U.S. Department
of Transportation
**Federal Aviation
Administration**

Advisory Circular

Subject: Best Practices for Airborne Software Development Assurance Using EUROCAE ED-12( ) and RTCA DO-178( )

Date: 07/21/2017

Initiated by: AIR-134

AC No: 00-69

Change:

1 **PURPOSE.** This advisory circular (AC) provides information in the form of "best practices" and, as such, is not intended as guidance but rather as complementary information to ED-12C/DO-178C (and related documents) and AC 20-115D.

2 **AUDIENCE.** We wrote this AC as a means of assisting applicants, design approval holders and developers of airborne systems and equipment containing software intended to be installed on type certificated aircraft, engines, and propellers, or to be used in TSO articles.

3 BEST PRACTICES.

3.1 Software Change Impact Analyses (CIA).

3.1.1 These practices provide complementary information to ED-12C/DO-178C and ED-12B/DO-178B, section 12.1.1, 12.1.2, and 12.1.3; and AC 20-115D section 9.b.(4). You may consider using these best practices when you need to conduct a software CIA.

3.1.2 The CIA identifies the released software baseline upon which the proposed software is to be built, providing:

3.1.2.1 A summary of the changes and impact of the changes;

3.1.2.2 A listing and descriptions of the problem reports to be corrected as part of the intended change and/or change requests related to those changes; and

3.1.2.3 A listing of new functions to be activated and/or implemented.

3.1.3 The CIA addresses changes in the following items, where applicable:

3.1.3.1 Software level;

3.1.3.2 Development or verification environment;

3.1.3.3 Software processes;

3.1.3.4 Tools (e.g. when a new tool version is introduced or a tool’s use is modified);

3.1.3.5 Processor or other hardware components and interfaces;

3.1.3.6 Configuration data, especially when activating or deactivating functions;

3.1.3.7 Software interface characteristics and input/output requirements; and

3.1.3.8 Software requirements, design, architecture, and code components, where such changes are not limited to the modified life-cycle data, but should also consider the ones affected by the change.

3.1.4 For each applicable item in subparagraph **3.1.3** (above), the CIA describes the resulting impact and identifies the activities to be performed to satisfy ED-12C/DO-178C and ED-12B/DO-178B and continue to satisfy requirements for safe operation.

3.2 **Clarification on Data Coupling and Control Coupling.** These practices provide complementary information to ED-94C/DO-248C, FAQ #67 for satisfying objective A-7 (8) of ED-12C/DO-178C and ED-12B/DO-178B:

3.2.1 Data coupling analysis is of different type and purpose than control coupling analysis. Both analyses are necessary to satisfy this objective.

3.2.2 Although they support a verification objective, data coupling and control coupling analyses rely on good practices in the software design phase; for example, through the specification of interfaces (I/O) and of dependencies between components.

3.3 **Error Handling at Design Level.**

3.3.1 These practices provide complementary information to ED-12C/DO-178C and ED-12B/DO-178B, sections 6.3.2, 6.3.3, and 6.3.4. Section 6.3.4.f. identifies potential sources of errors that require specific activity focused at the source code review level. However, in order to protect against foreseeable unintended software behavior, it is beneficial and recommended to handle these sources of error at the design level.

3.3.2 To reduce the possibility of unintended software behavior, consider the following activities:

3.3.2.1 Identification of foreseeable sources of software errors, which include:

3.3.2.1.1 Runtime exceptions or errors like fixed/floating point arithmetic overflow, stack/heap overflow, division by zero, or counter and timer overrun/wrap-around.

3.3.2.1.2 Data/memory corruption or timing issues like those due to lack of partitioning or to improper interrupt management or cache management.

3.3.2.1.3 Features leading to unpredictable program execution like dynamic allocation, out of order execution, or resource contention.

3.3.2.2 For each foreseeable source of software error, identification of the associated mitigation.

3.3.2.3 Specification of protection mechanisms in the software requirements (high level requirements or low level requirements), which in particular include the specification and verification of handling mechanisms.

3.3.2.4 For software levels A and B, it is recommended that consideration be given to incorporating runtime protection mechanisms, since reliance on probabilistic approaches or static analyses alone may not be adequate. It may be a good practice to implement such runtime mechanisms for the other software levels.

3.3.3 Use of Formal Methods according to ED-216/DO-333 may enhance the detection of runtime errors.

4 RELATED PUBLICATIONS.

4.1 14 CFR Applicable Sections. 14 CFR parts 21, 23, 25, 27, 29, 33, and 35.

4.2 FAA Advisory Circulars (ACs).

- AC 20-170, *Integrated Modular Avionics Development, Verification, Integration and Approval using RTCA DO-297 and Technical Standard Order C-153.*
- AC 20-171, *Alternatives to RTCA/DO-178B for Software in Airborne Systems and Equipment*.
- AC 20-174, *Development of Civil Aircraft and Systems*.
- AC 21-50, *Installation of TSOA Articles and LODA Appliances*.
- AC 23.1309-1, *System Safety Analysis and Assessment for Part 23 Airplanes.*
- AC 25.1309-1, *System Design and Analysis*.
- AC 27-1309, *Equipment, Systems, and Installations* (included in AC 27-1, *Certification of Normal Category Rotorcraft*).
- AC 29-1309, *Equipment, Systems, and Installations* (included in AC 29-2, *Certification of Transport Category Rotorcraft*).
- AC 33.28-1, *Compliance Criteria for 14 CFR § 33.28, Aircraft Engines, Electrical and Electronic Engine Control Systems*.
- AC 33.28-2, *Guidance Material for 14 CFR 33.28, Reciprocating Engines, Electrical and Electronic Engine Control Systems*.
- AC33.28-3, *Guidance Material for 14 CFR § 33.28, Engine Control Systems.*

- AC 35.23-1, *Guidance Material for 14 CFR 35.23, Propeller Control Systems*.

4.3 **Industry Documents.**

- RTCA DO-178, *Software Considerations in Airborne Systems and Equipment Certification*, dated January 1982 (no longer in print).
- RTCA DO-178A, *Software Considerations in Airborne Systems and Equipment Certification*, dated March 1985 (no longer in print).
- RTCA DO-178B, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 1, 1992.
- RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 13, 2011.
- RTCA DO-248C, *Supporting Information for DO-178C and DO-278A*, dated December 13, 2011.
- RTCA DO-297, *Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations*, dated November 8, 2005.
- RTCA DO-330, *Software Tool Qualification Considerations*, dated December 13, 2011.
- RTCA DO-331, *Model-Based Development and Verification Supplement to DO-178C and DO-278A*, dated December 13, 2011.
- RTCA DO-332, *Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A*, dated December 13, 2011.
- RTCA DO-333, *Formal Methods Supplement to DO-178C and DO-278A*, dated December 13, 2011.
- EUROCAE ED-12, *Software Considerations in Airborne Systems and Equipment Certification*, dated May 1982 (no longer in print).
- EUROCAE ED-12A, *Software Considerations in Airborne Systems and Equipment Certification*, dated October 1985 (no longer in print).
- EUROCAE ED-12B, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 1992.
- EUROCAE ED-12C, *Software Considerations in Airborne Systems and Equipment Certification*, dated January 2012.
- EUROCAE ED-94C, *Supporting Information for ED-12C and ED-109A*, dated January 2012.
- EUROCAE ED-215, *Software Tool Qualification Considerations*, dated January 2012.
- EUROCAE ED-216, *Formal Methods Supplement to ED-12C and ED-109A*, dated January 2012.

- EUROCAE ED-217, *Object-Oriented Technology and Related Techniques Supplement to ED-12C and ED-109A*, dated January 2012
- EUROCAE ED-218, *Model-Based Development and Verification Supplement to ED-12C and ED-109A*, dated January 2012.

5 WHERE TO FIND THIS AC.

5.1 You may find this AC at http://www.faa.gov/regulations_policies/advisory_circulars/.

5.2 If you have suggestions for improvement or changes, you may use the template in appendix A at the end of this AC.

Susan JM Cabler

Susan J. M. Cabler
Manager, Design, Manufacturing, &
Airworthiness Division
Aircraft Certification Service

Appendix A. Advisory Circular Feedback Information

If you find an error in this AC, have recommendations for improving it, or have suggestions for new items/subjects to be added, you may let us know by (1) complete the form online at https://ksn2.faa.gov/avs/dfs/Pages/Home.aspx or (2) emailing this form to 9-AWA-AVS-AIR-DMO@faa.gov

Subject: AC 00-SW Date: ___________

Please check all appropriate line items:

□ An error (procedural or typographical) has been noted in paragraph _______ on page _______.

□ Recommend paragraph _______ on page _______ be changed as follows:

□ In a future change to this AC, please cover the following subject:
(Briefly describe what you want added.)

□ Other comments:

□ I would like to discuss the above. Please contact me.

Submitted by: ________________________________ Date: __________________