Software Certification

BECA APPLIED TECHNOLOGIES

03 NOVEMBER 2022

Agenda

- Introductions
- About us – who Beca Applied Technologies is and what we do
- Key Aviation Projects
- Software Certification
- Airborne Electronic Hardware Certification
- Market Position
- Questions

Images of NZDF equipment in this presentation are sourced from NZDF and used with NZDF's permission

Speakers

Brian Fearnley:
Business Director – Major Programmes,

More than 30 years of technical programme, business, project, and commercial management experience across defence, aviation and rail.

Brian has held senior positions in:

- BAE Systems Australia
- Airbus Group Australia
- Alstom Transport NZ Ltd
- Civil Aviation Authority of New Zealand
- Royal New Zealand Air Force

Robert McGivern:
Technical Director - Software Engineering

DDH & Senior Person for Inspection & Test

32 Years Software Development Experience

- 17 Years Aviation Software
- 7 Years Military Real Time Control Systems
- Specialist Subjects:
  - Software development
  - Mathematical Algorithms
  - DO-178B/C

Beca In Brief

- One of **Asia Pacific's leading professional services** consultancies
- Over **3600 employees** worldwide
- Delivering projects in over **70 countries**
- **Highly engaged,** values driven culture
- **Employee-owned multidisciplinary professional services organisation** offering services across business advisory, engineering, architecture and planning, project and cost management, digital and software technologies and valuation
- **End to end delivery** across the asset, infrastructure and business lifecycle

Beca Group of Companies

Beca Group Limited

Chair	Group Chief Executive
David Carter	**Greg Lowe**

Asia Region	Australia	International	New Zealand
Beca Carter Hollings & Ferner (S.E. Asia) Pte Ltd (Sg)	Beca Pty Ltd	Beca International Consultants Ltd	Beca Ltd
Beca PCM Pte Ltd (Sg)	Beca Consultants Pty Ltd	Beca Nouvelle Caledonie S.A.R.L (New Caledonia)	Beca Engineering New Zealand Ltd
Beca Philippines Ltd	Hunter H2O Holdings Pty Ltd	Beca Pacific, Inc. (American Samoa)	Beca Projects NZ Ltd
Beca (Thailand) Co., Ltd ("Beca Warnes")*		BICL (NL) B.V. Netherlands)	Beca Applied Technologies Ltd
Myanmar Beca Ltd			Wood Beca Ltd*
PT Bimatekno Kayatama Konsultan (Indo)			CH2M Beca Ltd*

As at May 2022
*Joint Venture

Beca Applied Technologies

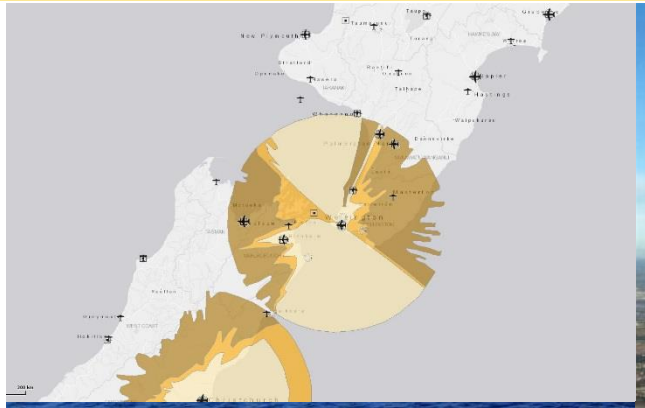
Clever people delivering smart solutions across the defence, aerospace and security sectors.

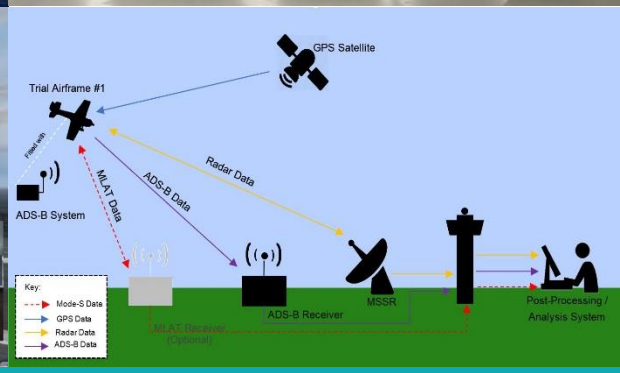
- 65 systems and software engineers
- Backgrounds across Engineering, Science, Advisory, Aviation, Maritime, Rail, Space, and Security
- 1x NZ CAA DDH - SW and AEH Design Approval Authority
- 4x NZDF Delegated Engineering Authorities for P-3K2 software
- 3 x NZDF authorisations for the SH-2G(I) ITAS

Our Clients

Organisations whose effective operation is reliant on safety or mission critical systems, software and related technology:

- Defence
- Civil Aviation
- Space
- Rail
- Security





What We Do

Sectors

Civil and military aviation, maritime, land, rail and space

Services

Safety and mission critical software and systems engineering and technology management

Roles

Partner, prime, integrator, project manager

Certificates

- NZCAA Part 146 Approved Design Organisation Level-A Software and AEH and delegation holder
- NZDF Approved Design Authority SH-2G(I) Seasprite Helicopter Integrated Tactical Avionics System software
- NZDF Approved Design Authority P-3K2 Orion Aircraft Mission System Software
- ISO 9001

Aviation Projects

SH-2G(I) Seasprite Helicopter Integrated Tactical Avionics System (ITAS)

Software lifecycle support (level-A)
Avionics obsolescence replacements and upgrades (ADS-B/IFF, CMFD, Comms, Radar)

P-3K2 Mission System

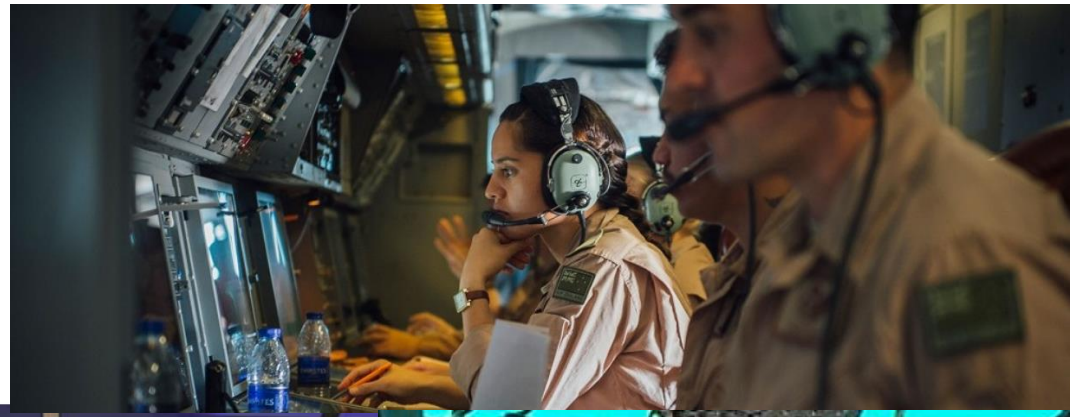
Data Management System (DMS) lifecycle support
Mission Planning & Analysis System
System Integration & Training Lab
Data Warehouse
Flight Deck & Part Task Trainers

Simulator Install, Support & Qualification

SH-2G(I) FMFS and PTTs
A109LUH(NZ) FTD and PTTs
B737 FFS
Joint Terminal Attack Controller

NZ Civil Aviation Authority

New Southern Sky GNSS and Navigation performance assessments
ADS-B Lite options



Project: P3-K2 Orion

Project Duration: 13 Years (& Counting)

Project Definition:

- Software Engineering & Systems Engineering services for the aircraft Data Management System (Aircraft Mission System)
- Software development: DO-178C (Mission Critical DAL)

Beca Role:

- Initial development & integration of the DMS
- Development of Software Integration Test Lab
- Ground up deployment of DO-178C process
- Software updates
  - Underwater ISR Capability Insertion
  - AIS Integration
  - Hardware obsolescence driven programs.
  - Integrated mission systems with Nav/Radar systems.

Project: SH2-G(I)

Project Duration: 6 Years (& Counting)

Project Definition:

- Provide all Software Engineering & Systems Engineering services for the Integrated Tactical Avionics System (≈Integrated FMS and weapons system)
- DO-178C (DAL A) software development & through life support.

Beca Role:

- Rebuilt and qualified Test Rig to DO-330
- Re-developed pre-mission data load system.
- Reworked OEM development process to be aligned with DO-178C
- Redeveloped the Design Control System
  - Implemented PLM/Config management tools
- Manage all software problem reports – continuing airworthiness
- Currently undertaking major aircraft modification
  - Primary flight display replacement
  - All aspects software, hardware, Integration & Certification
- Planning Phase – Major capability sustainment program(s)

Merlin Labs Take-off to Touchdown Autonomy System STC

- Flight Structurers are the lead P146
- Beca Applied Technologies Role:
  - Certification planning
  - Certification (assessing compliance) of airborne software and electronic hardware:
    - Flight Control Computer Software
      - Murray Core Application
      - Board Support Package (BSP)
      - Real Time Operating System (RTOS)
    - Flight Control Computer Airborne Electronic Hardware (AEH)
    - Servo software
  - CAA liaison for SW and AEH

Software Certification

Audience Poll: 4 Questions

Who knows what DO-178c is?

Audience Poll: 4 Questions

Who knows what DO-178c is?

Who cares what DO-178c is?

Audience Poll: 4 Questions

Who knows what DO-178c is?

Who cares what DO-178c is?

Are there any Software Engineers/DDHs here?

Audience Poll: 4 Questions

- Who knows what DO-178c is?
- Who cares what DO-178c is?
- Are there any Software DDHs here?
- Are you awake?

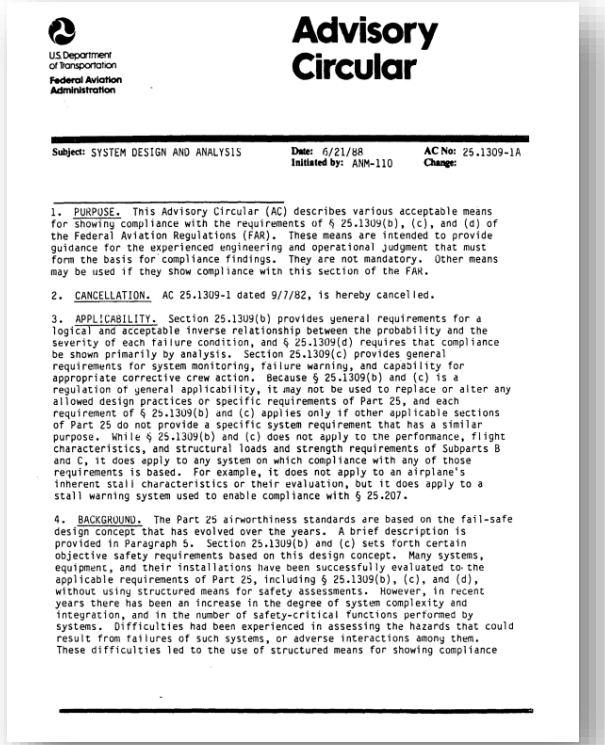
14 CFR 25.1309

- **§ 25.1309 Equipment, systems, and installations.**
- **(a)** The equipment, systems, and installations whose functioning is required by this subchapter, must be designed to ensure that they perform their intended functions under any foreseeable operating condition.
- **(b)** The airplane systems and associated components, considered separately and in relation to other systems, must be designed so that -
- **(1)** The occurrence of any failure condition which would prevent the continued safe flight and landing of the airplane is extremely improbable, and
- **(2)** The occurrence of any other failure conditions which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions is improbable.
- **(c)** Warning information must be provided to alert the crew to unsafe system operating conditions, and to enable them to take appropriate corrective action. Systems, controls, and associated monitoring and warning means must be designed to minimize crew errors which could create additional hazards.
- **(d)** Compliance with the requirements of paragraph (b) of this section must be shown by analysis, and where necessary, by appropriate ground, flight, or simulator tests. The analysis must consider -
- **(1)** Possible modes of failure, including malfunctions and damage from external sources.
- **(2)** The probability of multiple failures and undetected failures.
- **(3)** The resulting effects on the airplane and occupants, considering the stage of flight and operating conditions, and
- **(4)** The crew warning cues, corrective action required, and the capability of detecting faults.
- **(e)** In showing compliance with paragraphs (a) and (b) of this section with regard to the electrical system and equipment design and installation, critical environmental conditions must be considered. For electrical generation, distribution, and utilization equipment required by or used in complying with this chapter, except equipment covered by Technical Standard Orders containing environmental test procedures, the ability to provide continuous, safe service under foreseeable environmental conditions may be shown by environmental tests, design analysis, or reference to previous comparable service experience on other aircraft.
- **(f)** EWIS must be assessed in accordance with the requirements of § 25.1709.

AC 25.1309-1A (Paragraph 7)

h. Section 25.1309(c) provides requirements for system monitoring, failure warning, and capability for appropriate corrective crew action. Guidance on acceptable means of compliance is provided in Paragraph 8g.

i. In general, the means of compliance described in this AC are not directly applicable to software assessments because it is not feasible to assess the number or kinds of software errors, if any, that may remain after the completion of system design, development, and test. Advisory Circular 20-115A dated August 12, 1986, "Radio Technical Commission for Aeronautics Document RTCA/DO-178A," or later revisions thereto, provides acceptable means for assessing and controlling the software used to program digital computer-based systems. Document RTCA/DO-178A dated March 22, 1985, "Software Considerations in Airborne Systems and Equipment Certification," defines and uses certain terms to classify the criticalities of functions. For information, these terms have the following relationships to the terms used in this AC to classify failure conditions: failure conditions adversely affecting non-essential functions would be minor, failure conditions adversely affecting essential functions would be major, and failure conditions adversely affecting critical functions would be catastrophic.



U.S. Department of Transportation
Federal Aviation Administration

Advisory Circular

Subject: SYSTEM DESIGN AND ANALYSIS | Date: 6/21/88 | Initiated by: ANM-110 | AC No: 25.1309-1A | Change:

1. PURPOSE. This Advisory Circular (AC) describes various acceptable means for showing compliance with the requirements of § 25.1309(b), (c), and (d) of the Federal Aviation Regulations (FAR). These means are intended to provide guidance for the experienced engineering and operational judgment that must form the basis for compliance findings. They are not mandatory. Other means may be used if they show compliance with this section of the FAR.

2. CANCELLATION. AC 25.1309-1 dated 9/7/82, is hereby cancelled.

3. APPLICABILITY. Section 25.1309(b) provides general requirements for a logical and acceptable inverse relationship between the probability and the severity of each failure condition, and § 25.1309(d) requires that compliance be shown primarily by analysis. Section 25.1309(c) provides general requirements for system monitoring, failure warning, and capability for appropriate corrective crew action. Because § 25.1309(b) and (c) is a regulation of general applicability, it may not be used to replace or alter any allowed design practices or specific requirements of Part 25, and each requirement of § 25.1309(b) and (c) applies only if other applicable sections of Part 25 do not provide a specific system requirement that has a similar purpose. While § 25.1309(b) and (c) does not apply to the performance, flight characteristics, and structural loads and strength requirements of Subparts B and C, it does apply to any system on which compliance with any of those requirements is based. For example, it does not apply to an airplane's inherent stall characteristics or their evaluation, but it does apply to a stall warning system used to enable compliance with § 25.207.

4. BACKGROUND. The Part 25 airworthiness standards are based on the fail-safe design concept that has evolved over the years. A brief description is provided in Paragraph 5. Section 25.1309(b) and (c) sets forth certain objective safety requirements based on this design concept. Many systems, equipment, and their installations have been successfully evaluated to the applicable requirements of Part 25, including § 25.1309(b), (c), and (d), without using structured means for safety assessments. However, in recent years there has been an increase in the degree of system complexity and integration, and in the number of safety-critical functions performed by systems. Difficulties had been experienced in assessing the hazards that could result from failures of such systems, or adverse interactions among them. These difficulties led to the use of structured means for showing compliance

Other Parts

- AC 23.1309 -1E

  "AC 20-115B discusses how RTCA/DO-178B provides an acceptable means for showing that software complies with pertinent airworthiness requirements"

- ASTM F3061/F3061M − 20

  4.2.5.1 In showing compliance with the provisions of 4.2.5, once a DAL is assigned, acceptable means of compliance may be found in RTCA DO-178 or RTCA DO-254

- AC 27-1B

  RTCA Document DO-178C, "Software Considerations in Airborne Systems and Equipment Certification," dated December 13, 2011, is the latest standard and is recommended to be used for qualification and subsequent approval of airborne software.

- AC 29-2C - see table ->

Table for Failure Condition Categories and Probability Definitions

Effect on rotorcraft	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margin	Large reduction in functional capabilities or safety margins (Note 4)	Loss of rotorcraft
Effect on occupants excluding flight crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a passenger or a cabin crew member (NOTE 2)	Multiple Fatalities
Effect on flight crew	No effect on flight crew	Slight increase in work load which involve crew actions well within crew capabilities such as routine flight plan changes	Physical discomfort or a significant increase in workload or in conditions impairing crew efficiency	Physical distress or excessive workload impairs ability to perform tasks accurately or completely	Fatalities or incapacitation
DO-178C Software Level (Note 3)	E	D	C	B	A
Failure Condition Category	No Effect	Minor	Major	Hazardous or Severe-Major	Catastrophic
Qualitative Probability	Frequent	Reasonably Probable	Remote	Extremely Remote	Extremely Improbable
Quantitative Probability :	No probability requirement	$\leq 10^{-3}$ (Note 1)	$\leq 10^{-5}$	$\leq 10^{-7}$	$\leq 10^{-9}$

Note 1: A numerical probability range is provided here as reference. The applicant is not required to perform a quantitative analysis, or substantiate by such an analysis, that this numerical criterion has been met for Minor Failure Conditions.

Note 2: This is true if it can be shown that the given failure condition can be contained to a fatal injury of one occupant only.

Note 3: This is not intended to imply that the identified software levels are assigned a probability value, but instead, shows a correlation to the Failure Condition Category.

Note 4: Hazardous or Severe-Major failure conditions can include events that are manageable by the crew by use of proper procedures which, if not implemented correctly or in a timely manner, may result in a Catastrophic event.

FIGURE AC 29.1309-2
Failure Condition Categories and Probability Definitions

AC 20-115D

Title:

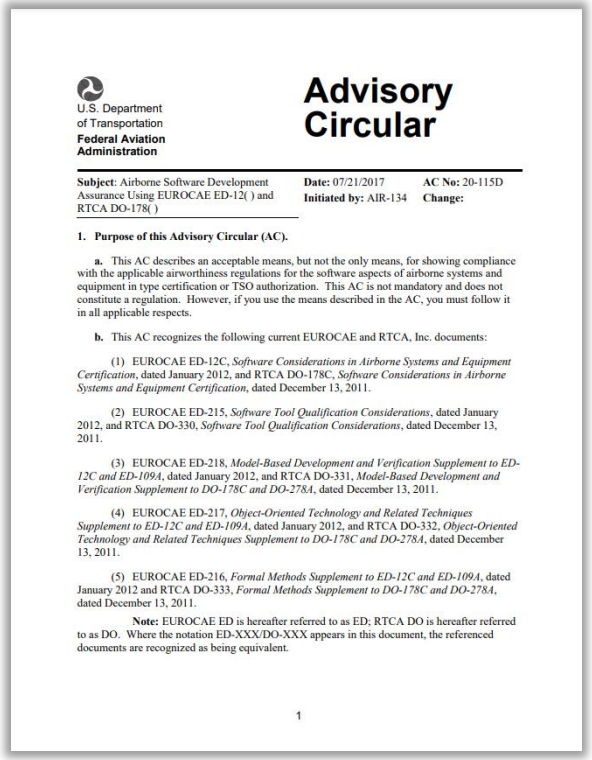
"Airborne Software Development Assurance Using EUROCAE ED-12( ) and RTCA DO-178( )"

Paragraph 6

"ED-12C/DO-178C is an acceptable means of compliance for the software aspects of type certification or TSO authorization."

Notes:

- ED-12C = DO-178C
- EUROCAE & RTCA co-developed these standards
- AC also provides guidance on when DO-178B / ED-12B is allowed



U.S. Department of Transportation
Federal Aviation Administration

Advisory Circular

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

Date: 07/21/2017 **AC No:** 20-115D
Initiated by: AIR-134 **Change:**

1. Purpose of this Advisory Circular (AC).

a. This AC describes an acceptable means, but not the only means, for showing compliance with the applicable airworthiness regulations for the software aspects of airborne systems and equipment in type certification or TSO authorization. This AC is not mandatory and does not constitute a regulation. However, if you use the means described in the AC, you must follow it in all applicable respects.

b. This AC recognizes the following current EUROCAE and RTCA, Inc. documents:

(1) EUROCAE ED-12C, *Software Considerations in Airborne Systems and Equipment Certification*, dated January 2012, and RTCA DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*, dated December 13, 2011.

(2) EUROCAE ED-215, *Software Tool Qualification Considerations*, dated January 2012, and RTCA DO-330, *Software Tool Qualification Considerations*, dated December 13, 2011.

(3) EUROCAE ED-218, *Model-Based Development and Verification Supplement to ED-12C and ED-109A*, dated January 2012, and RTCA DO-331, *Model-Based Development and Verification Supplement to DO-178C and DO-278A*, dated December 13, 2011.

(4) EUROCAE ED-217, *Object-Oriented Technology and Related Techniques Supplement to ED-12C and ED-109A*, dated January 2012, and RTCA DO-332, *Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A*, dated December 13, 2011.

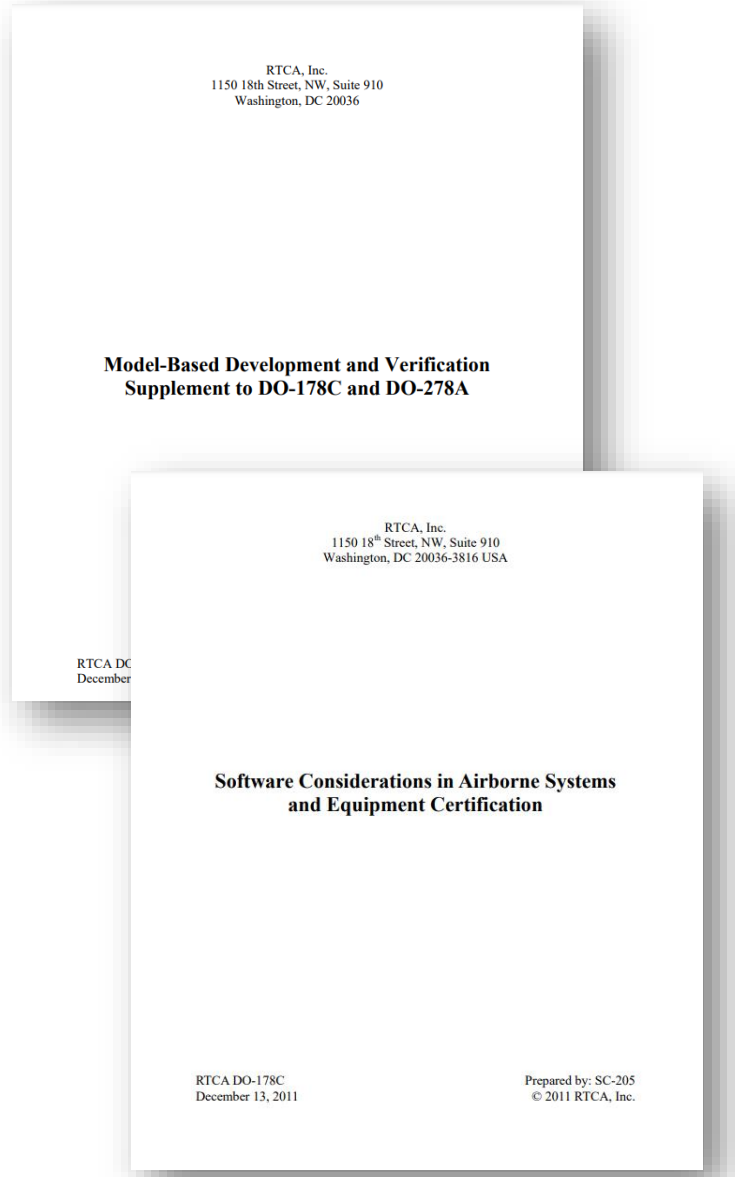
(5) EUROCAE ED-216, *Formal Methods Supplement to ED-12C and ED-109A*, dated January 2012 and RTCA DO-333, *Formal Methods Supplement to DO-178C and DO-278A*, dated December 13, 2011.

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

1

DO-178C

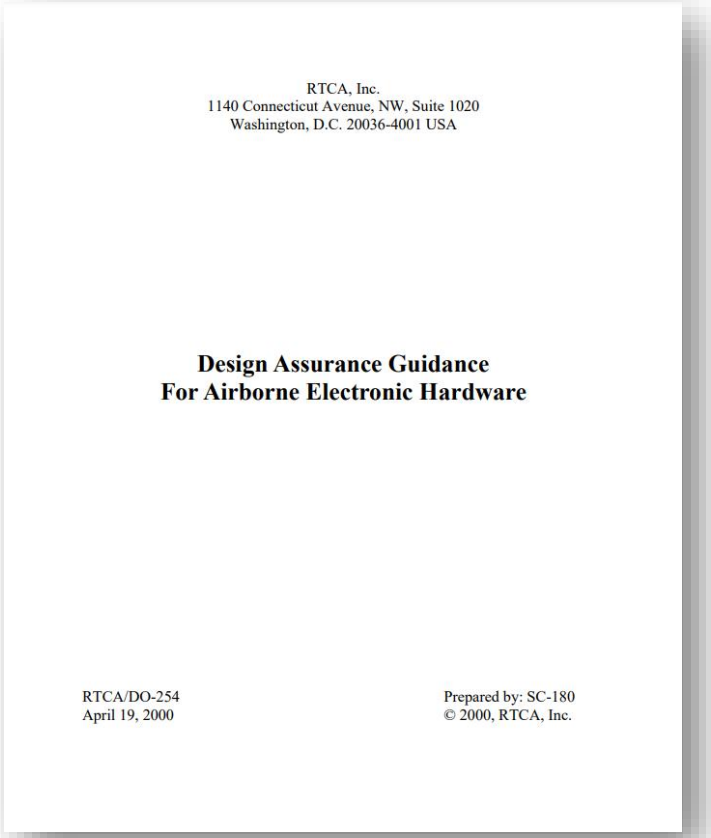
- Defines development objectives to be satisfied i.e. the things the development process must do
- Objectives cover
  - Software Requirements
  - Software Design
  - Software Coding
  - Requirements Coverage Testing
  - Source Code Coverage Testing
- There are also Objectives for the “Integral Processes”
  - Quality Assurance,
  - Configuration Management, and
  - Certification Liaison
- There are 5 Levels corresponding to the 5 Design Assurance Levels (Part 25 & 29):
  - DAL-E - No Effect => 0 objectives
  - DAL-A - Catastrophic => 71 objectives
- Objectives can be modified depending on the technologies used:
  - DO-331 – Model Based Development
  - DO-332 – Object Oriented Technologies
  - DO-395 – COTS Software (in development)



Airborne Electronic Hardware Certification

DO-254 – Development Assurance Standard for Hardware

- Typically complex electronic devices that can exist in multiple states at any one time.
- Not an environmental standard
- Original intent is to block “Software by Stealth” whereby developers were building functionality into micro coded devices (i.e. FPGAs, ASIC)
- Similar concepts to DO-178C
  - Developed by many of the same people
  - Defines Process objectives
  - Different objectives for different DALs


RTCA, Inc.
1140 Connecticut Avenue, NW, Suite 1020
Washington, D.C. 20036-4001 USA

Design Assurance Guidance
For Airborne Electronic Hardware

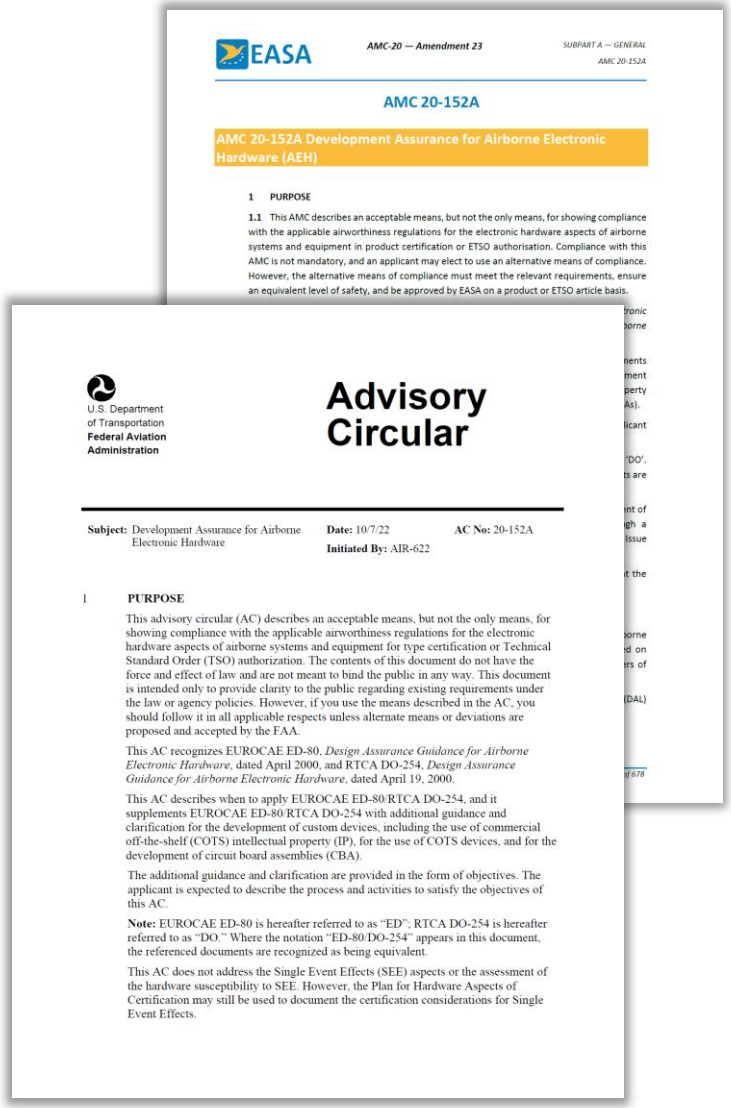
RTCA/DO-254
April 19, 2000

Prepared by: SC-180
© 2000, RTCA, Inc.

Simple Hardware Item - A hardware item is considered simple if a comprehensive combination of deterministic tests and analyses can ensure correct functional performance under all foreseeable operating conditions with no anomalous behavior.

AC 20-152A

- Defines additional objectives to be used with DO-254.
- Jointly developed with EASA
- Re-defines Simple/Complex
- Guidance material
  - EASA Appendix B to AMC 20-152A,
  - FAA AC 00-79
- Guidance Material includes examples on when COTS components are Simple or Complex.



Wrap Up

Technical Notes

- It is (generally) not possible to prove that Software is free from error.
- DO-178/254 are frequently viewed as acceptable means of compliance.
- DO-178/254 define objectives the development processes must achieve.
- Certification is based on processes being:
  - defined,
  - approved, and
  - followed.
- Design Control Systems needs to support the development processes, and retention of process evidence.

Why does Beca have an ADO?

- Business Opportunity
  - Part of the NZ advanced aerospace sector
  - Merlin Labs NZ was the catalyst

- Market Factors
  - We expect there will be an increased demand for technology in aircraft
  - Foreign companies are coming to NZ for R&D programs
  - Levers the software capability developed in support of NZDF Military Programs
  - Provide a national capability
  - Follow the bouncing ball:
    - Operational concept -> operational certificates ->airworthiness standards -> method of compliance

Questions