardware,* July 2020

(c) ED Decision 2020/006/R, *AMC 20 — Amendment 18, AMC 20-42, Airworthiness information security risk assessment,* 24 June 2020

(d) ED Decision 2014/029/R, *AMC and GM to Part-CAT — Issue 2, Amendment 1, Portable electronic devices*, AMC/GM to CAT.GEN.MPA.140, 24 September 2014, as amended by ED Decision 2019/008/R of 27 February 2019

(e) EASA Certification Memorandum No CM-ES-001, *Certification of Power Supply Systems for Portable Electronic Device*, Issue 1, 7 June 2012

(f) EASA Certification Memorandum No CM-ES-003, *Guidance to Certify an Aircraft as PED tolerant*, *Issue 1*, 23 August 2017

(g) International Civil Aviation Organization (ICAO) Doc 9284-AN/905, *Technical Instructions for the Safe Transport of Dangerous Goods by Air* (Addendum No. 2), 30 June 2005

(h) Federal Aviation Administration (FAA) Advisory Circular (AC) 21-16G, RTCA Document DO-160 versions D, E, F, and G, 'Environmental Conditions Initiated by: AIR-100 and Test Procedures for Airborne Equipment', 22 June 2011

(i) FAA Policy Memorandum PS-ANM100-2000-00105 (also numbered 00-111-160), *Interim Policy Guidance for Certification of In-Flight Entertainment Systems on Title 14 CFR Part 25 Aircraft (Policy Number 00-111-160)*, 18 September 2011

(j) FAA AC 91.21-1D, *Use of Portable Electronic Devices Aboard Aircraft*, 27 October 2017

(k) FAA AC 20.168, *Certification Guidance for Installation of Non-Essential, Non-Required Aircraft Cabin Systems & Equipment (CS&E)*, 21 July 2010

(l) FAA AC 20.115D, *Airborne Software Development Assurance Using EUROCAE ED-12( ) and RTCA DO-178( )*, 21 July 2017

(m) FAA AC 21.49, *Gaining Approval of Seats with Integrated Electronic Components*, 9 February 2011

(n) EUROCAE ED-14G, RTCA DO-160G, *Environmental Conditions and Test Procedures for Airborne Equipment*, May 2011, December 2010

(o) RTCA DO-313, *Certification Guidance for Installation of Non-Essential, Non-Required Aircraft Cabin Systems and Equipment*, 2 October 2008

(p) Society of Automotive Engineers Aerospace Recommended Practice (SAE ARP) 5475, *Abuse Load Testing for In-Seat Deployable Video Systems*, 20 June 2005

(q) Aeronautical Radio, Incorporated (ARINC) 628, *Cabin Equipment Interfaces*, 27 December 1993

(r) MIL-STD-1472G, *Human Engineering*, 11 January 2012

3.1 Abbreviations

The following abbreviations are used in this AMC:

AC	advisory circular
AFM	aircraft flight manual
AMC	acceptable means of compliance
AMM	aircraft maintenance manual
ARP	aerospace recommended practice
CB	circuit breaker
CCOM	cabin crew operations manual
COTS	commercial off-the-shelf
CRI	certification review item
CSs	certification specifications
DAH	design approval holder
DDP	declaration of design and performance
DBS	direct-broadcast satellite
EASA	European Union Aviation Safety Agency
ELA	electrical-load analysis
EMI	electromagnetic interference
ESD	electrostatic discharge
ETSO	European technical standard order
EWIS	electrical-wiring interconnection system
FCOM	flight crew operations manual
FDAL	functional development assurance level
FHA	functional hazard assessment
GM	guidance material
GSM	global system for mobile communications
GUI	graphical user interface
ICA	Instructions for Continued Airworthiness

ICAO	International Civil Aviation Organization
IDAL	item development assurance level
IEEE	Institute of Electrical and Electronics Engineers
IFE	in-flight entertainment
LAN	local area network
MCA	mobile communications on aircraft
MMEL	master minimum equipment list
MoC	means of compliance
OEM	original-equipment manufacturer
PA	public address
PABX	private automatic branch exchange
PED	portable electronic device
PFIS	passenger flight information system
PSS	power supply system
RTCA	Radio Technical Commission for Aeronautics
R/T	real time; real-time (as modifier)
SAE ARP	Society of Automotive Engineers Aerospace Recommended Practice
SP	special condition
STC	supplemental type certificate
SWPM	standard wiring practices manual
TC	type certificate
T-PED	transmitting portable electronic device
USB	universal serial bus
VAC	volts alternating-current
VDC	volts direct-current
Wi-Fi	wireless fidelity
WLAN	wireless local area network

3.2 Definitions

The following definitions used in this AMC apply:

Term	**Definition**
In-flight entertainment systems	On-board systems that provide passengers with (safety) information, connectivity and entertainment

Installer	Type certificate (TC), supplemental type certificate (STC) or design approval holder (DAH)
COTS equipment	Equipment that is not designed or manufactured for use in aircraft, but is purchased by the installer for use in a particular aircraft system

4 SCOPE

Communication, information and entertainment systems are often provided for the convenience of aircraft passengers. As customer services improve, those systems are becoming more sophisticated and complex. Subsystem design features are often unique, based on the needs of operators, thus leading to many different possible IFE system configurations that depend both on the specific operator requirements and the cabin layout.

The following non-exhaustive list contains some examples of IFE systems:

(a) systems that provide passengers with audio entertainment and the related controls;

(b) systems that provide passengers with video entertainment and the related controls;

(c) passenger flight information systems (PFISs);

(d) systems that provide passengers with information, e.g. safety videos;

(e) interfaces to, and functions of, systems for controlling some cabin environment parameters such as, for example, reading lights, general cabin illumination, crew call buttons, air vents, etc.;

(f) systems that provide passengers with wired and/or wireless data distribution for entertainment connectivity including television (TV) and communication access (i.e. telephone, internet).

The aim of this AMC is to provide general criteria for the approval of such systems and equipment as they are installed in aircraft. The following aspects are addressed: mechanical installation, electrical installation, software/hardware aspects and electromagnetic compatibility, as well as the assessment of the potential hazards. In some cases, the application of this AMC, in conjunction with the certification basis for the product, is deemed to be sufficient.

For certain systems and equipment, additional certification material may be needed to address the aspects that are not covered by this AMC. Some examples are:

— IFE systems with wireless-communication capabilities (e.g. wireless fidelity (Wi-Fi) access points, mobile-phone systems);

— electrical outlets installed in the cabin for connecting portable electronic devices (PEDs);

— lithium batteries;

— data-loading systems;

— data communication systems (e.g. satellite TV, radios, passenger telephone systems, etc.); and

— large monitors/displays.

5 APPROVAL CONSIDERATIONS (AT AIRCRAFT LEVEL)

Section 6 below provides a summary of the issues that are pertinent to the safety of the aircraft, its occupants and maintenance personnel, which the equipment manufacturer and the installer should consider. Since IFE system installations are typical for commercially used large aeroplanes, it is expected that the approach to be followed for General Aviation (GA) aircraft will be different (for the purpose of this AMC, 'General Aviation aircraft' are those aircraft that comply with the CS-23 specifications). Section 6.7 below provides guidance in this regard. Some general considerations are presented below:

(a) The applicant for the approval of an IFE system should demonstrate compliance with the applicable aircraft certification basis. The installed IFE system should function as intended, and no 'credit' should be given for its performance capability. Substantiation is required to demonstrate that the IFE system and equipment in their installations and in operation do not interfere with the operation of other aircraft systems, or do not cause any hazard to the aircraft, to its occupants, or to maintenance personnel.

(b) If part of an IFE system is designed to transmit the required safety information (e.g. the passenger briefing), the replacement system should also meet the safety objectives required for that function. The installer should identify these safety objectives, which depend on the type of function for which the IFE system is used.

(c) The applicant may use existing approvals for interfacing equipment (e.g. IFE system parts mounted in seats). However, the applicant should ensure that all the applicable airworthiness provisions are addressed. For example, European technical standard orders (ETSOs) on seats do not contain electrical provisions; therefore, the electrical aspects of the seats should be reviewed to ensure that the installation of IFE system equipment does not invalidate the original ETSO for the seats.

(d) If other aircraft system installations are affected by the installation of the equipment of the IFE system, then the applicable requirements for these affected systems should be taken into account.

(e) If an IFE system is designed to be available for the operating crew, EASA should approve the related flight operation limitations.

(f) The applicant should demonstrate that any non-essential equipment (which includes equipment installed for the purpose of passenger entertainment), as installed:

- is not a source of danger in itself;
- does not prejudice the proper functioning of an essential service; and
- does not in any way reduce the airworthiness of the aircraft to which it is fitted, even in the event of a failure to perform its intended functions.

For example, for large aeroplanes, compliance should be demonstrated with CS 25.1309. A functional hazard assessment (FHA) should be performed to identify the IFE system failure scenarios and the worst possible consequences (e.g. electrical shock) for the aircraft and its occupants. This assessment should take into account electrical, electronic, and component faults that may result in a short circuit and/or electrical arcing and/or the release of smoke. Particular attention should be given to the likelihood of the following:

— accidental damage due to exposure of wiring or components in the cabin, such as wires that are pinched in the seat track;

— misuse of the equipment by passengers, such as the incorrect stowage of video screens, stepping on or kicking the seat electronic box, spilling liquids, etc.;

— electronic-component breakdowns; and

— wire chafing.

(g) The installer should demonstrate that the equipment of the IFE system has been installed in accordance with the equipment manufacturer's declaration of design and performance (DDP) and their installation instructions. The demonstration may, in addition, involve the examination and testing of the equipment. Subpart O 'EUROPEAN TECHNICAL STANDARD ORDER AUTHORISATIONS' of Annex I (Part 21) to Regulation (EU) No 748/2012 and the related AMC 21.A.608 provide guidance on drafting and formatting the DDP.

(h) If an operator allows passengers to use PEDs on board the aircraft, it should have procedures in place to control the use of those PEDs. Regulation (EU) No 965/2012 and the related ED Decisions contain, respectively, requirements and associated AMC and GM on PEDs. For commercial air transport (CAT) operations, the corresponding requirement is point CAT.GEN.MPA.140 of Annex IV (Part-CAT).

(i) If environmental testing of the IFE system equipment is required, EUROCAE ED-14/RTCA DO 160 'Environmental Conditions and Test Procedures for Airborne Equipment' may be followed. This is addressed in Section 0.1 below.

6 SYSTEMS INSTALLATION

6.1 Mechanical systems — aspects

6.1.1 Equipment location

The equipment and its controls should be positioned in locations where they do not impede the movement or the duties of the flight crew or the cabin crew (including in crew rest areas), or the normal movement of passengers.

(a) In a light aircraft, for example, if audio entertainment is audible to the pilot, a means to control the sound level should be provided to the pilot. Visual-entertainment equipment should be located where it does not distract the crew.

(b) Equipment should be located and, where necessary, protected to minimise the risk of injury to the occupants of the aircraft during a normal flight or an emergency landing. For equipment with cords in large aeroplanes, for example, the lengths of the cords should be determined by their possible effects on the egress capability of the occupants. The cords should not span across a main aisle such that they may become entangled in other features (such as armrests), thus impeding egress. Means for proper and easy stowage should be provided.

(c) Equipment used for screens should not obscure any required notices or information signs (e.g. 'EXIT', 'NO SMOKING', 'FASTEN SEAT BELT' signs, etc.). For video monitors in large-aeroplane installations, the following should apply:

(1) For video monitors installed above the aisle:

– all the installations should be such that the required 'EXIT' signs are still visible whether the monitors are fixed or retractable; if this is not possible, additional 'EXIT' signs are required;

– fixed video monitors should be such that the minimum distance between the cabin floor and the lowest point of the monitor is 185 cm (73 in); and

– retractable video monitors that do not meet the 185-cm (73-in) limit in the deployed position should not have sharp edges or should be padded, and they should be able to be stowed manually without requiring exceptional strength.

(2) For video monitors installed underneath overhead compartments:

– all the installations should be such that the required signs (e.g. 'NO SMOKING', 'FASTEN SEAT BELTS' signs, etc.) are visible whether the monitors are fixed or retractable; if this is not possible, additional signs are required;

– fixed video monitors should be padded and should not be installed above or between the seat backs of seat rows that border the access to emergency exits; and

– retractable video monitors should be able to be stowed manually without requiring exceptional strength and should not be installed above or between the seat backs of seat rows that border the access to emergency exits.

(d) Connecting units for wired on-board data exchange (e.g. USBs, local area networks (LANs), etc.) should be designed so that their use is obvious to the crew and passengers. Placards close to their outlet units should describe their capabilities and functions.

Units that are capable of supplying power with:

— a voltage greater than or equal to 42 V;

— power greater than 15 W; or

— a current greater than 3 A,

should be treated as power outlets.

(e) For individual video monitors attached to the seats (e.g. to the seat armrests, seat backs, movable hinge arms), the protection of the seat occupants, as well as of the crew and passengers moving around the cabin, should be considered. Video monitor installations should be such that injuries due to contact with sharp edges/corners during normal operation and turbulence are avoided. The abuse loading of video monitors (e.g. if a passenger leans on the monitor when taking or leaving their seat) should be accounted for. The criteria of SAE ARP5475 'Abuse Load Testing for In-Seat Deployable Video Systems' or alternatives, as agreed by EASA, may be used in assessing designs regarding this aspect.

6.1.2 Construction and attachment strength

(a) Any seat/monument installation, after modification, should continue to comply with the original certification basis.

(b) Equipment, attachments, supporting structures, and their constituent parts should be constructed such that they do not break loose when subjected to the loads (either for flight or for emergency ditching) that are prescribed in the relevant CSs. Some commercial off-the-shelf (COTS) equipment

might not comply with these provisions and may need to be strengthened before being installed in an aircraft (see Section 6.6 below on COTS equipment).

(c) The design of IFE-system-related antennas, their location and manner of attachment should be such that there is no adverse effect on the aircraft systems and no danger to the aircraft under any foreseeable operating conditions.

Remark: If external antennas are installed, the applicant should address the corresponding certification aspects, for which specific guidance is available (i.e. antennas in pressurised areas, the installation of large and/or deployable antennas, etc.). The certification approach for such external antenna installations should be agreed with EASA.

(d) As far as practicable, the equipment should be positioned so that if it breaks loose, it is unlikely to cause injury or to nullify any of the escape facilities for use after an emergency landing or after ditching. When such positioning is not practicable, each such item of equipment should be restrained under any load up to the prescribed ultimate inertia forces for the emergency landing conditions. Furthermore, for each item of equipment that is subject to frequent installation and removal, the local attachments of these items should be designed to withstand 1.33 times the specified loads (see CS 25.561(c)(2)). Compliance with CS 25.365(g) should also be considered.

Note 1: The structural provisions applicable to equipment can vary depending upon the type and size of the aircraft in which the equipment is installed; if the equipment is designed to be installed in any aircraft, then the applicant should consult all the relevant airworthiness CSs and create an envelope of conditions for design purposes.

Note 2: If an STC holder installs the equipment, they may need to consult the TC holder to obtain data on the vertical-acceleration factors (resulting from gusts and aircraft manoeuvres) that are applicable to a given aircraft type and to the proposed location of the equipment.

(e) If the IFE system is installed in a seat or in a monument adjacent to a seat, the installation may need to be reapproved for structural integrity and, if appropriate, for the emergency-landing dynamic conditions, including the occupant injury criteria. For large aeroplanes, for example, to avoid head injuries (CS 25.562(b) and CS 25.562(c), as referenced in CS 25.785) caused by seat-back-mounted IFE equipment, compliance with CS 25.562(c)(5) should be shown for a fully equipped seat back in the take-off and landing position.

(f) Weight and stress assessments should be made in cases of already embodied shelves that need to be relocated.

(g) Glass surfaces may be part of IFE system components, e.g. in display units. The potential hazard for the occupants in case of breakage of large sheets of glass should be considered. The approach that the applicant should follow should be agreed with EASA based on CS 25.788 (b). Compliance with CS.25.365(g) should also be considered.

6.2 Electrical systems — aspects

6.2.1 Power supplies

The IFE system equipment should be powered by an electrical busbar that does not supply power to the aircraft systems that are necessary for continued safe flight and landing.

The IFE system should be designed to provide circuit protection from overloads and short circuits by means of suitable protective devices.

(a) The method of connection of the equipment to the aircraft electrical system and the operation of the equipment should not adversely affect the reliability or integrity of the electrical system or any other electrical unit or system that is essential for the safe operation of the aircraft.

(b) If applicable, the aircraft electrical system should be protected from any unacceptable EMI caused by a connected PED.

(c) The flight/cabin crew should be provided with a clearly labelled and conspicuous means to disconnect an IFE system from its source of power at any time, and that means should be as close as practically possible to the source of power. The disabling/deactivating of component outputs should not be considered to be an acceptable means to cut off power, i.e. the disabling/deactivating of the output of a power supply unit, seat electronic box, etc., as opposed to cutting off the input power of the system. Moreover, pulling system circuit breakers (CBs) as the sole means to cut off the IFE system power is not considered to be acceptable. This is because CBs are not normally designed to be used as switches. The pulling and resetting of CBs over a period of time may degrade their trip characteristics, and then the CBs might not trip when required.

(d) An electrical-load analysis (ELA) should be carried out, taking into account the maximum load that the IFE system may utilise, to substantiate that the aircraft electrical-power generating system has sufficient capacity to safely provide the maximum amount of power required by the IFE system to operate properly. The applicant should base the IFE system ELA on an ELA that accurately reflects the aircraft's electrical loads prior to the installation of the IFE system. If this is not available, the applicant should make measurements of the aircraft's condition prior to the installation of the IFE system, and use these measurements for the ELA of the IFE system.

(e) The potential cumulative effect of the installation of multiple IFE units on the harmonic content of the electrical-power supply should be considered. There have been cases in which the installation of multiple IFE units with switched mode power supplies has changed the shape of the alternating current (AC) voltage waveform to the extent that the operation of the aircraft electrical power supply system (PSS) has been affected.

(f) Where batteries are used, consideration should be given to the stored energy, and provisions should be made for protection from short circuits and other potential failure modes.

The safety issues associated with the use in the IFE system of batteries whose technology may pose hazards that are not covered by the current provisions should be addressed by additional provisions to be agreed with EASA (e.g. for lithium battery technology).

6.2.2 Bonding

The electrical bonding, as well as the protection against static discharge of the installed system and equipment, should be such as to:

(a) prevent a dangerous accumulation of electrostatic charge; and

(b) minimise the risk of electrical shock to the crew, passengers and maintenance personnel.

The system bonding arrangements should be in accordance with the aircraft manufacturer's standard practices, and suitable for conducting any current, including a fault current, which may need to be conducted. The designer should take into account bonding connections in the system design such that the loss of a single bond does not result in the loss of more than one essential circuit or in the dangerous inadvertent operation of any aircraft system.

Cabin equipment designers should adhere to the standard practices for bonding, grounding and shielding, as well as to other methods for eliminating or controlling electrostatic discharge.

All electrical and electronic equipment and/or components should be installed so as to provide a continuous low-resistance path from their metallic enclosures and wiring to the aircraft bonding structure.

6.2.3 Interference

6.2.3.1 Magnetic effects

Whether the installed IFE system equipment is operating or not, the aircraft compass systems should continue to meet the prescribed accuracy standards. Where other equipment approved as part of the aircraft is installed, the installer should take account of the declared compass safe distance when designing the installation.

Account should be taken of the compass safe distance in respect of both the compass and the flux detector. The installer should also consider potential interference of the installed IFE system equipment with the relatively low-level signal of the compass system interconnecting cables.

6.2.3.2 Electromagnetic interference (EMI)

The levels of conducted and radiated interference generated by the equipment via power supply feeders, by system interfacing or by EMI should not cause an unacceptable degradation of the performance of other aircraft systems. If some equipment or functions are never used, the applicable system function should be properly disabled and/or terminated to prevent any interference with other aircraft systems.

(a) Antennas

Antennas for IFE systems should not be located where an unacceptable reduction in the performance of a mandatory radio system would result. In addition, the effects of a lightning strike on these antennas should be considered to ensure that essential services are not disrupted by electrical transients conducted to the aircraft via these antenna leads.

(b) Cumulative interference effects

The actual interference effect on an aircraft receiver may be the cumulative effect of many potentially interfering signals. For this reason, a system consisting of multiple units should be operable even in the worst-case orientation when interference tests/demonstrations are conducted. Tests/demonstrations should take into account the critical configurations of the use of the IFE system, including the critical configurations of passengers' portable electronic devices (PEDs) connected to the IFE system. The test configuration should be agreed with EASA.

(c) Flight phases

If the whole IFE system or parts of it are to be active during the critical flight phases (i.e. take-off and landing), particular attention should be paid to the demonstration of non-interference during these critical flight phases.

6.2.4 Electrical shock

Occupants should be protected against the hazard of electrical shock. Therefore, the applicant should demonstrate the means to minimise the risk of electrical shock as per CS 25.1360(a). Particular attention should be given to high-voltage equipment. If high- or low-voltage power outlets are available for passenger use, the aspects related to the use of PSSs for PEDs should be considered.

6.2.5 Wiring harness and routing

The electrical-wiring interconnection system (EWIS) associated with the IFE system should be installed, as for all other electrical systems, in accordance with the provisions of CS-25 Subpart H, or any equivalent document accepted by EASA. In order to meet these provisions, the applicant should adhere to the following guidelines:

— the wiring installation should be in accordance with the standard wiring practices manual (SWPM) of the aircraft or any equivalent standard accepted by EASA;

— standard original-equipment manufacturer (OEM) wiring or compatible types of wiring should be used;

— all the data necessary to define the design, in accordance with point 21.A.31 (Annex I (Part 21) to Regulation (EU) No 748/2012), including the installation drawings and wiring diagrams, shall be available; and

— where the IFE system EWIS is routed through standard aircraft wiring looms, spacers or equivalent means of separation should be used to keep the IFE EWIS at a minimum distance from any other electrical system in accordance with the SWPM of the aircraft.

In the absence of more specific guidelines in the SWPM of the aircraft, 230 VAC voltage power supply wires should not be routed through standard aircraft wiring looms. As the EWIS connected to the IFE system is present throughout the cabin (exposed in some cases), the potential for system faults is increased by the wide exposure to varying hazards (e.g. EWIS chafing in the seat tracks, passengers stepping on or kicking the seat electronic box, spilled liquids, etc.). Since these systems are exposed to hazards, the potential to adversely affect other systems that are necessary for the safe operation of the aircraft significantly increases, as well as the possibility of shock hazards to occupants. Special consideration should be given to the protection against damage to the IFE EWIS components installed in the seat itself: they should have appropriate protection means so that passengers cannot damage them with their feet or access them with their hands. The engineering data that controls the installation of IFE EWIS and equipment should contain specific and unambiguous provisions for the routing, support and protection of all IFE EWIS and equipment, and should specify all the parts that are necessary for those installations.

Care should be taken to ensure that any electrical IFE system equipment installed in aircraft seat assemblies does not invalidate the seat certification (e.g. the applicable ETSO). In addition, it should be noted that compliance alone with any applicable ETSO for seats does not cover the electrical equipment installation aspects of the IFE system.

6.3 Aircraft interaction and interfaces

If an IFE system is electrically interfaced with other aircraft systems, the performance and integrity of those aircraft systems should not be degraded. Appropriate means should be provided to isolate the IFE system from the aircraft systems.

(a) If an IFE system is connected to the aircraft avionics system (or any other system that may have a safety-related function), the installer should demonstrate that no malfunction of the IFE system may affect the aircraft avionics system. The installer should conduct a safety analysis to substantiate this. Supplementary to this safety analysis, special attention may be required due to cybersecurity issues. The installer should assess the information security aspects in accordance with AMC 20-42.

(b) If an IFE system interfaces with the public address (PA) function, the use of this system should not impair the audibility of crew commands or instructions. A PA override feature should be considered to allow cabin announcements to be heard by passengers.

(c) If an IFE system is available for the operating crew, the operation of this system should not interfere with, or adversely affect, the crew's ability to operate other aircraft systems and respond to alerting systems. The aircraft flight manual (AFM) should contain appropriate limitations and procedures.

The applicant should consider the following design interface features as acceptable means of compliance:

(1) no access to any form of visual entertainment equipment;

(2) automatic muting of the IFE systems when any cockpit aural caution or warning is sounding; there should be no perceptible delay between the muting of the IFE system and the activation of the caution/warning;

(3) automatic muting of the IFE systems when any real-time (R/T) transmission or reception is in progress; there should be no perceptible delay between the muting of the IFE system and the activation of the R/T transmission or reception; and

(4) readily available controls such that the volume of the IFE system is easily reduced.

(d) If an IFE system includes wireless capabilities (wireless local area network (WLAN), mobile phone, Bluetooth, etc.) to connect with other aircraft equipment and/or passenger or crew transmitting portable electronic devices (T-PEDs), the installer should address the electromagnetic compatibility of the aircraft with the intentional emissions of the IFE system, and the approach to be followed in that respect should be agreed with EASA.

Note: The responsibility for establishing the suitability for use of a PED on a given aircraft model continues to rest with the operator, as required by point CAT.GEN.MPA.140 (Annex IV (Part-CAT) to Regulation (EU) No 965/2012).

The design interface features used to comply with the above should be designed with a development rigour that depends on the function that is being interfaced with or replaced by the IFE system.

6.4 Software/airborne electronic hardware (AEH)

6.4.1 Software architecture

The software architecture of IFE system components should consider the following distinction between:

— core software as part of the functional scope defined in the specification of the component (e.g. operating systems, hardware drivers, functional applications such as PA), including all the required core software configuration data (the core software may be field loadable); and

— content data, including content configuration data (it may be field loadable by the aircraft operator); for IFE system equipment, the aircraft operator is usually required to make some adjustments and/or changes in the short term; such changes may be related to the content data and/or content configuration data — some examples of the latter are the following:

  — the selection of passenger-accessible graphical user interface (GUI) elements;

  — the activation of predefined GUI designs; and

  — the selection of regional information data (e.g. different country borderlines).

A change in the core software requires a component modification or redesign (change of part number) and, therefore, leads to a change in the aircraft configuration.

A change in the content data remains in the operational responsibility of the aircraft operator (field-loadable software) and, therefore, does not lead to a change in the aircraft configuration.

6.4.2 Software development assurance

The item development assurance level (IDAL) required for the IFE system software should be determined through the functional hazard assessment (FHA) that identifies the worst failure to which the software may contribute. If the IDAL is equal to IDAL D or greater, AMC 20-115, latest revision, provides guidance for the production of airborne systems and equipment software that performs its intended function with a level of confidence in its safety that is compliant with airworthiness provisions. This is an acceptable standard, and it should be taken into consideration for software in IFE systems, in particular those that replace or interface with the required functions of the aircraft.

6.4.3 Airborne electronic hardware (AEH) development assurance

The functional development assurance levels (FDALs) identified through the FHA should be used, in conjunction with the system architecture considerations, in order to determine the IDAL to be used for the development of airborne electronic hardware (AEH), and to identify the rigour of the development processes used.

For the development assurance of AEH of IFE systems that replace or interface with the required functions of the aircraft, the provisions of AMC 20-152, latest revision, apply.

6.5 Other risks

For the risks associated with hazards that may be caused by the IFE system equipment due to the operating environment of the aircraft, the standard environmental and operational test conditions and test procedures of EUROCAE ED-14/RTCA DO-160 may be used in combination with FAA AC 21-16G.

The responsibility for selecting the appropriate environmental and operational test conditions and test procedures lies with the installer. Section 6.5.1 below provides guidance on the selection of the test types. Sections 6.5.2, 6.5.3 and 6.5.4 below address other associated risks.

6.5.1 Environmental qualification

If the IFE system equipment is not linked to any other aircraft systems and is only connected to a non-essential power busbar, the following is recommended as a minimum list of environmental tests:

— temperature and altitude,

— temperature variation,

— operational shocks and crash safety,

— vibration,

— power input,

— voltage spikes, and

— emissions of radio frequency energy.

The installer is responsible for selecting the appropriate test conditions and for agreeing them with EASA. The assessment of the installation may prove that some of the above test types are unnecessary or, contrarily, that additional tests should be performed.

6.5.2 Touch temperature

In addition to CS 25.1360(b), the following should be considered: any hot surfaces of IFE system components that are accessible to the crew or passengers should not be exposed if inadvertent contact with those surfaces may pose a hazard.

The definition of MIL-STD-1472G 'HUMAN ENGINEERING' applies:

Equipment which, in normal operation, exposes personnel to surface temperatures greater than:

— *For momentary contact: 60°C for metal, 68°C for glass, 85°C for plastic or wood;*

— *For prolonged contact: 49°C for metal, 59°C for glass, 69°C for plastic or wood;*

or less than 0°C should be appropriately guarded.

6.5.3 Fluid exposure

If the equipment is mounted in a position where exposure to fluid is possible, for example on or under a passenger seat, or where catering operations take place or liquid cleaning agents are used regularly, it should be established that fluid spillage does not render the equipment hazardous. Where possible, installations in areas susceptible to moisture should be avoided. Otherwise, consideration should be given to minimise the hazard of liquid ingress, e.g. the inclusion of drip loops in wiring harnesses and the installation of drip trays.

If the approach described above is followed, the fluid susceptibility test may be disregarded.

6.5.4 Rapid decompression and high-altitude operation

The installer should ensure that no arcing that causes a fire risk or unacceptable levels of interference will occur in the equipment when the equipment is subjected to an atmospheric pressure that

corresponds to the maximum operating altitude of the aircraft. Alternatively, means should be provided to automatically disconnect the electrical supply to the equipment when the cabin pressure reduces to a level below which the safe operation of the equipment is not ensured (e.g. rapid decompression). The guidance of RTCA DO-313 in this area may also be followed.

This section should be followed in addition to the test conditions of Section 6.5.1.

6.5.5 Explosion, fire, fumes and smoke

(a) The installer should pay particular attention to the quality and design of components such as transformers, motors and composite connectors in order to minimise the risk of them overheating. The design of the mounting provisions for IFE system components installed in the passenger cabin (e.g. passenger seats, closet/cabin partition walls, overhead compartments, etc.) should fully reflect the cooling provisions for the equipment, including heat sinking, ventilation, proximity to other sources of heat, etc.

(b) All materials should meet the appropriate flammability provisions. Inadvertent blockage (e.g. by passengers' coats, luggage or litter) of any cooling vents should be prevented either by the design or by operational procedures. Appropriate protection against overheating should be part of the design of such in-seat systems.

(c) For the installation of IFE system components in racks located in the equipment bay that are not accessible in flight, the installer should address the potential hazard to other essential or critical systems/equipment located in the equipment bay, in case of an IFE system malfunction. The installer should substantiate that the worst-case scenario of a possible malfunction of the IFE system does not affect the components located in the equipment bay that are necessary for safe flight and landing. This demonstration should account for the risks of:

— overheating,

— smoke release,

— electrical failure, and

— fire propagation.

For large aeroplanes, for example, the following is considered an acceptable means of compliance in that respect: a hazard analysis to demonstrate that none of the potential ignition risks that originate from IFE system malfunctions pose a risk of a sustained fire in any area where IFE system components are located; this demonstration should account for:

— the fire containment properties of the equipment,

— the non-fire-propagating properties of the adjacent materials, and

— the detectability of fire and smoke.

(d) The installer should consider protecting IFE system components that are located in the cabin to ensure that fault conditions will not result in the failure of components within a unit that may generate smoke or fumes (e.g. if using tantalum capacitors). In addition, power supplies should have current-limiting output protection at a suitable level (e.g. in-seat equipment). The IFE system installation should comply with the applicable fire and smoke provisions of CS 25.831(c), CS 25.853(a), CS 25.863 and CS 25.869(a).

(e) Procedures should be established to terminate the operation of the IFE system at any time, in case of smoke/fire/explosion. The crew should maintain overall control over the IFE system. If control over the IFE system is possible via cabin controls only, appropriate procedures should address flight crew compartment–cabin coordination.

The guidance of RTCA DO-313 in this area may also be followed.

6.6 Commercial off-the-shelf (COTS) equipment

This section provides guidance for the cases in which the installer uses COTS equipment as part of an IFE system modification.

In principle, the installation of COTS equipment, as for all other IFE system equipment, should follow the guidance provided in this document. It is, nevertheless, recognised that COTS equipment is supplied from a market whose industry standards differ from the aviation ones. As a consequence, it may be difficult to follow some of the guidance of this document.

The main impediments are the following:

— traceability and configuration control; and

— it is burdensome to perform most of the testing in accordance with the state-of-the-art aviation standards (e.g. EUROCAE ED-14/RTCA DO-160).

In certain cases, the installer may directly follow the guidance provided in this document by using specific design features/adaptations and mitigations in terms of design or operational instructions.

The steps described below compose a road map that the installer may follow to apply for the approval of COTS equipment as part of an IFE system:

— The installer should perform a safety risk assessment of the potential hazards associated with the installation of the COTS equipment, either during normal operation of the equipment or in case of its failure.

— Based on the identified hazards, some evidence of environmental qualification for the equipment may be required. This could be achieved either by testing or by providing alternative laboratory standards to which the equipment has been tested, or industry standards to which the equipment has been certified. The acceptability of these standards should be agreed with EASA.

— A design solution may be developed in some cases to provide means of compliance that are alternatives to testing, e.g.:

  — hosting of the COTS component in a ‘shelter case’ (an air-tight-sealed housing) with electrical isolation of all the needed interfaces; or

  — a declaration of ‘loose equipment’ that is temporarily brought on board and is permanently accessible and visible by the crew.

— It should be ensured that the design specifications of the COTS equipment manufacturer are followed (in terms of the operating environmental conditions, cooling, etc.).

— Configuration control: quality control criteria should be provided for those aspects of the COTS equipment whose malfunctions may create hazards. If detailed design data is not available for such aspects, the applicant should propose a process by which the configuration control of the

design is maintained and should ensure that any changes in the design or any non-compliance introduced during manufacturing are identified. Critical characteristics of COTS equipment may include power, dimensions, weight, electrical power, software and hardware parts, material flammability behaviour, etc. This should also encompass subsequent changes to those parts.

The above points should help the installer in the certification of the COTS equipment. RTCA DO-313 Appendix D follows a similar approach and is considered to be an acceptable alternative.

6.7 Approach for General Aviation (GA) aircraft

This section provides guidance for the installation of IFE system equipment in GA aircraft.

The installer may follow the approach described in Sections 6.1 to 6.6, or follow the approach described below:

— Perform an assessment of the potential hazards associated with the installation of the IFE system equipment.

— Identify the list of hazards and possible safety issues created through either normal operation of the IFE system equipment or its failure.

— The hazards and issues described in Section 6 of this AMC may be used as a reference, but the applicant is not expected to demonstrate the same level of compliance as that required for large aircraft. Some evidence of environmental qualification (and/or testing) may be needed, but it is expected that in many cases, alternative compliance solutions may be provided. Some examples are the following:

  — specific-installation solutions or the use of mitigations (via limitations and/or placards) may provide an adequate level of safety and circumvent the need for environmental testing; and

  — industry and/or laboratory standards may provide an acceptable alternative.

  The acceptability of the above should be agreed with EASA.

— It should be ensured that the design specifications of the IFE system equipment manufacturer are followed (in terms of the operating environmental conditions, cooling, etc.).

— Configuration control: the configuration of the IFE system equipment should be identified, at least for those design features whose malfunctions may create hazards.

It is worth mentioning that in many cases, the IFE system equipment installed in GA aircraft is COTS equipment, thus the described approach largely reflects the approach to COTS equipment in Section 6.6 above.

7 DOCUMENTATION

This section provides guidance on the documentation that should be developed for IFE system installations.

7.1 Certification documentation

The certification documentation may consist of but it is not limited to:

— equipment specifications,

— the system description,

— analysis reports,

— test reports, and

— a DDP.

It should include references to the standards that are met.

The installer should demonstrate that they have taken proper account of the equipment manufacturer's DDP and installation instructions. This demonstration may, in addition, involve the examination and testing of the equipment. Point 21.A.608 (Subpart O of Annex I (Part 21) to Regulation (EU) No 748/2012) and AMC 21.A.608 provide guidance on the drafting and formatting of the DDP.

Appropriate documentation should be provided to define the designer's responsibilities for equipment installed in non-IFE system components of the cabin (e.g. IFE system equipment installed in seats or galleys, or in-seat wiring harnesses). A DDP should be provided to confirm that the installation of the IFE system equipment does not invalidate the approvals of existing equipment (e.g. seat ETSOs, or the certification of the galley).

Wire routing should be specified in detail to minimise the variability in manufacture, installation and maintenance in order to avoid the risk of wire chafing and damage.

7.2 Operations and training manuals

The design and installation of the IFE system should minimise its impact on the operational procedures. However, since flight or cabin crew procedures should comply with the applicable airworthiness provisions, these procedures should be included in the corresponding manufacturer's documentation to be provided to operators and, if appropriate, in the AFM.

7.3 Instructions for Continued Airworthiness (ICA)

For IFE system installations on board an aircraft, the installer should draft appropriate ICA and submit them to EASA. The installer should accomplish this task not only at the aircraft level, but also at the equipment level.

7.3.1 Equipment level

At the equipment level, the manufacturer should provide the installer with the necessary information for the safe operation and maintenance of the component. In particular, it should be highlighted whether a component requires scheduled maintenance or contains life-limited parts or has any other limitation that affects its continued airworthiness.

Suitable means of providing ICA information at equipment level are the following (examples only):

— operator's guides,

— CMMs,

— illustrated parts catalogues, or

— dedicated ICA manuals.

The documents that contain the ICA for the component/equipment should be referenced in the corresponding DDP and cross-referenced in the documentation at the aircraft level.

7.3.2 Aircraft level

At the aircraft level, CS 25.1529, CS 25.1729 (or an equivalent SC if contained in the certification basis) and Appendix H of CS-25, as applicable to the installation under consideration, determine the format and the minimum content of the ICA. The ICA for an IFE system may include the following:

— system descriptions and operating instructions such as (non-exhaustive list):
  — AFM supplements,
  — supplements to the master minimum equipment list (MMEL),
  — supplements to the flight crew operations manual (FCOM), and
  — supplements to the cabin crew operations manual (CCOM);
— maintenance instructions (including information on testing, inspections, troubleshooting, servicing, the replacement of parts, lifetime limitations, tooling and software loading) via supplements to the following (non-exhaustive list):
  — the aircraft maintenance manual (AMM),
  — the wiring manual,
  — the illustrated parts catalogue,
  — the maintenance planning document, and
  — the service manual.

The amount and content of the necessary ICA may vary depending on the kind of installation.

7.3.3 Scheduled maintenance tasks

The installer should draft the ICA by following the method applied during the certification process of the aircraft, including the development of scheduled maintenance tasks. However, some of these methods may not properly address the specific operational and technical conditions of the IFE system installations:

— in-service occurrences have shown that failures in or damage to the IFE system installation may become a potential source of ignition and heat, creating a smoke hazard and/or a fire hazard;
— particular attention should be given to in-seat equipment and wiring that is vulnerable to damage induced by passengers, servicing personnel, crew, changes to the cabin configuration or maintenance actions, which therefore may become potential sources of an electrical shock or other risks due to degraded or damaged electrical insulation; and
— contamination by dust, debris or spilled liquids in the cabin may cause overheating and a risk of smoke or fire.

These kinds of potential causes of failure, especially if the failure or damage is not easily detectable by the crew or the maintenance personnel while performing their normal duties, should also be considered when defining the scheduled maintenance tasks for IFE system installations.

The scheduled maintenance of IFE system installations may include but is not limited to the following tasks:

— functional checks of latent systems (e.g. the power shutdown function and/or IFE-system-specific smoke detection function);

— inspections (e.g. of the condition of system cabling and/or seat-mounted components; the correct position of physical protection, such as insulation, ducting, covers and/or drip trays);

— discarding/replacement of components (e.g. air filters and/or IFE system batteries); and

— restoration tasks (e.g. the cleaning of cooling vents or filters, the removal of dust and debris).

8 OPERATIONAL PROCEDURES

The regulatory requirements related to air operations are specified in Regulation (EU) No 965/2012 (see also the related AMC and GM). The operator should ensure that both the flight crew and the cabin crew are fully familiar with the operation of the IFE system, and that passengers are provided with appropriate information, including restrictions on the use of the IFE systems in normal, abnormal and emergency conditions.

7. The following AMC 20-152A is inserted:

AMC 20-152A Development Assurance for Airborne Electronic Hardware (AEH)

1 PURPOSE

1.1 This AMC describes an acceptable means, but not the only means, for showing compliance with the applicable airworthiness regulations for the electronic hardware aspects of airborne systems and equipment in product certification or ETSO authorisation. Compliance with this AMC is not mandatory, and an applicant may elect to use an alternative means of compliance. However, the alternative means of compliance must meet the relevant requirements, ensure an equivalent level of safety, and be approved by EASA on a product or ETSO article basis.

1.2 This AMC recognises EUROCAE ED-80, *Design Assurance Guidance for Airborne Electronic Hardware*, dated April 2000, and RTCA DO-254, *Design Assurance Guidance for Airborne Electronic Hardware*, dated 19 April 2000.

1.3 This AMC describes when to apply EUROCAE ED-80/RTCA DO-254, and it supplements EUROCAE ED-80/RTCA DO-254 with additional guidance and clarification for the development of custom devices, including the use of commercial off-the-shelf (COTS) intellectual property (IP), for the use of COTS devices and for the development of circuit board assemblies (CBAs).

The additional guidance and clarifications are provided in the form of objectives. The applicant is expected to describe the process and activities to satisfy the objectives of this AMC.

Note: EUROCAE ED is hereafter referred to as 'ED'; RTCA DO is hereafter referred to as 'DO'. Where the notation 'ED-80/DO-254' appears in this document, the referenced documents are recognised as being equivalent.

1.4 This AMC does not address the Single Event Effects (SEE) aspects or the assessment of the hardware susceptibility to SEE. AMC SEE aspects are usually addressed through a certification review item (CRI), and further guidance may be found in EASA CM-AS-004 Issue 01, issued 8 January 2018.

However, the Plan for Hardware Aspects of Certification may still be used to document the certification considerations for SEE.

2 APPLICABILITY

This AMC may be used by applicants, design approval holders, and developers of airborne systems and equipment containing airborne electronic hardware (AEH) to be installed on type-certified aircraft, engines, and propellers. This applicability includes the developers of ETSO articles.

This AMC is applicable to AEH that contributes to hardware development assurance level (DAL) A, DAL B, or DAL C functions.

When an objective is not applicable to a specific hardware DAL, the applicability restriction is directly indicated within the objective text with the following convention, for instance 'For DAL A hardware, …' For AEH contributing to hardware DAL C functions, only a limited set of objectives applies.

Even though there is a benefit in having a structured development process that ensures a proper flow-down of requirements to the hardware and the fulfilment by the hardware of the intended function, the

use of this AMC is not required for AEH contributing to hardware DAL D functions. Appendix B provides some clarifications that may be used to ensure that the DAL D hardware performs its intended function.

3 DOCUMENT HISTORY

This document is the initial issue of AMC 20-152. This initial issue, jointly developed with FAA, is intentionally set at Revision A.

4 BACKGROUND

This AMC is related to the development of custom devices in AEH, including the use of commercial off-the-shelf intellectual property (COTS IP) within custom devices, the use of COTS devices, and the development of circuit board assemblies (CBAs). Each of these topics is organised with:

— background information dedicated to each major topic,

— applicability, and

— sections where objectives are described and uniquely identified.

A unique identifier for each objective is defined with a prefix and an index number (i) as follows:

— for the development of custom devices, the identifier is ‘CD-i’;

— for the use of COTS IP in custom devices, the identifier is ‘IP-i’;

— for the use of COTS devices, the identifier is ‘COTS-i’;

— for the development of CBAs, the identifier is ‘CBA-i’.

Objectives are also differentiated from the rest of the text by formatting in italics.

The applicant should document in the Plan for Hardware Aspects of Certification (PHAC), or any other related planning document, the process and activities that the applicant intends to perform to satisfy the objectives of this AMC. The PHAC, as well as those related planning documents, should be submitted for certification.

5 CUSTOM DEVICE DEVELOPMENT

This section provides guidance for the development assurance of programmable logic devices (PLDs), field-programmable gate arrays (FPGAs), or application-specific integrated circuits (ASICs), which are collectively referred to as ‘custom devices’. These custom devices are addressed in ED-80/DO-254, Section 1.2, Item 3 as ‘custom micro-coded components’.

Developing a custom device demands a well-defined development process. However, it is understood that the process to develop complex custom devices requires more comprehensive activities and artefacts than for a simple device.

Section 5.1 identifies custom devices that are within the scope of this AMC.

Section 5.2 provides guidance on simple/complex classification for custom devices.

Section 5.3 provides guidance on development assurance for complex custom devices.

Section 5.4 provides guidance on development assurance for simple custom devices. In particular, Section 5.4 defines which sections from 5.5 to 5.11 are applicable to the development assurance of simple electronic devices.

Sections 5.5 to 5.10 provide clarifications on ED-80/DO-254.

Section 5.11 provides background information and guidance specific to COTS IP used in custom devices.

5.1 Applicability to Custom Devices

Section 5 is applicable to a digital- or mixed-signal custom device that contributes to hardware DAL A, B or C functions.

Appendix A to ED-80/DO-254 modulates the ED-80/DO-254 life-cycle data based on the DAL allocated to the hardware function. This document recognises Appendix A for the modulation of the life-cycle data according to the hardware DAL for the development of custom devices.

5.2 Simple/Complex Classification

ED-80/DO-254 introduces the notion of simple and complex hardware items. This section clarifies and provides criteria that could be used to classify a device as simple by considering the design content of the custom device, and subsequently, the ability to comprehensively verify the device.

A hardware custom device is classified as simple only if a technical assessment of the design content supports the ability of the device to be verified by a comprehensive combination of deterministic tests and analyses that ensure correct functional performance under all foreseeable operating conditions with no anomalous behaviour. The following criteria should be used for assessing whether a device should be classified as simple:

— simplicity of the functions and their number,

— number and the simplicity of the interfaces,

— simplicity of the data/signal processing or transfer functions, and

— independence of functions/blocks/stages.

Additional criteria specific to the digital part of the design include:

— whether the design is synchronous or asynchronous,

— number of independent clocks,

— number of state machines, number of states and state transitions per state machine, and

— independence between the state machines.

The applicant may propose other or additional criteria for the technical assessment of simplicity.

When an item cannot be classified as simple, it should be classified as complex. However, note that an item constructed entirely from simple items may itself be complex.

Objective CD-1

For each custom device, the applicant should document in the PHAC or any related planning document:

1. *the development assurance level,*
2. *the simple or complex classification, and*
3. *if a device is classified as simple, the justification based on the simple classification criteria.*

5.3 Development Assurance for Complex Custom Devices

ED-80/DO-254 is recognised as the industry standard for the development assurance of complex custom devices.

The applicant should satisfy ED-80/DO-254 and the additional objectives or clarifications described in this AMC from Sections 5.5 to 5.11.

5.4 Development Assurance for Simple Custom Devices

For the development of simple custom devices, it is understood that the life-cycle data might be significantly reduced compared with the data required for a complex custom device.

ED-80/DO-254 acknowledges that the documentation for the design process of a simple hardware device is less extensive than the one needed for a complex device. In addition, while verification and configuration management are also needed, these supporting processes also require less documentation for a simple device.

However, it is important that a simple custom device performs its intended function, and is under configuration management, thus allowing the device to be reproduced, conformed, and analysed to ensure continued operational safety.

Objective CD-2

The applicant should propose a process in the PHAC, or any other appropriate planning document, to develop simple custom devices which encompasses the following:

1. *definition of the device functions,*
2. *complete verification of the device functions through tests and analyses,*
3. *configuration management of the device, including problem reporting and the instructions to reproduce the device,*
4. *assessment of the build conformance of the device.*

Sections 5.5.2.4 and 5.5.2.5 of this document also apply to the verification process for simple custom devices.

The life-cycle data for simple devices can be combined with other hardware data.

If tools are used for the simple custom device development process, the objectives or clarifications of those objectives described in Section 5.8 of this document are also applicable.

When the applicant intends to reuse a previously developed simple device, ED-80/DO-254 Section 11.1 and the clarifications provided in Section 5.9 of this document should be used.

If the applicant intends to use COTS IP, the objectives or clarifications of those objectives described in Section 5.11 of this document are also applicable.

5.5 Clarifications to ED-80/DO-254 Validation and Verification Processes

5.5.1 Validation Process

Establishing a correct and complete set of requirements is the cornerstone of the development assurance process. ED-80/DO-254 Section 6.1 addresses the validation process to ensure the completeness and correctness of derived requirements. Nevertheless, the validation process is essential

for all the requirements. Indeed, the upper-level requirements allocated to the custom device are often refined, decomposed or restated at the custom device level, and in terms that support the hardware design. These custom device requirements, which are traceable from/to the upper-level requirements and, therefore, not considered to be 'derived', should also be correct and complete.

Objective CD-3

The applicant should validate all the custom device requirements by following the ED-80/DO-254 validation process (ED-80/DO-254 Section 6). This validation activity covers both derived and non-derived requirements.

For DAL A and B development, validation activities should be performed with independence.

Note: ED-80/DO-254 Appendix A defines acceptable means for establishing independence.

5.5.2 Verification Process

ED-80/DO-254 broadly describes the verification process, but additional guidance is needed to ensure the verification of the custom device is complete, particularly in the area of:

— design reviews,
— reviews of test cases and procedures, and
— verification of the implementation.

5.5.2.1 Conceptual Design Review

Conceptual design is the process of generating a high-level design description from the hardware requirements (see ED-80/DO-254 Section 5.2). The conceptual design review is typically used to ensure that the outcome of the conceptual design activities (see ED-80/DO-254 Section 5.2.2) is consistent with the requirements, and identifies constraints for the interfacing components (hardware or software) and architectural constraints for the detailed design activities of the custom device.

Since this conceptual design review is already addressed in ED-80/DO-254 Section 5.2.2 through the note, no separate objective is needed.

5.5.2.2 Detailed Design Review

Detailed design is the process of generating, from the conceptual design and the requirements, a hardware description language (HDL) or analogue representation of the design, constraints for the implementation (e.g. timing constraints, pinout, I/O characteristics), and the hardware–software interface description.

ED-80/DO-254 introduces design reviews in Section 6.3.3.2. A design review is considered to be an essential step during the detailed design process (ED-80/DO-254 Section 5.3) supporting the implementation process, and complementing requirements-based verification.

Objective CD-4

For hardware DAL A or DAL B, the applicant should review the detailed design with respect to the design standards, and review the traceability between the detailed design and the custom device requirements, in order to demonstrate that the detailed design covers the custom device requirements, is consistent with the conceptual design, and is compliant with the hardware design standards.

For hardware DAL C, the applicant should demonstrate that the detailed design satisfies the hardware design standards.

5.5.2.3 Implementation Review

Within a custom device development process, tools are used to convert the detailed design data into the physical implementation. While ED-80/DO-254 does not explicitly address it, a review of the design tool reports (e.g. synthesis and place and route reports) is necessary to ensure that the execution of the tool to generate its output was performed correctly.

Objective CD-5

When tools are used to convert the detailed design data into the physical implementation, the applicant should review the design tool reports (e.g. synthesis and place and route reports) to ensure that the tool executed properly when generating the output.

5.5.2.4 Review of Verification Cases and Procedures

ED-80/DO-254 introduces verification coverage analysis in Section 6.2.2 Item 4 to satisfy the ED-80/DO-254 verification process objectives and determine whether the verification process is correct and complete. A part of the coverage analysis is clarified by the following objective.

Objective CD-6

Each verification case and procedure should be reviewed to confirm that it is appropriate for the requirements to which it traces and that the requirements are correctly and completely covered by the verification cases and procedures.

5.5.2.5 Verification of the Timing Performance of the Implementation

ED-80/DO-254 Section 6.2 addresses the verification of the implementation. The implementation results from the process to generate the physical custom device from the detailed design data. The post-layout netlist is the closest virtual representation of the physical custom device, resulting from synthesis (for the digital part of the device) and place and route.

While it is recommended to test the implementation in its intended operational environment (i.e. by a physical test), verification using the post-layout netlist may be necessary to complement the verification of the implementation for certain requirements (e.g. features not accessible from the I/O pins of the device, timing, abnormal conditions, or robustness cases). In such cases, the coverage of the requirements by means other than a physical test should be justified.

The requirement to capture the activities in ED-80/DO-254 Section 5.1.2 Item 4.g introduces the need for the requirements to address signal timing characteristics under normal- and worst-case conditions. Nevertheless, ED-80/DO-254 does not explicitly address the necessity to verify the performance of the device under all possible (best-case and worst-case) timing conditions that could possibly occur during the operation of the device.

The following objective clarifies the need to take into account the variation of the environmental conditions (temperature, voltage, etc.) during the evaluation of the timing performance of the design, as well as the semiconductor device process variations.

Objective CD-7

The applicant should verify the timing performance of the design accounting for the temperature and power supply variations applied to the device and the semiconductor device fabrication process variations as characterised by the manufacturer of the semiconductor device.

Note: Static timing analysis (STA) with the necessary timing constraints and conditions is one of the possible means of compliance with this objective for the digital parts of custom devices.

5.6 Clarifications to ED-80/DO-254 'Robustness Aspects'

ED-80/DO-254 mentions robustness defects but does not explicitly address robustness. The robustness of the design is defined as the expected behaviour of the design under abnormal and boundary/worst-case operating conditions of the inputs and internal design states. These conditions are often captured as derived requirements when they are not allocated from the upper-level process. When subjected to these conditions, it is understood that the design may not continue to perform as it would under normal conditions.

Objective CD-8

For DAL A or DAL B hardware, the abnormal and boundary conditions and the associated expected behaviour of the design should be defined as requirements.

5.7 Recognition of HDL Code Coverage Method

HDL code coverage analysis is an assessment of whether the HDL code of the design has been exercised through HDL simulations.

The HDL code coverage method provides an assessment of the coverage of the design logic structure, giving an indication of which aspects of the logic structure are exercised and which are not.

When performed during requirements-based verification (per ED-80/DO-254 Section 6.2), HDL code coverage is recognised as a method to perform ED-80/DO-254 elemental analysis per Appendix B Section 3.3.1 for digital devices. HDL code coverage supports the assessment of whether the HDL code elements are fully covered by requirements-based simulations. As such, it does not represent an assessment of the completeness of the requirements-based testing activities or the effectiveness of the requirement coverage.

Objective CD-9

For hardware DAL A or DAL B, where HDL code coverage is used to perform elemental analysis (ED-80/DO-254 Appendix B Section 3.3.1), the applicant should define in the planning documents the

detailed coverage criteria of the HDL code elements used in the design. The criteria should ensure coverage over the various cases of the HDL code elements used in the design (e.g. branches, conditions, etc.). Any non-covered case or element should be analysed and justified.

Note: Code coverage might need to be complemented by additional analysis for any hardware items that are identified as not covered by the code coverage analysis, in order to complete the elemental analysis of all elements. This situation may occur in the use of some COTS IP instantiations.

5.8 Clarifications to ED-80/DO-254 'Tool Assessment and Qualification'

ED-80/DO-254 introduces the notion of tool assessment and qualification. ED-80/DO-254 Figure 11-1 includes a flow chart indicating the tool assessment considerations and activities, and provides guidance for when tool qualification may be necessary. This AMC uses the flow chart and its related text as a basis for providing further clarification, as follows:

ED-80/DO-254 — Figure 11-1 Item 1 — Identify the Tool

Information capturing the environment required for tool operation and the tool revision should be included with the tool identification.

ED-80/DO-254 — Figure 11-1 Item 2 — Identify the Process the Tool Supports

When identifying the design or verification process that the tool supports, it is important to also identify what purpose or activity within the hardware development process the tool satisfies. While assessing the tool limitations, evidence of formal assessment of the tool problem reports is not required if the tool output has been completely and independently assessed.

ED-80/DO-254 — Figure 11-1 Item 3 — Is the Tool Output Independently Assessed?

The purpose of assessing the tool output is to completely cover, with an independent means, the potential errors that the tool could introduce into the design or fail to detect during verification.

Objective CD-10

When the applicant intends to independently assess a tool output, the applicant should propose an independent assessment that verifies the tool output is correct. The independent assessment should justify that there is sufficient coverage of the tool output. The completeness of the tool assessment should be based on the design/implementation and/or verification objectives that the tool is used to satisfy.

ED-80/DO-254 — Figure 11-1 Item 4 — Is the Tool a Level A, B or C Design Tool or a Level A or B Verification Tool?

ED-80/DO-254 Figure 11-1 Item 4 of the tool assessment/qualification flow excludes the need for activities for tools 'used to assess the completion of verification testing, such as in an elemental analysis'.

The last statement is misleading regarding the intent of code coverage tools used for elemental analysis. As stated in Section 5.7 of this document, 'when a code coverage tool is used for elemental analysis, it

does not represent an assessment of the completeness of the requirements-based testing activities or the effectiveness of the requirement coverage'.

It is therefore necessary to provide some further clarifications.

— This document recognises the Figure 11-1 Item 4 exclusion of tool assessment/qualification activities for code coverage tools only when they are used to assess whether the code has been exercised by requirements-based testing/simulations (elemental analysis).
— If test cases or procedures are automatically generated by a tool and this tool uses coverage to determine the completion of the requirements verification, then the tool should be considered to be a verification tool to answer the question raised in Figure 11-1 Item 4.

ED-80/DO-254 — Figure 11-1 Item 5 — Does the Tool have Relevant History?

In ED-80/DO-254, the supporting text for Figure 11-1 Item 5 can be misinterpreted to suggest that when the tool has been previously used, no further tool assessment is necessary. Item 5 should be understood to mean that the applicant will provide sufficient data and justification to substantiate the relevance and credibility of the tool history.

Objective CD-11

When the applicant intends to claim credit for the relevant history of a tool, sufficient data should be provided as a part of the tool assessment to demonstrate that there is a relevant and credible tool history to justify that the tool will produce correct results for its proposed use.

ED-80/DO-254 — Figure 11-1 Item 9 — Design Tool Qualification

For design tools, contrary to the note in the supporting text for Figure 11-1 Item 9, the tool history should not be used as a stand-alone means of tool assessment and qualification. A relevant tool history may be used to compensate for some particular gaps in the tool assessment and qualification process, for example, to explain the method of independent assessment of the tool output. In this case, a relevant tool history is considered to be complementary data, providing more assurance for a tool.

In addition to what is already referenced in ED-80/DO-254 Figure 11-1 Item 9 for tool qualification guidance, ED-12C/DO-178C and ED-215/DO-330 may also be used.

5.9 Clarifications to ED-80/DO-254 regarding Previously Developed Hardware (PDH)

Previously developed hardware (PDH) is defined as custom-developed hardware that has been installed in an airborne system or equipment either approved through EASA type certification (TC/STC) or authorized through ETSOA. The section providing clarification on the use of PDH also covers PDH that was developed and approved prior to the use of ED-80/DO-254 in civil certification.

This section provides guidance on the use of ED-80/DO-254 Section 11.1 for PDH.

Objective CD-12

When an applicant proposes to reuse PDH, the applicant should use ED-80/DO-254 Section 11.1 and its subordinate paragraphs. The applicant should perform the assessments and analyses required in ED-80/DO-254 Section 11.1 in order to ensure that using the PDH is valid and that the compliance shown during the previous approval was not compromised by any of the following:

1. *Modification of the PDH for the new application or for obsolescence management;*
2. *Change to the function, change to its use, or change to a higher failure condition classification of the PDH in the new application; or*
3. *Change to the design environment of the PDH.*

The results should be documented in the PHAC or any other appropriate planning document.

In the context of custom device development, any one of these three points potentially invalidates the original development assurance credit for the PDH. In case of change or modification, the applicant should assess these changes using ED-80/DO-254 Section 11.1 and its subordinate paragraphs. When the original design assurance of the PDH is invalidated by one of the above points, the custom device should be upgraded based on the assessment per ED-80/DO-254 Section 11.1. When upgrading the hardware, the applicant should consider the objectives of this document that are applicable per the assessment.

5.10 Clarifications to ED-80/DO-254 Appendix A

This section clarifies the life-cycle data referenced in ED-80/DO-254 Appendix A as follows.

- The row corresponding to 10.1.6 ‘Hardware Process Assurance Plan’ in Table A-1 should also indicate HC2 for Level C to be consistent with row 10.8.
- The row corresponding to 10.2.2 ‘Hardware Design Standard’ in Table A-1 should also indicate HC2 for Level C. HDL Coding Standards are part of the Hardware Design Standards.
- The row corresponding to 10.3.2.2 ‘Detailed Design Data’ in Table A-1 should indicate HC1 for Levels A, B and C.
- The row corresponding to 10.4.2 ‘Hardware Review and Analysis Procedures’ in Table A-1 should also indicate HC2 for Level C to be consistent with row 10.4.3.
- The Top-Level Drawing referenced in ED-80/DO-254 Appendix A corresponds to a Hardware Configuration Index (HCI) document. The HCI document completely identifies the hardware configuration, the embedded logic, and the development life-cycle data. To support consistent and accurate replication of the custom device (ED-80/DO-254 Section 7.1), the Top-Level Drawing includes the hardware life cycle environment or refers to a Hardware Environment Configuration Index (HECI) document.

5.11 Use of COTS IP in Custom Device Development

This section addresses COTS IP that is instantiated within FPGAs/PLDs/ASICs during the development of the custom device.

This section addresses COTS IP and its integration within custom devices and describes objectives to support the demonstration of compliance with the applicable airworthiness regulations for the hardware aspects of airborne systems and equipment certification.

Section 5.11.2, on ‘Applicability to COTS IP’, identifies COTS IP that are within the scope of Section 5.11.

5.11.1 Background

IP refers to design functions (design modules or functional blocks, including IP libraries) used to design and implement a part of or a complete custom device such as a PLD, FPGA, or ASIC. IP is considered to be commercial off-the-shelf intellectual property, i.e. 'COTS IP', when it is a commercially available function, used by a number of different users, in a variety of applications and installations. Custom IP, developed for a few specific aircraft equipment, is not considered to be COTS IP.

COTS IP are available in various source formats. COTS IP are categorised as Soft IP, Firm IP, or Hard IP based on the stage in the custom device design flow where the IP is instantiated. A function can be a combination of source formats and each part needs to be addressed. Definitions for Soft IP, Firm IP, and Hard IP can be found in Appendix A 'Glossary'.

Figure 1 shows a 'simplified' design flow of a PLD, FPGA, or ASIC, and where Soft IP, Firm IP, and Hard IP are located in the design flow.

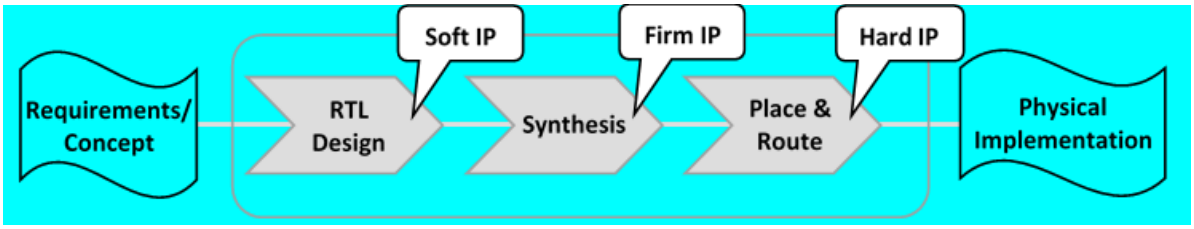


Figure 1 — Position of COTS IP within a 'simplified' design representation flow

The availability of a COTS IP does not guarantee that it is suitable to be used in a custom device for aircraft systems. Some COTS IP may have been developed using ED-80/DO-254, and will therefore have the necessary life-cycle data to demonstrate satisfaction of ED-80/DO-254. However, most COTS IP are not developed to meet aviation development assurance standards and, therefore, there are risks associated with their use in a custom device for aircraft systems or equipment.

The risks of using COTS IP may include:

- Incomplete or missing documentation/data regarding:
  - the behavioural operation of the COTS IP,
  - how to integrate it into the design;
- Insufficient verification performed by the COTS IP provider;
- Deficient quality of the COTS IP.

The potential for design errors may be increased by the lack of development assurance and/or by insufficient service experience.

Possible design errors within COTS IP or in the use of COTS IP may lead to a failure mode. Risk factors for these types of errors include:

- Unknown level of rigour of the COTS IP design and verification process;
- Misalignment between the intended usage of the COTS IP by the IP provider and the usage in the custom device by the IP user;
- Incomplete or missing details regarding the detailed operation of the COTS IP;
- Incorrect integration of the COTS IP with the rest of the custom device design;

— Integrator lacking expertise with the function of the IP.

Additionally, the COTS IP user completes the development of the integrated COTS IP up to the physical implementation of the device. The COTS IP user may introduce a design error while completing the physical implementation of the COTS IP because of the user's incomplete knowledge of the internal design of the COTS IP.

5.11.2 Applicability to COTS IP

Section 5.11 is applicable to COTS IP used in a custom device that meets the definition of 'commercial off-the-shelf intellectual property' in the Glossary of Appendix A. This scope encompasses digital, analogue, and mixed-signal COTS IP.

Note: Analogue COTS IP is within the above-mentioned scope, as it could be instantiated within a custom, mixed-signal device.

Section 5.11 is applicable to COTS IP contributing to hardware DAL A, B or C functions.

Section 5.11 is applicable to Soft IP, Firm IP, and Hard IP that are inserted within a custom device by the applicant. However, Section 5.11 does not apply to Hard IP that is embedded in the silicon of an FPGA or a PLD by the FPGA/PLD device manufacturer. This type of IP is considered to be part of the COTS device, and is covered in Section 6 'Use of Commercial Off-the-Shelf Devices.

5.11.3 Development Assurance for COTS IP

A COTS IP development assurance approach should be based on the category of the COTS IP (Soft, Firm, Hard) and on the identified risks of failure due to a design error in the COTS IP itself or an error in the way it is used in the custom device.

This section provides objectives addressing development assurance when using COTS IP. These objectives are intended to cover the particular aspects of development when using COTS IP, and are expressed in connection with the custom device development process that follows ED-80/DO-254 and the custom device objectives of this document.

The development aspects related to COTS IP start from the custom device process that captures the allocated requirements for the function that will be performed by the COTS IP. From this entry point, the following aspects provide a basis to define the development assurance objectives for the use of COTS IP:

— Selection of the COTS IP,
— Assessment of the IP provider and the IP data,
— Planning activities, including the verification strategy,
— Definition of the requirements/derived requirements,
— Design integration, implementation, and verification of the COTS IP in the custom device.

5.11.3.1 Selection of the COTS IP to implement the function

COTS IP can be available in different forms/source formats and various levels of quality. Some COTS IP may not be acceptable for use in airborne systems. The selection criteria below are intended to address the essential characteristics that are considered a minimum for the use of IP in custom AEH devices.

Objective IP-1

The applicant should select a COTS IP that is considered to be an acceptable solution, based on at least the following criteria:

1. *The IP is technically suitable for implementing the intended function;*
2. *The description of the COTS IP architecture or IP design concept provides an understanding of the functionality, modes, and configuration of the IP. The description should also include an understanding of the source format or combination of source formats of the COTS IP;*
3. *The availability and quality of data and documentation allow the understanding of all aspects of the COTS IP functions, modes, and behaviour, and enable the integration and verification of the COTS IP (e.g. datasheets, application notes, user guide, knowledge of errata, etc.);*
4. *Information exists for the IP user to be able to create the physical implementation of the COTS IP (e.g. synthesis constraints, usage and performance limits, physical implementation, and routing instructions);*
5. *It can be demonstrated that the COTS IP fulfils its intended function.*

5.11.3.2 Assessment of the COTS IP Provider and COTS IP Data

Objective IP-2

The applicant should assess the COTS IP provider and the associated data of the COTS IP based on at least the following criteria:

1. *The IP provider provides all the information necessary for the integration of the COTS IP within the custom device and to support the implementation of the COTS IP within the device (e.g. synthesis constraints, usage domain, performance limits, physical implementation, and routing instructions);*
2. *The configurations, selectable options, and scalable modules of the COTS IP design are documented so that the implementation of the COTS IP can be properly managed;*
3. *The COTS IP has been verified by following a trustworthy and reliable process, and the verification covers the applicant's specific use case for the COTS IP (including the used scale for scalable IP and the IP functions selected for selectable functions);*
4. *The known errors and limitations are available to the IP user, and there is a process to provide updated information to the IP user;*
5. *The COTS IP has service experience data that shows reliable operation for the applicant's specific use case for the COTS IP.*

The assessment should be documented. The results of the assessment should be submitted together with the planning documents.

5.11.3.3 Planning of the Hardware Development Assurance Approach related to COTS IP

5.11.3.3.1 Complementary Development Assurance

Objective IP-3

When the IP-2 Objective criteria items 1, 2, 4 or 5 cannot be completely met using the IP provider's data, the applicant should define an appropriate development assurance activity to mitigate the criteria that were not met and address the associated risk of development errors. The development assurance activity should be based on the ED-80/DO-254 objectives.

Note: The results of the assessment of Objective IP-2 Item 3 are considered in Section 5.11.3.3.2.

5.11.3.3.2 The Verification Strategy for COTS IP Functions

In addition to the verification of the custom device functions supported by the COTS IP, there is a need to ensure that the aspects related to the COTS IP and its usage are addressed. This section focuses on defining a verification strategy to cover those aspects.

The verification performed by the COTS IP provider typically does not follow the ED-80/DO-254 verification process but may provide some credit to be used for the verification strategy. However, the verification process for COTS IP generally differs from one IP vendor to another, and the level of assurance varies depending on the IP provider's development practices.

The verification strategy may combine different means to complement the traditional requirements-based testing approach.

Based on the applicant's assessment of the IP provider and the IP data through Objective IP-2, the applicant is expected to establish a verification strategy. The aim of this verification strategy is to cover all three of the following aspects:

— The COTS IP: the purpose is to ensure that the COTS IP is verified, addressing the risk identified from the IP-2 Item 3 objective;

— Its implementation: the purpose is to ensure that the COTS IP still performs its allocated function, and that no design errors have been introduced by the design steps performed by the applicant (e.g. synthesis/place and route);

— Its integration within the custom device: the purpose is to ensure that the COTS IP has been properly connected, configured, and constrained within the custom device.

The strategy may accomplish more than one aspect within a common verification step.

This section identifies a general objective for the verification of COTS IP used in a custom device, enabling various verification approaches.

Objective IP-4

The applicant should describe in the hardware verification plan, PHAC, or any related planning document, a verification strategy that should encompass all three of the following aspects:

1. The verification of the COTS IP itself, addressing the risk identified from the IP-2 Item 3 objective;
2. The verification of the COTS IP after the design steps performed by the applicant (e.g. synthesis/place and route);
3. The verification of the integrated COTS IP functions within the custom device.

Note 1: Reliable and trustworthy test data, test cases or procedures from the COTS IP provider may be used as part of the verification strategy to satisfy this objective.

Note 2: If the COTS IP implements functions based on an industry standard, proven standardised test vectors verifying compliance with the standard may be used in the verification strategy of the COTS IP.

Note 3: The verification strategy covers at a minimum the used functions of the COTS IP and ensures that the unused functions are correctly disabled or deactivated and do not interfere with the used functions.

5.11.3.3.3 COTS IP and Planning Aspects

The applicant has to define the activities that are needed for the hardware development assurance approach related to COTS IP.

Objective IP-5

The applicant should describe in the PHAC, or any related planning document, a hardware development assurance approach for using the COTS IP that at least includes:

1. *identification of the selected COTS IP (version) and its source format(s) associated with the point(s) in the design flow where the COTS IP is integrated into the custom device;*
2. *a summary of the COTS IP functions;*
3. *the development assurance process that the applicant defines to satisfy the objectives of Section 5.11.3;*
4. *the process related to the design integration and to the usage of the COTS IP in the development process of the custom device;*
5. *tool assessment and qualification aspects when the applicant uses a tool to perform design and/or verification steps for the COTS IP.*

5.11.3.4 Requirements for COTS IP Function and Validation

Custom device requirements typically contain requirements that relate to the function supported by the COTS IP. The granularity of these requirements may be very different depending on the COTS IP function and the visibility of the functions supported by the IP at the custom device level.

Depending on the extent of requirements-based testing as a part of the chosen verification strategy of the COTS IP, the level of detail and the granularity of the AEH custom device requirements may need to be refined to specifically address the COTS IP functions and the implementation of the COTS IP.

In addition, requirements should be captured to encompass all the necessary design detail used to connect, configure, and constrain the COTS IP and properly integrate it into the AEH custom device.

Objective IP-6

The requirements related to the allocated COTS IP functions should be captured to an extent commensurate with the verification strategy.

In addition, derived requirements should be captured to cover the following aspects associated with the integration of the COTS IP into the custom device design:

1. *COTS IP used functions (including parameters, configuration, selectable aspects);*
2. *Deactivation or disabling of unused functions;*
3. *Correct control and use of the COTS IP, in accordance with the data from the COTS IP provider.*

When the applicant chooses a verification strategy (see Section 5.11.3.3.2) that solely relies on requirements-based testing, the 'extent commensurate with the verification strategy' corresponds to a complete requirement capture of the COTS IP following ED-80/DO-254.

Regarding the validation aspects, the COTS IP requirements should be validated as a part of the validation process of the AEH custom device.

5.11.3.5 Verification

The applicant should ensure that the COTS IP is verified as a part of the overall custom device verification process per ED-80/DO-254 and based on the verification strategy for the COTS IP that has been described in the PHAC or a related planning document.

For the requirements-based verification part, the applicant should satisfy ED-80/DO-254 Section 6.2 for the verification of the requirements related to the COTS IP (see Section 5.11.3.4 above). This can be performed as a part of the overall custom device process, therefore there is no separate objective.

5.11.3.6 DO-254 Appendix B considerations

When developing a hardware DAL A or B custom device, ED-80/DO-254 Appendix B is applicable.

Code coverage analysis that is recognised as part of elemental analysis (refer to Section 5.7 of this document) might not be possible for the COTS IP part of the design. However, ED-80/DO-254 Appendix B offers other acceptable methods, including safety-specific analysis. The following objective further clarifies the expectations when using safety-specific analysis.

Objective IP-7

For COTS IP used in DAL A or DAL B hardware, the applicant should satisfy ED-80/DO-254 Appendix B.

The applicant may choose safety-specific analysis methods to satisfy Appendix B on the COTS IP function and its integration within the custom device functions. This safety-specific analysis should identify the safety-sensitive portions of the COTS IP and the potential for design errors in the COTS IP that could affect the hardware DAL A and DAL B functions in the custom device or system.

For unmitigated aspects of the safety-sensitive portions of the IP, the safety-specific analysis should determine which additional requirements, design features, and verification activities are required for the safe operation of the COTS IP in the custom device.

Any additional requirements, design features and/or verification activities that result from the analysis should be fed back to the appropriate process.

6. USE OF COMMERCIAL OFF-THE-SHELF DEVICES

Applicants are increasingly using COTS electronic devices in aircraft/engines/propellers/airborne systems, which may have safety implications for the aircraft, engines/propellers, or systems.

Section 6 addresses the use of COTS devices through objectives that support the demonstration of compliance with the applicable airworthiness regulations for hardware aspects of airborne systems and equipment certification when using complex COTS devices. Section 6.2 ‘Applicability to COTS devices’ enables applicants to identify the COTS devices that are within the scope of Section 6.

Note: The term ‘COTS device’ used in this document applies to a semiconductor product that is fully encapsulated in a package. This term does not apply to circuit board assemblies (CBAs).

6.1 Background

COTS devices continue to increase in complexity and are highly configurable. COTS devices provide ‘off-the-shelf’ already developed functions, some of which are highly complex. Their development and production processes undergo a semiconductor industry qualification based on their intended market (consumer, automotive, telecom, etc.). Their usage by the aerospace industry provides additional integration and higher performance capabilities than were possible in the past.

The design data for these COTS devices is usually not available to the COTS user. Since these devices are generally not developed for airborne system purposes, assurance has not been demonstrated that the rigour of a COTS manufacturer’s development process is commensurate with the aviation safety risks.

ED-80/DO-254 introduces a basis for the development assurance for the use of COTS devices in Section 11.2 ‘COTS components usage’. This section states that ‘the use of COTS components will be verified through the overall design process, including the supporting processes’.

Since ED-80/DO-254 was released in the year 2000, the number of functions embedded and integrated in a single COTS device has significantly increased. Functions which were previously split into various components, making the interface between those components accessible for verification, are now embedded within a single chip. While there are clearly some benefits of integrating more functions within a device, the increased level of integration makes it difficult for the user to verify the different hardware functions in the device due to lack of access to the interfaces between functions. Since these devices are more complex and highly configurable than the older separate devices, the risk is greater

that the COTS device will not achieve the intended function in particular use cases over the required operating conditions.

Furthermore, some additional assurance is needed because design errors may still be discovered after the COTS device is released to the market, or when an applicant extends the use of the device beyond the manufacturer's specifications.

6.2 Applicability to COTS Devices

Section 6 is applicable to digital, hybrid, and mixed-signal COTS devices that contribute to hardware DAL A, B or C functions. For COTS devices contributing to hardware DAL C functions, a limited set of the objectives of this section will apply.

Section 6 is also applicable to FPGA and PLD devices that embed Hard IP (see definition) in their produced/manufactured silicon, but only for the COTS part of the FPGAs/PLDs.

Section 6.4 only applies to COTS devices that are complex, as determined by the following COTS complexity assessment.

6.3 COTS Complexity Assessment

In order to define which COTS devices are complex, the following high-level criteria should be used, considering all functions of the device, including any functions intended to be unused:

A COTS device is complex when the device:

1. has multiple functional elements that can interact with each other; and
2. offers a significant number of functional modes; and
3. offers configurability of the functions, allowing different data/signal flows and different resource sharing within the device.

Or when the device:

4. contains advanced data processing, advanced switching, or multiple processing elements (e.g. multicore processors, graphics processing, networking, complex bus switching, interconnect fabrics with multiple masters, etc.).

For complex COTS devices, it is impractical to completely verify all possible configurations of the device, and it is difficult to identify all potential failures.

Objective COTS-1

The applicant should assess the complexity of the COTS devices used in the design according to the high-level criteria of Section 6.3, and document the list of relevant devices (see Note 1), including the classification rationale, in the PHAC or any related hardware planning document.

Note 1: The applicant is not expected to assess the complete bill of material to satisfy the above objective, but only those devices that are relevant for the classification, including devices that are at the boundary between simple and complex. The resulting classification (simple or complex) for those devices that are at the boundary and those that are definitely complex should be documented.

Note 2: A classification rationale is required for those devices that are at the boundary (meeting a part of the high-level criteria) and are classified as simple.

Some examples of classification are provided in the GM Appendix for illustration.

6.4 Development Assurance for Use of Complex COTS

ED-80/DO-254 Section 11.2.1 identifies some electronic component management process (ECMP) items when using a COTS device. ED-80/DO-254 Section 11.2.2 and Section 6.1 of this document identify some concerns with using a COTS device. The following objectives acknowledge and supplement ED-80/DO-254 Section 11.2 in clarifying how to gain certification credit when using complex COTS devices.

6.4.1 Electronic Component Management Process (ECMP)

As stated in ED-80/DO-254 Section 11.2, 'the use of an electronic component management process, in conjunction with the design process, provides the basis for COTS components usage.'

Objective COTS-2

The applicant should ensure that an electronic component management process (ECMP) exists to address the selection, qualification, and configuration management of COTS devices. The ECMP should also address the access to component data such as the user manual, the datasheet, errata, installation manual, and access to information on changes made by the component manufacturer.

As part of the ECMP, for devices contributing to hardware DAL A or B functions, the process for selecting a complex COTS device should consider the maturity of the COTS device and, where risks are identified, they should be appropriately mitigated.

Note: Recognised industry standards describing the principles of electronic component management may be used to support the development of the ECMP. See Appendix B.

6.4.1.1 Using a Device outside Ranges of Values Specified in its Datasheet

The device reliability is established by the device manufacturer through the device qualification process (see definition of 'qualification of a device' in the glossary). ED-80/DO-254 Section 11.2.1 Item 6 mentions that a device is selected based on the technical suitability of the device for the intended application.

In some cases, the applicant may need to use the device outside the specified operating conditions guaranteed by the device manufacturer. ED-80/DO-254 Section 11.2.1 Item 4 and Item 6 should be addressed when the device is used outside its guaranteed specification. The following objective describes what to achieve when using a device outside the ranges of values specified in its datasheet.

Objective COTS-3

When the complex COTS device is used outside the limits of the device manufacturer's specification (such as the recommended operating limits), the applicant should establish the reliability and the technical suitability of the device in the intended application.

6.4.1.2 Considerations when the COTS Device has Embedded Microcode

COTS devices may need microcode to execute some hardware functions. When those functions are used by the applicant, there is a risk if the microcode has not been verified by the device manufacturer during the COTS device qualification, or if the microcode is proposed to be modified by the applicant.

If the microcode is delivered by the device manufacturer, is controlled by the device manufacturer's configuration management system, and is qualified together with the device by the device manufacturer, it is accepted that the microcode is part of the qualified COTS device. If the microcode is not qualified by the device manufacturer or if it is modified by the applicant, the microcode cannot be considered to be part of the qualified COTS device.

Objective COTS-4

If the microcode is not qualified by the device manufacturer or if it is modified by the applicant, the applicant should ensure that a means of compliance for this microcode integrated within the COTS device is proposed by the appropriate process, and is commensurate with the usage of the COTS device.

Note: The PHAC (or any other related planning document) should document the existence of the microcode and refer to the process (hardware, software, system) where it is addressed.

6.4.2 COTS Device Malfunctions

Some COTS devices may contain errors that may or may not have been detected by the device manufacturer.

Objective COTS-5

The applicant should assess the errata of the COTS device that are relevant to the use of the device in the intended application, and identify and verify the means of mitigation for those errata. If the mitigation means is not implemented in hardware, the mitigation means should be fed back to and verified by the appropriate process.

Note: The above objective refers to any mitigation means (such as hardware, software, system, or other means).

Objective COTS-6

The applicant should identify the failure modes of the used functions of the device and the possible associated common modes, and feed both of these back to the system safety assessment process.

6.4.3 Usage of COTS Devices

This section focuses on the usage of complex COTS devices, while Section 7 covers the overall circuit board assembly development process. This Section 6.4.3 refers to the term 'intended function of the hardware', which is considered to be defined through the CBA development process.

Complex COTS devices can have multiple functions and many configurations of those functions. The configuration of a device should be managed in order to provide the ability to consistently apply the required configuration settings, to replicate the configuration on another item, and to modify the configuration in a controlled manner, when modification is necessary.

The configuration of the device addresses at least the following topics:

— Used functions (e.g. identification of each function, configuration characteristics, modes of operation),

— Unused functions and the means (internal/external) used to deactivate them,

— Means to control any inadvertent activation of the unused functions, or inadvertent deactivation of the used functions,

— Means to manage device resets,

— Power-on configuration,

— Clocking configuration (e.g. identification of the different clock domains), and

— Operating conditions (e.g. clock frequency, power supply level, temperature, etc.).

Objective COTS-7

The applicant should ensure that the usage of the COTS device has been defined and verified according to the intended function of the hardware. This also includes the hardware–software interface and the hardware to (other) hardware interface.

When a COTS device is used in a hardware DAL A or B function, the applicant should show that unused functions of the COTS device do not compromise the integrity and availability of the COTS device's used functions.

Note 1: For unused functions of the COTS device, it is recommended that an effective deactivation means is used and verified, when available.

Note 2: Verification should be performed at an appropriate level (hardware, software, equipment).

ED-80/DO-254 Section 10.3.2.2.4 introduces hardware/software (HW/SW) interface data, which can be used as a reference to define the software interface data of the COTS device.

Some additional consideration should be given to the critical configuration settings. Those are defined as the settings that are deemed necessary by the applicant for the proper usage of the hardware, which, if inadvertently altered, could change the behaviour of the COTS device, causing it to no longer fulfil the hardware intended function.

Objective COTS-8

If the complex COTS device contributes to DAL A or B functions, the applicant should develop and verify a means that ensures an appropriate mitigation is specified in the event of any inadvertent alteration of the 'critical configuration settings' of the COTS device.

Note: The mitigation means might be defined at the hardware, software, or system level, or a combination of these. The mitigation means may also be defined by the safety assessment process.

7 Development Assurance of Circuit Board Assemblies (CBAs)

This section provides guidance for the development assurance of CBAs (a board or a collection of boards).

7.1 Applicability

Section 7 is applicable to CBAs that contribute to hardware DAL A, B or C functions.

7.2 Development Assurance of Circuit Board Assemblies (CBAs)

While it is already a common practice for applicants to have an internal process to address the development of CBAs, it is necessary to clarify the expectations for development assurance, including the flow-down of the equipment/system requirements to the hardware. For consolidation of the development and/or the use of complex devices, it is essential to ensure consistency in the overall development assurance approach for the hardware domain. Moreover, definition of the CBA function is also necessary to enable the allocation of requirements and their flow-down to the complex devices.

Objective CBA-1

The applicant should have a process to address the development of CBAs that contain complex custom devices or complex COTS devices, in order to ensure that the CBA performs its intended function. The process should include requirements capture, validation, verification, and configuration management activities, and ensure an appropriate flow-down of requirements. See Appendix B for additional information.

Note: The applicant's process to address the development of the CBA may be defined together with the equipment process, when relevant.

8 RELATED REGULATORY, ADVISORY AND INDUSTRY MATERIAL

(a) Related EASA Certification Specifications (CSs)

(1) CS-23, *Certification Specifications and Acceptable Means of Compliance for Normal, Utility, Aerobatic, and Commuter Category Aeroplanes*

(2) CS-25, *Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes*

(3) CS-27, *Certification Specifications and Acceptable Means of Compliance for Small Rotorcraft*

(4) CS-29, *Certification Specifications and Acceptable Means of Compliance for Large Rotorcraft*

(5) CS-E, *Certification Specifications and Acceptable Means of Compliance for Engines, and AMC 20-3B, Certification of Engines Equipped with Electronic Engine Control Systems*

(6) CS-P, *Certification Specifications for Propellers, and AMC 20-1A, Certification of Aircraft Propulsion Systems Equipped with Electronic Control Systems*

(7) CS-ETSO, *Certification Specifications for European Technical Standard Orders*

(8) CS-APU, *Certification Specifications for Auxiliary Power Units*; and AMC 20-2B, *Certification of Essential APU Equipped with Electronic Controls*

(b) FAA Advisory Circulars (ACs)

(1) AC 20-152, *Development Assurance for Airborne Electronic Hardware*

(2) *AC 00-72, Best Practices for Airborne Electronic Hardware Design Assurance Using EUROCAE ED-80( ) and RTCA DO-254( )*

(3) AC 23.1309-1, *System Safety Analysis and Assessment for Part 23 Airplanes*

(4) AC 25.1309-1, *System Design and Analysis*

(5) AC 27-1309, *Equipment, Systems, and Installations (included in AC 27-1, Certification of Normal Category Rotorcraft*)

(6) AC 29-1309, *Equipment, Systems, and Installations (included in AC 29-2, Certification of Transport Category Rotorcraft*)

(c) Industry Documents

(1) EUROCAE ED-79A, *Guidelines for Development of Civil Aircraft and Systems,* dated December 2010

(2) EUROCAE ED-80, *Design Assurance Guidance for Airborne Electronic Hardware,* dated April 2000

(3) RTCA DO-254, *Design Assurance Guidance for Airborne Electronic Hardware,* dated 19 April 2000

(4) SAE International Aerospace Recommended Practice (ARP) 4754A, *Guidelines for Development of Civil Aircraft and Systems,* dated 21 December 2010

(5) SAE International Aerospace Recommended Practice (ARP) 4761, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment,* dated December 1996

9 AVAILABILITY OF DOCUMENTS

(a) EASA Certification Specifications (CSs) and Acceptable Means of Compliance (AMC) may be downloaded from the EASA website: www.easa.europa.eu

(b) FAA Advisory Circulars (ACs) may be downloaded from the FAA website: www.faa.gov

(c) EUROCAE documents may be purchased from:

European Organisation for Civil Aviation Equipment
102 rue Etienne Dolet, 92240 Malakoff, France
Telephone: +33 1 40 92 79 30, Fax: +33 1 46 55 62 65
(Email: eurocae@eurocae.net, website: www.eurocae.net)

(d) RTCA documents may be purchased from:

RTCA, Inc.
1150 18th Street NW, Suite 910, Washington DC 20036, USA
(Email: info@rtca.org, website: www.rtca.org)

APPENDIX A — GLOSSARY

Abnormal conditions: conditions that are inconsistent with specified normal operating conditions.

Airborne electronic hardware: an electronic 'hardware item' (see ED-80/DO-254 for definition of 'hardware Item'), intended to be installed in airborne equipment/systems.

Batch: a manufacturing lot of a semiconductor device that is reproduced using the same semiconductor fabrication process.

Commercial off-the-shelf (COTS) device: a device, integrated circuit or multi-chip module developed by a supplier for a wide range of customers (not restricted to airborne systems), whose design and configuration is controlled by the supplier or an industry specification. A COTS device can encompass digital, analogue, or mixed-signal technology. COTS electronic components are generally developed by the semiconductor industry for the commercial market, not particular to the airborne domain. These devices have widespread commercial use and are developed according to the semiconductor manufacturer's proprietary development processes.

COTS device usage: definition of the used and unused functions that are implemented in the device. This is further defined as an exhaustive list of conditions/constraints (such as configuration settings, usage rules, protocol, timing constraints, input–output (I–O) interface, and addressing schemes) associated with the performance characteristics of the used COTS functions. Respecting the defined usage of the COTS will ensure the expected performance of the device for a given set of constraints.

Commercial off-the-shelf intellectual property (COTS IP): intellectual property (IP) refers to design functions (design modules or functional blocks, including IP libraries) used to design and implement a part of or a complete custom device such as a PLD, FPGA, or an ASIC. Intellectual property is considered

to be 'COTS IP' when it is a commercially available function used by a number of different users in a variety of applications and installations. In this document, the terminology 'a/the COTS IP' refers to a piece of hardware that is COTS IP per this definition. COTS IP is available in various source formats:

(a) **Soft IP**

Soft IP is COTS IP defined as register transfer level (RTL) code, captured in an HDL such as Verilog or VHDL, that may be readable or encrypted. It is instantiated by the IP user within the custom device HDL code or by selecting the COTS IP function in a library. Soft IP will be synthesised, placed and routed in the AEH custom device.

In this document, the terminology 'a/the Soft IP' refers to a piece of hardware that is Soft IP per this definition.

(b) **Firm IP**

Firm IP is COTS IP defined as a technology-dependent netlist. It is instantiated within the custom device netlist (inserted by the user, called from a library, or selected by the user as a library function). Firm IP will be placed and routed in the AEH custom device.

In this document, the terminology 'a/the Firm IP' refers to a piece of hardware that is firm IP per this definition.

(c) **Hard IP**

Hard IP is COTS IP defined as a physical layout (stream, polygon, GDSII format, etc.).

Hard IP is instantiated by the IP user during the physical design layout stage; alternatively, Hard IP is embedded into the silicon of the FPGA/PLD by the FPGA provider/device manufacturer.

In this document, the terminology 'a/the Hard IP' refers to a piece of hardware that is Hard IP per this definition.

Complex COTS device maturity: a complex device is mature when the risk of an unintended function or misbehaviour is low. The risk of anomalous behaviour decreases as a device is widely used and device errata are documented and communicated to the users of the device.

Critical configuration settings: those configuration settings that the applicant has determined to be necessary for the proper usage of the hardware, which, if inadvertently altered, could change the behaviour of the COTS device, causing it to no longer fulfil its intended function.

Development assurance for use of COTS device: all the planned and systematic activities conducted to provide adequate confidence and evidence that the complex COTS device safely performs its intended function under its operating conditions.

Hardware design assurance level of a function: refer to ED-80/DO-254 Table 2-1 for the definition of DAL A, B, C and D functions.

Hybrid device: an integrated circuit combining different semiconductor dies and passive components on a substrate.

IP libraries: 'IP libraries' used in the COTS IP definition refers to all submodules, sub-blocks, or other design subfunctions that are formally/commercially made available by a COTS IP provider and intended for integration within a COTS IP by the COTS IP user. However, Macro Cells for FPGAs or Standard Cells

for ASICs are not considered to be IP libraries, hence they are not related to the COTS IP topic referred to in this document.

Microcode: this term often refers to a hardware-level set of instructions. It is typically stored in the COTS device's high-speed memory, and microcode instructions are generally translated into sequences of detailed circuit-level operations. Microcode may be used in general-purpose microprocessors, microcontrollers, digital-signal processors, channel controllers, disk controllers, network interface controllers, network processors, graphics processing units, and other hardware. A Basic Input/Output System (BIOS) is an example of microcode, which is used to initialise microprocessor input and output process operations.

Mixed-signal device: a device that combines digital and analogue technologies.

Note: a note in this document is supporting information used to provide explanatory material, emphasise a point, or draw attention to related items which are not entirely within context.

Objective: an objective in this document is a requirement for development assurance that should be met to demonstrate compliance with the applicable airworthiness requirements.

Previously developed hardware (PDH): a custom-developed hardware device that has been installed in an airborne system or equipment either approved through EASA type certification (TC/STC) or authorised through ETSOA.

Qualification of a device: SAE EIA-STD-4899 defines component qualification as 'The process used to demonstrate that the component is capable of meeting its application specification for all the required conditions and environments.' Component qualification results in a 'qualified device.' Note that the use of 'qualification' is not intended to refer to ED-14/DO-160 environmental qualification testing.

APPENDIX B — GUIDANCE MATERIAL TO AMC 20-152A

B.1 Purpose

This document provides additional clarifications, explanatory text, or illustrations that could be helpful when addressing some of the objectives of AMC 20-152A. This document is not intended to cover each section of AMC 20-152A.

This AMC is a means of assisting applicants, design approval holders (DAH), and developers of airborne systems and equipment containing electronic hardware intended to be installed on type-certified aircraft, engines, and propellers, or to be used in European technical standard order (ETSO) articles.

B.2 Guidance Material

B.2.1 Custom Devices

This guidance material provides complementary information to AMC 20-152A, Custom Device Development, Section 5. Applicants may use this guidance material when developing custom devices.

B.2.1.1 Clarifications to ED-80/DO-254 Appendix A for the Top-Level Drawing

B.2.1.1.1 Hardware Environment Configuration Index (HECI)

The purpose of the HECI is to aid the reproduction of the hardware life cycle environment for hardware regeneration, reverification, or hardware modification. The HECI may be included or referenced in the Hardware Configuration Index (HCI). The HECI should identify:

1. the life-cycle environment hardware (e.g. computer or workstation) and operating system (OS) when relevant;
2. hardware design tools;
3. the test environment and validation/verification tools; and
4. qualified tools and qualification data.

B.2.1.1.2 Hardware Configuration Index (HCI)

The purpose of the HCI is to identify the configuration of the hardware item(s). The HCI should include:

1. ASIC/PLD part number;
2. Media used to produce the physical component (e.g. the PLD/FPGA programming file or ASIC netlist/GDSII);
3. Identification of each source code component, including individual source files, constraints, scripts and versions;
4. Identification of any previously developed hardware;
5. Identification of any COTS Intellectual Property;
6. Identification of the test bench source code and scripts, including the versions;

7. Hardware life-cycle data items and their versions as defined in ED-80/DO-254 Table A-1;

8. Archive and release media (e.g. for the source data);

9. Instructions for building a PLD programming file or ASIC netlist;

10. Instructions for loading the bitstream file into the target PLD or FPGA hardware;

11. Reference to the HECI; and

12. Data integrity checks for the PLD programming file (n/a for ASICs).

B.2.1.2 Additional Information for Objective CD-1 on Simple/Complex Classification

Based on the definition of simple hardware in ED-80/DO-254, a custom device with complex functions that is exhaustively verified with the help of a formal analysis or a verification tool could be theoretically classified as simple. AMC 20-152A clarifies that the classification as simple or complex is based on the design content of the device, regardless of the proposed verification method. Therefore, such a device would be classified as complex following the criteria of AMC 20-152A.

Here below is an illustration of the types of criteria commonly used by industry, and it is not an exhaustive list. The applicant is responsible for determining the criteria that are applicable to its own development process:

— Simplicity of the functions, simplicity of data/signal processing or transfer functions;

— Number of functions, number of interfaces;

— Independence of functions/blocks/stages.

Specific to digital designs:

— Synchronous or asynchronous design;

— Number of independent clocks, number of state machines and their independence, number of states, and state transitions per state machine.

B.2.1.3 Additional Information for Objective CD-2 on Development Assurance of Simple Custom Devices

A simple device is defined and designed to implement specific hardware functions. Due to the simplicity of the device, the life-cycle data is reduced.

The functional performance of the device has to be ensured by verification means in order to demonstrate that the simple device adequately and completely performs its intended functions within the operating conditions without any anomalies.

The functions of a simple device may be defined through a requirement capture process, or may be as part of the definition of functions for the overall hardware.

Operating conditions, in addition to the environmental conditions, encompass all the functional modes for the device configurations and all the associated sets of inputs as

determined to completely cover the functions of the device in its intended hardware implementation.

B.2.1.4 Additional Information for Objective CD-7 on Verification of Implementation Timing Performance

Objective CD-7 specifies that applicants should verify the timing performance of the design, accounting for the temperature and power supply variations applied to the device and the semiconductor device fabrication process variations.

There are certain variations in the conditions in which the device performs its function that may impact the timing behaviour of the device. If not all the cases are verified, the timing aspects might result in device malfunctions under certain conditions.

The following examples identify constraints that may impact the timing behaviour of a device, and information to help assess them:

— The temperature range is a design constraint input from the equipment environment or taken from the device limitation/characterisation limits. Two different temperatures need to be managed:

  — junction temperatures: the static timing analysis (STA) tools and technology limitations are based on the junction temperatures; and
  — external temperature: application constraints are related to the external temperature of the device.

  Conversions between these two constraints have to be carefully managed when analysis is performed.

— For voltage ranges, there are also two characteristics to take into account: constraints from the environment (the board, voltage generator accuracy) and constraints from the chosen device. Note that the voltage aspect is unambiguous.

— Device process variation is related to the chosen device, and the device manufacturer often characterises the technology variations within the library.

To verify the timing performance of the design accounting for the temperature and power supply variations applied to the device and the semiconductor device fabrication process variations, an analysis is expected to be performed on all the corner cases to measure the impact of such constraints (temperature, voltage, and process) in terms of timing that could also affect the frequency at which the device can operate.

Static timing analysis (STA) can be used to conduct such an analysis. The source of each STA constraint (delays and frequency constraints) has to be identified. In addition, the timing parameters to be considered for launching an STA include:

— the input frequency: an external constraint with different characteristics (e.g. accuracy, duty cycle); and

— input/output delays (e.g. setup, hold, skew).

STA provides timing results that highlight setup and hold violations, but does not analyse delays longer than a clock period (multi-cycle paths, pulse width generation, etc.). Additional verification may be needed to address those timing aspects not covered by STA.

B.2.1.5 Additional Information for Objective CD-9 on Recognition of HDL Code Coverage Method

For Objective CD-9, the applicant determines the code coverage criteria that support the code coverage method. The applicant should define criteria covering the hardware description language (HDL) code elements that are used in the design and exercising the various cases of HDL code. The following items suggest the type of criteria that could be used to cover the HDL logic. These criteria are still to be translated into the specific metrics proposed by the chosen code coverage tools:

1. Every statement has been reached;
2. All the possible branch directions have been exercised;
3. All the conditions expressed in a statement or for taking a branch have been exercised;
4. Every state of a finite state machine (FSM) and every state transition has been exercised.

B.2.1.6 Additional Information for Objective CD-10 on Tool Assessment and Qualification

As described in Objective CD-10, in a context where the applicant plans to use a verification tool for a DAL A or B custom device, or a design tool for a DAL A, B or C custom device, the applicant can choose to provide confidence in the use of the tool through an independent assessment of the tool outputs.

Example:

Custom device development using the following tools:

— Design tools: synthesis tools, layout tools, programming file generation tools;

— Verification tools: simulation tools, STA tools.

Confidence in design tools can be gained through the fact that the outputs from the design tools are independently verified by post-layout simulation and physical tests during requirements-based testing. No further tool assessment is needed.

Confidence in verification tools can also be gained through independent assessment. For instance, physical tests, either by rerunning part of the simulation test sequences or retesting the requirements, allow confirmation of the results generated via the simulation test cases or procedures. The following criteria can be used to determine whether the tool can be independently assessed using this approach:

— a significant and representative set of custom device requirements is covered by both simulation and physical tests; and

— the results for the simulation and the physical test of the same requirement are equivalent.

Another example of independent assessment can be to rerun simulation tests on a dissimilar simulation tool and compare the results obtained from each simulation tool to ensure their equivalence.

Generally, independent assessment of the tool outputs is the preferred method for tool assessment.

When the applicant largely covers custom device requirements through physical tests, it reinforces the confidence in the tools.

B.2.1.7 Additional Information for Objective CD-11 on Tool Assessment and Qualification

When the applicant intends to present tool history to claim credit for tool assessment, Objective CD-11 expects the applicant to provide sufficient data and justification to substantiate the relevance and credibility of the tool history.

In general, the tool history is applicable to a specific version of the tool, because it is difficult to determine whether different versions or releases of the same tool constitute the same tool.

If using a different version of the tool compared with the one that has a relevant tool history, the applicant would then be expected to analyse the differences between the tool versions to ensure that the tool history is relevant to the version of the tool used.

A list of characteristics/criteria that can be part of the relevant history data of the tool includes:

— The similarity of the tool operational environment in which the tool service history data was collected to the one used by the applicant;

— The stability/maturity of the tool linked to the change history of the tool;

— The service experience of the custom devices developed using the tool;

— The tool has a good reputation and is well supported/maintained by the tool supplier;

— The number of tool users is significant;

— The tool has already been used in the applicant’s company on certified developments without raising any major concerns;

— The list of errata is available and shows that these errata do not impact the use of the tool in the development of the particular custom device.

If the tool has not been used by the applicant’s company in the frame of another custom device development, it is preferable not to use the tool history for assessing the tool, and instead to conduct an independent assessment approach.

B.2.1.8 Use of COTS IP in Custom Device Development

This guidance material provides complementary information to AMC 20-152A, Custom Device Development, Section 5.11. Applicants may use this guidance material when using commercial off-the-shelf intellectual property (COTS IP) in a custom device.

B.2.1.8.1 Clarification of Objective IP-2 on Assessment of the COTS IP Provider and COTS IP Data

B.2.1.8.1.1 Assessment of Service Experience of COTS IP

The COTS IP should have been used in numerous application cases, and the IP errata should be available and stable. The applicant will assess and document the relevance of the service experience from data collected from previous or current usage of the component, and consider the equivalence of the usage domain to ensure a certain level of maturity of the IP for the user's application. This data might be obtained with the support of the COTS IP provider, but it might be difficult to demonstrate relevant service experience especially for Soft and Firm IP. Some additional development assurance needs to be defined to address the risk of insufficient or unrelated service experience.

B.2.1.8.1.2 Assessment of the COTS IP Provider and COTS IP data

The following paragraph provides some high-level examples of the assessment of different source formats of COTS-IP; they are included for illustration only.

The following are two typical cases of insufficient coverage when assessing COTS IP with the Objective IP-2 criteria:

— A Soft IP is proposed by an experienced provider, but with unknown COTS IP service experience. The COTS IP provider offers limited support for the COTS IP, which may be part of an FPGA provider's catalogue.

— A new Soft IP is proposed by a new company with some documentation. The COTS IP provider does not offer any support. There is insufficient evidence of complete verification to make it trustworthy. The applicant may be the first user.

An example of a COTS IP assessment with the Objective IP-2 criteria that helps to define the appropriate development assurance activity on the COTS IP is as follows:

— A communication Soft IP is proposed by an experienced provider. The COTS IP has existed for more than 2 years and has been used in many applications by many customers. The version of the IP is stable, and errata are available. The COTS IP is also available as COTS hardware in an FPGA family. The Soft IP is distributed with a set of design constraints and the associated implementation results are usable for various sets of technology targets (which could be PLDs/FPGAs or ASICs). The test procedures used by the COTS IP provider are not available, but a report providing results of those tests is delivered. Moreover, compliance with the communication standard has been established by the COTS IP provider through an external set of procedures and reports that are also available. This assessment and availability of external sets of procedures support the applicant in defining an acceptable verification strategy.

B.2.1.8.2 Clarification of Objective IP-4 on Verification Strategy for the COTS IP Function

The COTS IP assessment should determine the extent to which the COTS IP provider verified their IP. This verification could vary from IP with no/little verification performed to IP that is

delivered with detailed life-cycle data. The amount of verification performed by the IP provider will drive the applicant's verification strategy.

Taken together, the verification performed by the COTS IP provider and the verification performed by the applicant in the integrated device shows complete verification of all the used functions of the COTS IP. Thus, if there is little verification data from the COTS IP provider, the applicant will need to do more verification activities to verify the functionality of the IP. If extensive data is provided, then the applicant may only need to show the proper implementation and integration of the IP within the custom device. This activity may be supported by the use of the COTS IP provider's test cases, or by proven test vectors for a COTS IP performing a standardised interface function.

The verification strategy describes the verification data delivered with the COTS IP, as well as the verification data to be developed by the applicant. The verification activities proposed by the applicant should address any missing items from the data delivered with the COTS IP and ensure the proper implementation and integration of the IP within the custom device.

B.2.1.8.3 Clarification of Objective IP-6 on the Requirements for the COTS IP Function and Validation

Depending on the need for requirements-based testing as a part of the chosen verification strategy for the COTS IP, the level of detail and the granularity of the AEH custom device requirements may need to be extended to particularly address the COTS IP function and further design steps of the COTS IP.

When custom device requirements need to be refined to capture the COTS IP functions per the verification strategy, it will be performed using all the documentation and design data available. The requirement capture process will encompass all the IP functions, including the means to deactivate any unused functions.

The following aspects could be captured as derived requirements:

1. Error or failure mode detection and correction behaviour performed by the IP;
2. Design constraints that control the interaction of the IP with the rest of the design of the custom device;
3. Configuration parameters or settings used to alter or limit the functions provided by the IP;
4. Controlling or deactivating unused features or characteristics of the design;
5. Design constraints to properly perform the implementation and mitigate the use of the IP features, modes, and design characteristics with known failures or limitations; for DAL A and DAL B, the behaviour of the IP during robustness conditions, boundary conditions, failure conditions, and abnormal inputs and conditions;
6. The mitigation of known errata that would adversely affect the correct operation of the function.

When the applicant chooses a verification strategy that solely relies on requirements-based testing, a complete requirement capture of the COTS IP following ED-80/DO-254 is necessary. It is recommended that this activity should begin with a thorough understanding of the COTS IP architecture, and both its used and unused functions. The applicant could propose a method in the Plan for Hardware Aspects of Certification (PHAC) for determining and assessing the completeness of the requirements capture process, in order to guarantee that the requirements cover all the used functions and the deactivation means for the unused ones (for non-interference with the used functions).

B.2.2 COTS DEVICES

These practices provide complementary information to AMC 20-152A, COTS Devices, Section 6. Applicants may use this guidance material when using COTS devices.

B.2.2.1 Additional Information for COTS Section 6.3 and Objective COTS-1 on COTS Complexity Assessment

The applicant should assess the complexity of the COTS devices used in the design and produce the list of all the complex COTS devices. This list of complex COTS devices is expected to be known at an early stage and documented in the PHAC, or delivered together with the PHAC. It is understood that the list may evolve during development, and the list should be made available to the regulatory authority once the parts selection process is completed.

As stated in AMC 20-152A, the applicant is not expected to assess the complete bill of material to meet Objective COTS-1, but only those devices that are relevant for the classification, including devices that are on the boundary between simple and complex. The assessment and the resulting classification (simple or complex) for those devices that are on the boundary and classified as simple would be documented in a life-cycle data item that is referred to in the PHAC and HAS.

The following examples provide some characteristics of complex and simple devices for illustration, and on which the complexity assessment is performed by applying the generic criteria identified in Section 6.3. These examples are provided for illustration only. Other combinations of characteristics will occur in actual projects.

EXAMPLES OF COTS DEVICES AND THEIR ASSOCIATED CHARACTERISTICS	COMPLEXITY ASSESSMENT
An example of a single-core processor/microcontroller with: — Multiple and complex functional elements that interact with each other: PCIe interface, Ethernet, Serial RapidIO, a single core processor; — A significant number of functional modes where each interface has several selectable channels/modes of operation;	Complex

— Configurable functions allowing different data/signal flows and different resource sharing within the device so the different data paths within the device are fully configurable in a dynamic manner.	
An example of a single-core processor/microcontroller with: — A single advanced, reduced instruction machine core processor; — Inter-processor communication that uses a simple mailbox protocol; — A programmable real-time unit (PRU) subsystem that contains 2 RISC processors and complex access to many peripherals; — A PRU that is highly programmable with 200 registers, and each of the peripherals is also configurable. The PRU is complex.	Complex
An example of a single-core processor/microcontroller with: — Several functional elements that interact with the single core processor but not with each other: PCI interface, SPI, I2C, JTAG, 1 core processor; — A significant number of functional modes where the interface has few modes of operation; — Limited configurable functions allowing one major data path using a limited number of discrete signals on SPI or I2C. There is limited and fixed resource sharing in the device.	Simple
An example of a 32-bit reduced instruction set computing (RISC) microcontroller with: — Internal buses that are all simple master–slave protocol, — A processor that has dedicated resources, — No interconnect fabric, no multiple masters, — A single point of access to all the peripherals, — Independent time processor units (TPUs) with microcode that are accessed through the slave peripheral control unit.	Simple
An example of a stand-alone controlled area network (CAN) controller with a serial peripheral interface (SPI) with: — A single controller with one SPI bus.	Simple
An example of a communications infrastructure digital signal processor (DSP) with: — A single DSP, — An interconnect between DSP and peripherals that is an interconnect switch with multiple masters, multiple slaves and is highly configurable,	Complex

— Multiple internal bridges between the peripherals and the interconnect switch and programmable priorities.	
An example of an analogue-to-digital converter with: — An 8-channel/16-channel, software selectable, 24-bit ADC.	Simple
An example of a digital SPI temperature sensor with: — An analogue temperature sensor, — Conversion to digital, — An SPI output.	Simple
An example of an FPGA component with some Hard IP embedded in silicon with: — An FPGA fabric (outside the COTS scope), — Embedded RAM/ROM memories, — Embedded FIFOS, — A PCI port, — A/D and D/A converters, — 16×16 configurable multiplier blocks.	Simple
An example of an FPGA component with Hard IP embedded in silicon with: — An FPGA fabric (outside the COTS scope), — Embedded RAM/ROM memories, — Embedded FIFOS, — A PCIe port, — A Processor Core, — A coherency fabric/interconnect, — A/D and D/A converters.	Complex

B.2.2.2 Additional Information for COTS Section 6.4.1 on the Electronic Component Management Process (ECMP)

B.2.2.2.1 Clarification of Objective COTS-2 on the Electronic Component Management Process (ECMP)

IEC 62239 and SAE EIA-STD-4899 define items and processes that support the establishment of industry electronic component management plans which would be considered as industry recommended standards to support the topics mentioned in Objective COTS-2.

Generally, the electronic component management process (ECMP) describes a standard process that is reused and reapplied from certification project to certification project. This approach is understood to ease the certification process.

Regarding the assessment of maturity:

When selecting a device, the applicant assesses the maturity of the device and analyses whether its maturity is sufficient to ensure that the potential for design errors has been reduced. This assessment of maturity could encompass some of the following items:

— The time of the device in service,

— Widespread use in service: an indication of widespread use could be given (multiple applications, a large minimum number of chips sold, etc.),

— Product service experience per DO-254/ED-80 Section 11.3 from any previous or current usage of the device,

— The maturity of the intellectual property embedded into the device,

— A decreasing rate of new errata being raised.

There are no quantitative targets expressed but there is a necessity for an engineering assessment of the device's maturity, starting with the selection process.

B.2.2.2.2 Clarification of Objective COTS-3 on Using a Device outside the Ranges of Values Specified in its Datasheet

Establishing the reliability of a complex COTS device that is used outside its specification (its recommended operating limits), as determined by the device manufacturer, is considered to be difficult and might introduce risks that should be mitigated.

One process to qualify the device, called an 'uprating' process, could be applied to verify the appropriate operation of the device itself and to guarantee that performance is achieved in the target environment in all operating conditions over the lifetime of the equipment. This uprating process focuses on the device itself and takes into account the different variations in technology (variation in performance over different batches/over different dies). This uprating process evaluates the performance of the device itself, so it is different from ED-14/DO-160 environmental qualification of equipment.

Thermal uprating is addressed in IEC/TR 62240-1. 'It provides information to select semiconductor devices, to assess their capability to operate, and to assure their intended

quality in the wider temperature range. It also reports the need for documentation of such usage.'

It is understood that each case of uprating might follow a different process depending on the 'uprated' characteristics (the frequency, temperature, voltage, etc.) and the performance guaranteed by the device manufacturer's datasheet. For that reason, Objective COTS-3 is separated from Objective COTS-2 and is only to be applied in cases of COTS device uprating.

IEC/TR 62240-1 states the following: 'For each instance of device usage outside the manufacturer's specified temperature range relevant data are documented and stored in a controlled, retrievable format.' This is considered to be a best practice for any uprating case as evidence satisfying Objective COTS-3.

Note: When a simple COTS device is used outside its datasheet values, applying an uprating process would be considered to be a best practice to ensure that the device functions properly within the newly defined and intended environment/usage conditions.

B.2.2.3 Additional Information for Section 6.4.2 'COTS Device Malfunctions'

The applicant needs access to errata information on the device during the entire life cycle of the product (before and after certification). Refer to AMC, Section 6.4.1.

In general, this assessment typically includes the analysis of which errata are, or are not, applicable to the specific installation of the equipment, and for each of the applicable errata:

— The description of the mitigation implemented, and

— The evidence that the implementation of errata mitigations are covered by relevant requirements, design data, and are verified.

The assessment of the errata of a simple COTS device is considered a best practice to remove the safety risks associated with device malfunctions.

While the applicant is expected to document the process applied for errata in the PHAC, the errata and evidence of assessment would typically be captured in other documents that can be referred to in the PHAC and HAS.

B.2.2.4 Additional Information for Objective COTS-6 on COTS Device Malfunctions

It is understood that the task linked with this objective is performed in close coordination with the hardware, software, and system teams.

In order to support the safety analysis process, this objective focuses on the failure effects and not on their root causes. The hardware domain, knowing the detailed usage of the device, starts by identifying the effects of failures of the device on the intended functions. This information will be provided to the system safety process. When necessary, mitigation means will be defined and verified by the appropriate domain or across the hardware, software, and system domains.

While the applicant is expected to document the process to satisfy Objective COTS-6 in the PHAC, the evidence would typically be captured in other documents that can be referred to in the PHAC and ultimately in the HAS.

When a simple COTS device interfaces with software, complying with Objective COTS-6 is considered to be a best practice.

B.2.3 Clarification of Objective CBA-1 on **Circuit Board Assembly Development**

In the aviation domain, the applicant typically has internal processes to develop circuit board assemblies. There is a clear benefit for the applicant (or developer of the airborne system and equipment) in having a process to address the development of a circuit board assembly (a board or a collection of boards) that encompasses the requirements capture, validation, verification, and configuration management activities, and ensures an appropriate requirements flow-down.

It is a common practice for the applicant's internal process to already encompass the above-mentioned activities that satisfy Objective CBA-1. Industry standards ED-80/DO-254 or ED-79A/ARP4754A provide guidance that may be used by applicants seeking further information.

Note 1: The applicant's internal processes might be tailored according to the equipment and hardware complexity if necessary.

Note 2: The organisation of the process life-cycle data is at the discretion of the applicant's internal process.

Note 3: The hardware requirements may be verified at a higher level of integration.

B.2.4 Development of Airborne Electronic Hardware Contributing to Hardware DAL D Functions

For airborne electronic hardware contributing to hardware DAL D functions, the acceptable means of compliance include ED-80/DO-254 or existing Level D hardware development assurance practices that demonstrate that the requirements allocated to the DAL D airborne electronic hardware have been satisfied. Additionally, system-level development assurance practices such as ED-79A/ARP4754A or other means may be used if the applicant can demonstrate at the system level that the requirements allocated to the DAL D airborne electronic hardware have been satisfied.

APPENDIX C — GLOSSARY OF GUIDANCE MATERIAL

This glossary complements the terms defined in AMC 20-152A with terms used only in this GM.

Uprating: A process to assess the capability of a COTS device to meet the performance requirements of the application in which the device is used outside the manufacturer's datasheet ranges (definition adapted from the IEC/TR 62240-1 Thermal uprating definition).

8. The following AMC 20-189 is inserted:

AMC 20-189 The Management of Open Problem Reports (OPRs)

1. PURPOSE

This AMC describes an acceptable means, but not the only means, for showing compliance with the applicable airworthiness regulations for the management of open problem reports (OPRs) in ETSO authorisations and type certification, for the system, software and airborne electronic hardware (AEH) domains. Compliance with this AMC is not mandatory, and an applicant may elect to use an alternative means of compliance. However, the alternative means of compliance must meet the relevant requirements, ensure an equivalent level of safety, and be approved by EASA on a product or ETSO article basis.

2. APPLICABILITY This AMC may be used by applicants, design approval holders, and developers of airborne systems and equipment to be installed on type-certified aircraft, engines, and propellers. This AMC applies to all airborne electronic systems and equipment, including to the software and AEH components contained in those systems, which could cause or contribute to Catastrophic, Hazardous, or Major failure conditions.

3. BACKGROUND

3.1. Each of the system, software and AEH domains relies on problem report (PR) management to ensure the proper management of open problem reports (OPRs) and to help ensure safe products at the time of approval. However, the existing guidance on PR and OPR management is inconsistent and incomplete across domains. Therefore, this AMC provides consistent guidance across these domains for PR management, OPR management, stakeholder responsibilities, reporting, and other aspects of OPR management. This AMC complements but does not alleviate the project-applicable system, software and AEH guidance.

3.2. The technical content of this AMC has been jointly developed with the Federal Aviation Administration (FAA), in order to harmonise as far as practicable.

4. DEFINITIONS

4.1. Terms defined in this AMC

Approval: the term ‘approval’ in this document addresses the approval by EASA of a product or of changes to a product, or authorisation of an ETSO article or of changes to an ETSO article.

Article: refer to Article 1(2)(f) of Regulation (EU) No 748/2012 (‘EASA Part 21’).

Development assurance: all of those planned and systematic actions used to substantiate, with an adequate level of confidence, that errors in requirements, design, and implementation have been identified and corrected such that the system satisfies the applicable certification basis (source: ARP4754A/ED-79A).

Equipment: an item or collection of items with a defined set of requirements.

Error: a mistake in the requirements, design, or implementation with the potential of producing a failure.

Failure: the inability of a system or system component to perform a function within specified limits (source: DO-178C/ED-12C and DO-254/ED-80).

Item: a hardware or software element that has bounded and well-defined interfaces (source: ARP4754A/ED-79A).

Open problem report (OPR): a problem report that has not reached the state 'Closed' at the time of approval.

Problem report (PR): a means to identify and record the resolution of anomalous behaviour, process non-compliance with development assurance plans and standards, and deficiencies in life-cycle data (adapted from DO-178C/ED-12C).

Product: refer to Article 3(3) of Regulation (EU) 2018/1139 (the 'EASA Basic Regulation').

System: a combination of interrelated equipment, article(s), and/or items arranged to perform a specific function (or functions) within a product.

4.2. States of PRs/OPRs

Recorded: a problem that has been documented using the problem-reporting process.

Classified: a problem report that has been categorised in accordance with an established classification scheme.

Resolved: a problem report that has been corrected or fully mitigated, for which the resolution of the problem has been verified but not formally reviewed and confirmed.

Closed: a resolved problem report that underwent a formal review and confirmation of the effective resolution of the problem.

4.3. Classifications of PRs/OPRs

'Significant': assessed at the product, system, or equipment level, a PR that has an actual or potential effect on the product, system, or equipment function that may lead to a Catastrophic, Hazardous or Major failure condition, or may affect compliance with the operating rules.

'Functional': a PR that has an actual or a potential effect on a function at the product, system, or equipment level.

'Process': a PR that records a process non-compliance or deficiency that cannot result in a potential safety, nor a potential functional, effect.

'Life-cycle data': a PR that is linked to a deficiency in a life-cycle data item but not linked to a process non-compliance or process deficiency.

5. PROBLEM REPORT MANAGEMENT

The PR management process is a key enabler for the management of OPRs. The PR management process enables the consistent and timely management of problems encountered across the system, software and AEH domains. Consequently, this process reduces the risk of a loss of visibility of critical issues remaining at the time of approval.

5.1 A PR management process across the system, software and AEH domains should be established and used during the development (both for initial certification and subsequent changes) of a

product or an ETSO article. The PR management process should address the review and resolution of PRs that impact the transition to other development assurance processes.

5.2 A problem recorded after approval should also be managed through the PR management process, and any related systemic process issues should be identified and corrected.

5.3 PRs that cannot be resolved by the current stakeholder should be reported in a manner that is understandable to the affected stakeholders.

5.4 For PRs that may have an impact on other products or articles that are developed within an organisation, a means should be established for sharing PR information so that any necessary corrective actions can be taken.

6. OPR MANAGEMENT

An OPR management process, based on the PR management process, should be established across the system, software and AEH domains, including the following process steps:

6.1 The classification of OPRs

6.1.1 The applicant should establish an OPR classification scheme including, at a minimum, the following classifications: 'Significant', 'Functional', 'Process' and 'Life-cycle data'. Other classifications or subclassifications may be created as needed. The classification scheme should be described in the appropriate planning document(s).

6.1.2 Each OPR should be assigned a single classification per the classification scheme. When multiple classifications apply, the OPR should be assigned the classification with the highest priority. The priority from highest to lowest (including the defined subclassifications) is:

1. 'Significant';
2. 'Functional';
3. 'Process';
4. 'Life-cycle data';
5. any other OPR classification.

Note: The classification of an individual OPR may differ from one stakeholder to another, depending on the known mitigations at the time of classification.

6.1.3 The classification of an OPR should account for and document all the mitigations known at the time of classification that are under the control of the classifying stakeholder. A mitigation that is controlled by another stakeholder may be considered in the classification only if validated with that stakeholder, and provided this mitigation remains acceptable in the frame of the type certificate (TC) / supplemental type certificate (STC) approval or European technical standard order (ETSO) article authorisation, as applicable.

6.1.4 A stakeholder, other than the aircraft TC or STC applicant, should classify as 'Significant' any OPR for which the classification may vary between 'Functional' and 'Significant', depending on the installation.

6.2 The assessment of OPRs

Each OPR should be assessed to determine:

1. any resulting functional limitations or operational restrictions at the equipment level (for ETSOs) or at the product level (for other types of approvals);
2. relationships that may exist with other OPRs; and
3. for a 'Significant' or 'Functional' OPR, the underlying technical cause of the problem.

6.3 **Disposition:** OPRs classified as 'Significant' per the classification in Section 6.1, for which no sufficient mitigation or justification exists to substantiate the acceptability of the safety effect, should be resolved prior to approval. The disposition of OPRs may involve coordination with the certification authority.

6.4 **Reporting:** an OPR summary report should be prepared and provided to the affected stakeholder(s), and to the certification authority upon request. The OPR summary report may be an aggregation of summaries (e.g. Software/Hardware Accomplishment Summaries or system-level OPR reports) prepared by all the involved stakeholders. The summary report should provide access to the following information for each OPR:

6.4.1 The identification of the OPR (for example, the OPR ID);

6.4.2 The identification of the affected configuration item(s) (for example, the item part number, component name, artefact name) or of the affected process(es);

6.4.3 Title or a summary of the problem, formulated in a manner understandable by the affected stakeholder(s);

6.4.4 Description of the problem, formulated in a manner understandable by the affected stakeholder(s);

6.4.5 The conditions under which the problem occurs;

6.4.6 The OPR classification and assessment results (per Sections 6.1 and 6.2), including:

1. for each OPR, regardless of its classification:
   a. the classification of the OPR, and
   b. the relationships that are known to exist with other OPRs;
2. for OPRs classified as 'Significant':
   a. a description of any mitigations or justifications used to substantiate the acceptability of the OPR safety effect (per Section 6.3), and
   b. the functional limitations and operational restrictions, if any;
3. for OPRs classified as 'Functional':
   a. a description of any mitigations or justifications used to reduce the safety effect to Minor or No Safety Effect, and
   b. the functional limitations and operational restrictions, if any;

4. for OPRs classified as 'Process', a description of the extent or nature of the process non-compliance or deficiency that might contribute to not satisfying the applicable development assurance objectives; and

5. for each OPR not classified as 'Significant' or 'Functional', the justification that the error cannot have a safety or functional effect.

6.5 ETSO specifics: The ETSO authorisation holder may exclude from the reporting process (per Section 6.4) any OPRs classified as 'Process' or 'Life-cycle data' that are not necessary for the installation approval. However, all OPRs should be available upon request by the certification authority for assessment in the frame of the ETSO approval.

7. STAKEHOLDER RESPONSIBILITIES

The levels of stakeholders include: item, equipment or ETSO article, system and product. The actual stakeholders for a specific project depend on the project organisation.

7.1 PR management (per Section 5) should be performed by the stakeholder at each level. The applicant has responsibility for the overall PR process for all the involved stakeholders.

7.2 OPR management (per Section 6) should be performed, at a minimum, at the ETSO article level, at the level of each individual system within a product, and at the product level.

8. RELATED REGULATORY, ADVISORY AND INDUSTRY MATERIAL

(a) Related EASA Certification Specifications (CSs)

(1) CS-23, *Certification Specifications and Acceptable Means of Compliance for Normal Category Aeroplanes*

(2) CS-25, *Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes*

(3) CS-27, *Certification Specifications and Acceptable Means of Compliance for Small Rotorcraft*

(4) CS-29, *Certification Specifications and Acceptable Means of Compliance for Large Rotorcraft*

(5) CS-E, *Certification Specifications and Acceptable Means of Compliance for Engines, and AMC 20-3A, Certification of Engines Equipped with Electronic Engine Control Systems*

(6) CS-P, *Certification Specifications for Propellers, and AMC 20-1, Certification of Aircraft Propulsion Systems Equipped with Electronic Control Systems*

(7) CS-ETSO, *Certification Specifications for European Technical Standard Orders*

(8) CS-APU, *Certification Specifications for Auxiliary Power Units*, and AMC 20-2A, *Certification of Essential APU Equipped with Electronic Controls*

(b) EASA Acceptable Means of Compliance (AMC)

(1) AMC 20-115( ), *Airborne Software Development Assurance Using EUROCAE ED-12 and RTCA DO-178*

(2) AMC 20-152( ), *Development Assurance for Airborne Electronic Hardware*

(c) FAA ACs

Refer to latest version.

(1) AC 20-115( ), *Airborne Software Development Assurance Using EUROCAE ED-12( ) and RTCA DO-178( )*

(2) AC 20-152( ), *Development Assurance for Airborne Electronic Hardware*

(3) AC 27-1309( ), *Equipment, Systems, and Installations (included in AC 27-1, Certification of Normal Category Rotorcraft)*

(4) AC 29-1309( ), *Equipment, Systems, and Installations (included in AC 29-2, Certification of Transport Category Rotorcraft)*

(d) Industry Documents

(1) EUROCAE ED-12, *Software Considerations in Airborne Systems and Equipment Certification*, dated May 1982 (no longer in print)

(2) EUROCAE ED-12A, *Software Considerations in Airborne Systems and Equipment Certification*, dated October 1985 (no longer in print)

(3) EUROCAE ED-12B, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 1992

(4) EUROCAE ED-12C, *Software Considerations in Airborne Systems and Equipment Certification,* dated January 2012

(5) EUROCAE ED-79A, *Guidelines for Development of Civil Aircraft and Systems*, dated December 2010

(6) EUROCAE ED-80, *Design Assurance Guidance for Airborne Electronic Hardware*, dated April 2000

(7) EUROCAE ED-94C, *Supporting Information for ED-12C and ED-109A*, dated January 2012

(8) EUROCAE ED-215, *Software Tool Qualification Considerations,* dated January 2012

(9) EUROCAE ED-216, *Formal Methods Supplement to ED-12C and ED-109A*, dated January 2012

(10) EUROCAE ED-217, Object-Oriented Technology and Related Techniques Supplement to ED-12C and ED-109A, dated January 2012

(11) EUROCAE ED-218, Model-Based Development and Verification Supplement to ED-12C and ED-109A, dated January 2012

(12) RTCA DO-178, Software Considerations in Airborne Systems and Equipment Certification, dated January 1982 (no longer in print)

(13) RTCA DO-178A, Software Considerations in Airborne Systems and Equipment Certification, dated March 1985 (no longer in print)

(14) RTCA DO-178B, Software Considerations in Airborne Systems and Equipment Certification, dated 1 December 1992

(15) RTCA DO-178C, Software Considerations in Airborne Systems and Equipment Certification, dated 13 December 2011

(16) RTCA DO-248C, Supporting Information for DO-178C and DO-278A, dated 13 December 2011

(17) RTCA DO-254, Design Assurance Guidance for Airborne Electronic Hardware, dated April 19, 2000

(18) RTCA DO-297, Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations, dated 8 November 2005

(19) RTCA DO-330, Software Tool Qualification Considerations, dated 13 December 2011

(20) RTCA DO-331, Model-Based Development and Verification Supplement to DO-178C and DO-278A, dated 13 December 2011

(21) RTCA DO-332, Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A, dated 13 December 2011

(22) RTCA DO-333, Formal Methods Supplement to DO-178C and DO-278A, dated 13 December 2011

(23) SAE International Aerospace Recommended Practice (ARP) 4754A, Guidelines for Development of Civil Aircraft and Systems

9. AVAILABILITY OF DOCUMENTS

(1) EASA Certification Specifications (CSs) and Acceptable Means of Compliance (AMC) may be downloaded from the EASA website: www.easa.europa.eu

(2) FAA Advisory Circulars (ACs) may be downloaded from the FAA website: www.faa.gov

(3) EUROCAE documents may be purchased from:

European Organisation for Civil Aviation Equipment
9-23 rue Paul Lafargue
"Le Triangle" building
93200 Saint-Denis, France

Telephone: +33 1 49 46 19 65
(Email: eurocae@eurocae.net, website: www.eurocae.net)

(4) RTCA documents may be purchased from:

RTCA, Inc.1150 18th Street NW, Suite 910, Washington DC 20036, USA

(Email: info@rtca.org, website: www.rtca.org)

10. GUIDANCE MATERIAL

GM 20-189 The Management of Open Problem Reports

GM1 to AMC 20-189 — PR management

Typically, PR processes include the following aspects:

1. PR Recording: a means to document problems resulting from the execution of life-cycle processes.

2. PR Classification: a means to classify PRs prior to the time of approval of the product or of the ETSO article, as early in the life cycle as practical. While early classification may be preliminary, it will help to focus attention on PRs with a potential safety or functional effect, as well as process PRs that may impact the development or development assurance processes.

3. PR Assessment: a means to assess the effect of having a PR remain open at the time of approval. The assessment of PRs classified as 'Significant', 'Functional' or 'Process' would typically be performed by a review board. The assessment of PRs classified as 'Life-cycle data' may be performed within the peer-review process instead of a review board.

4. PR Resolution: a means to correct or mitigate PRs prior to the time of approval, as early in the life cycle as practical. The PR resolution process may depend on the classification of the PR; for example, shorter closure loops could be set for PRs classified as 'Life-cycle data'.

5. PR Closure: a means to close PRs, which includes the review and confirmation of the resolution of the problem, and indicated through a documented authorisation process (e.g. Change Control Board sign-off).

GM2 to AMC 20-189 — OPR classification

The following paragraph links the classifications presented in DO-248C/ED-94C, DP #9 to those defined in AMC 20-189, subparagraph 6.1. This paragraph highlights the clarifications made to the former scheme (e.g. removing the overlaps between the classifications).

1. The most important clarification compared with the former classification scheme is to give each OPR a single classification using a given order of priority as reflected in AMC 20-189 subparagraph 6.1.2. This promotes visibility of the most relevant issues and helps to prevent inconsistencies in classification. For example, a missing or incorrect requirement issue can be classified as 'Life-cycle data' only if it is confirmed that it cannot be classified as 'Significant', 'Functional', or 'Process', in that order of priority.

2. Type 'Significant': this typically maps to 'Type 0'. However, some applicants may have used 'Type 1A' to characterise some PRs, for instance, those linked to Major failure conditions. The AMC 20-189 scheme clarifies that those PRs potentially causing or contributing to Catastrophic, Hazardous or Major failure conditions belong to the class 'Significant'.

3. Type 'Functional': this typically maps to 'Type 1A' or 'Type 1B', that is, a problem that results in a failure with a minor or no adverse impact on safety. A PR whose consequences are a failure that can potentially lead to a Minor failure condition could be mapped to 'Type 1A', and a PR leading to a failure having No Safety Effect could be mapped to 'Type 1B'. Two separate subclassifications could therefore be created in the applicant's classification scheme to ease the

mapping: problems having a functional effect leading to a Minor failure condition could be classified separately (e.g. 'Functional 1') from the ones having No Safety Effect (e.g. 'Functional 2'). Moreover, an important clarification is that AMC 20-189 does not explicitly consider the 'operational' nature of a PR in the classification scheme to avoid creating overlaps, as a PR with operational consequences could either be classified as 'Significant' or 'Functional'. Creating an 'Operational' subclassification within the classification 'Significant' or 'Functional' is nevertheless an option available to stakeholders to create a specific emphasis on operational issues within the proposed classification scheme.

4. Type 'Process': this may map to 'Type 3A'; however, not in cases where the process non-compliance or deficiency could result in either not detecting a failure or creating a failure. An important clarification in AMC 20-189 is the removal of the ambiguous notion of 'significant deviation from the plans or standards' used in the definition of 'Type 3A'. The 'Process' classification in AMC 20-189 should be used for PRs that record a process non-compliance or deficiency, provided they cannot result in a potential safety or potential functional effect. An example of an OPR that should not be classified as a 'Process' PR is one related to a requirement that was not completely verified due to a process deficiency, because the potential safety or functional impact remains undetermined. Considering the highest priority classification would, in such a case, lead to a 'Significant' or 'Functional' classification, thus putting even more emphasis on the need to resolve the shortcoming in the verification activities.

5. Type 'Life-cycle data': this typically maps to 'Type 2' or 'Type 3B'. Since 'Life-cycle data' OPRs may range widely, subclassifications may be proposed by stakeholders to distinguish the different types of OPRs. Examples of OPRs classified as 'Life-cycle data' may range from issues in a component having no potential safety or functional impact to PRs on pure documentary issues. Moreover, the removal of the notion of 'non-significant deviation from the plans or standards' from the definition of 'Type 3B' helps to remove the ambiguity and overlap between the 'Process' and 'Life-cycle data' classifications.

6. Other OPR classification: additional classifications of OPRs may be created to cover 'Type 4' or any other classification not specified in AMC 20-189, paragraph 6.1.1.

GM3 to AMC 20-189 — Additional GM related to the 'Significant' classification

In the frame of an engine or propeller TC/STC or of an ETSO article authorisation, the definition of 'Significant' is based on the anticipation of a potential effect on the product, system, or equipment function that could lead to a Catastrophic, Hazardous or Major failure condition. The goal is to identify and enhance the visibility of OPRs that may pose potential safety risks at the aircraft installation level (see AMC 20-189 paragraph 6.1.4).

For example, in the case of an engine TC, a partial or complete loss of thrust or power is regarded as a Minor Engine Effect, whereas it may have a more severe effect at the aircraft level. Unless the engine manufacturer can confirm that the effect at the installation level is no more than Minor, the OPR would be classified as 'Significant'. The associated assumptions or mitigations are usually recorded through instructions for installing and operating the engine, e.g. in an engine installation manual.

In the case of an ETSO authorisation, classification of the failure condition is either based on assumptions defined by the applicant, or mandated through the ETSO standard, and is the basis of the

safety analysis at the ETSO article level. An OPR is classified as ‘Significant’ when the OPR may lead to a functional failure associated with a Catastrophic, Hazardous or Major failure condition.

9. The following Subpart B is inserted:

SUBPART B — LIST OF AMC-20

Index 1

EASA AMC-20 reference	Title	Last amended by
AMC 20-1A	The Certification of Aircraft Propulsion Systems Equipped with Electronic Controls	AMC-20 Amdt 19
AMC 20-2B	The Certification of Essential APUs Equipped with Electronic Controls	AMC-20 Amdt 19
AMC 20-3B	The Certification of Engines Equipped with Electronic Engine Control Systems	AMC-20 Amdt 19
AMC 20-4A	Airworthiness Approval and Operational Criteria For the Use of Navigation Systems in European Airspace Designated For Basic RNAV Operations	Cancelled (By AMC-20 Amdt 17)
AMC 20-5	Airworthiness Approval and Operational Criteria for the use of the Navstar Global Positioning System (GPS)	Cancelled (By AMC-20 Amdt 17)
AMC 20-6 rev 2	Extended Range Operation with Two-Engine Aeroplanes ETOPS Certification and Operation	AMC-20 Amdt 7
AMC 20-8A	Occurrence Reporting	AMC-20 Amdt 19
AMC 20-9	Acceptable Means of Compliance for the Approval of Departure Clearance via Data Communications over ACARS.	AMC-20 Amdt 1
AMC 20-10	Acceptable Means of Compliance for the Approval of Digital ATIS via Data Link over ACARS.	AMC-20 Amdt 1
AMC 20-11	Acceptable Means of Compliance for the Approval of use of Initial Services for Air Ground Data Link in Continental Airspace	Cancelled (by AMC-20 Amdt 11)
AMC 20-12	Recognition of FAA Order 8400.12a for RNP 10 Operations	Cancelled (By AMC-20 Amdt 17)
AMC 20-13	Certification of Mode S Transponder Systems for Enhanced Surveillance	Cancelled (by AMC-20 Amdt 11)
AMC 20-15	AMC 20-15 Airworthiness Certification Considerations for the Airborne Collision Avoidance System (ACAS II) with optional Hybrid Surveillance	AMC 20 Amdt 8
AMC 20-19	In-Flight Entertainment	AMC-20 Amdt 19
AMC 20-20	Continuing Structural Integrity Programme	AMC-20 Amdt 3

EASA AMC-20 reference	Title	Last amended by
AMC 20-21	Programme to enhance aeroplane Electrical Wiring Interconnection System maintenance	AMC- 20 Amdt 4
AMC 20-22	Aeroplane Electrical Wiring Interconnection System Training Programme	AMC- 20 Amdt 4
AMC 20-23	Development of Electrical Standard Wiring Practices documentation	AMC- 20 Amdt 4
AMC 20-24	Certification Considerations for the Enhanced ATS in Non-Radar Areas using ADS-B Surveillance (ADS-B-NRA) Application via 1090 MHZ Extended Squitter	AMC-20 Amdt 3
AMC 20-25A	Airworthiness consideration for Electronic Flight Bags (EFBs)	AMC-20 Amdt 16
AMC 20-26	Airworthiness Approval and Operational Criteria for RNP Authorisation Required (RNP AR) Operations	Cancelled (By AMC-20 Amdt 17)
AMC 20-27A	Airworthiness Approval and Operational Criteria for RNP APPROACH (RNP APCH) Operations Including APV BARO-VNAV Operations	Cancelled (By AMC-20 Amdt 17)
AMC 20-28	Airworthiness Approval and Operational Criteria related to Area Navigation for Global Navigation Satellite System approach operation to Localiser Performance with Vertical guidance minima using Satellite Based Augmentation System	Cancelled (By AMC-20 Amdt 17)
AMC 20-29	Composite Aircraft Structure	AMC-20 Amdt 6
AMC 20-42	Airworthiness information security risk assessment	AMC-20 Amdt 18
AMC 20-115D	Software considerations for certification of airborne systems and equipment	AMC-20 Amdt 14
AMC 20-128A	Design Considerations for Minimizing Hazards Caused by Uncontained Turbine Engine and Auxiliary Power Unit Rotor Failure	AMC-20 Initial issue
AMC 20-136	Aircraft electrical and electronic system lightning protection	AMC-20 Amdt 13
AMC 20-152A	Airborne Electronic Hardware	AMC-20 Amdt 19
AMC 20-158	Aircraft electrical and electronic system high-intensity radiated fields (HIRF) protection	AMC-20 Amdt 13
AMC 20-170	IMA	AMC-20 Amdt 15
AMC 20-189	The Management of Open Problem Reports	AMC-20 Amdt 19