AEROSPACE CANON

2026-03-18

Dexter Hadley, MD/PhD

Hadley Lab CANONIC

Abstract

Example

Contents

All airborne software MUST be developed and verified according to DO-178C objectives at the assigned Design Assurance Level.

Example: DO-178C (Software Considerations in Airborne Systems and Equipment Certification) defines five Design Assurance Levels based on failure condition severity: DAL A (catastrophic loss of aircraft, e.g., flight control law software), DAL B (hazardous/severe-major large reduction in safety margins, e.g., engine FADEC), DAL C (major significant reduction in safety margins, e.g., navigation display), DAL D (minor slight reduction, e.g., maintenance logging), DAL E (no effect no safety impact, e.g., passenger entertainment). Software lifecycle: planning development (requirements, design, coding, integration) verification configuration management quality assurance. Objectives by level: DAL A = 71 objectives (33 with independence), DAL B = 69 objectives (18 with independence), DAL C = 62 objectives (5 with independence), DAL D = 26 objectives (2 with independence). Independence requirement: DAL A/B verification activities must be performed by personnel not involved in development. Technology supplements: DO-332 (OOT), DO-333 (formal methods), DO-330 (tool qualification TQL 1-5). MAGIC gate: bitwise AND of required DAL dimensions before flight-critical software release.

0.1 2. Hardware Assurance

All airborne electronic hardware MUST be developed and assured according to DO-254 with appropriate design assurance.

Example: DO-254 (Design Assurance Guidance for Airborne Electronic Hardware) applies to custom micro-coded components: FPGAs, ASICs, PLDs, and complex COTS components. Design assurance levels mirror DO-178C (DAL A-E). Hardware lifecycle: planning requirements capture conceptual design detailed design implementation production transition certification liaison. FPGA-specific concerns: single-event upsets (SEU) from cosmic radiation DAL

A/B requires SEU mitigation (TMR, ECC, scrubbing). SEU rate analysis per JEDEC JESD89A. COTS components: complex COTS (processors, FPGAs with embedded IP) require additional assurance activities per AC 20-152. Hardware/software interface (HSI): shared resources (memory, I/O, interrupts) must be documented and verified. Errata management: silicon errata tracking and impact assessment for all DAL A-C designs. Design assurance process: requirements design verification (simulation, formal verification, bench testing, environmental testing per DO-160G).

0.2 3. Cybersecurity

Airborne systems and networks MUST be protected against intentional unauthorized electronic interactions.

Example: DO-326A (Airworthiness Security Process Specification) establishes security risk assessment process for aircraft systems. DO-356A (Airworthiness Security Methods and Considerations) provides security implementation guidance. Security risk assessment: threat source identification (nation-state, insider, opportunistic), attack vector analysis (maintenance ports, wireless interfaces, datalink, removable media), vulnerability assessment, threat scenario development, risk determination (likelihood Œ impact). Aircraft domains: Aircraft Control Domain (ACD flight critical), Airline Information Services Domain (AISD), Passenger Information and Entertainment Domain (PIED). Network security: ARINC 664 Part 7 (AFDX deterministic Ethernet), network segregation, data flow monitoring. EWIS (Electrical Wiring Interconnection System): physical security of wiring against tampering. Ground-to-aircraft datalink security: ACARS, ADS-B (unencrypted vulnerability), SATCOM. Security event logging and incident response per operator security program. Integration with DO-178C/DO-254: security requirements allocated to SW/HW with appropriate DAL.

0.3 4. System Safety

Aircraft systems MUST undergo systematic safety assessment to identify, classify, and mitigate failure conditions.

Example: ARP4754A (Guidelines for Development of Civil Aircraft and Systems) defines system development lifecycle: aircraft-level FHA system-level FHA allocation of safety requirements system design system verification system validation. ARP4761 (Guidelines and Methods for Conducting the Safety Assessment Process): Functional Hazard Assessment (FHA) identifies failure conditions and classifies severity (catastrophic, hazardous, major, minor, no safety effect). Fault Tree Analysis (FTA) top-down deductive analysis of failure events to determine probability. Failure Mode and Effects Analysis (FMEA) bottom-up inductive analysis of component failures. FMECA adds criticality assessment. Common Cause Analysis (CCA): Zonal Safety Analysis (ZSA), Particular Risks Analysis (PRA), Common Mode Analysis (CMA). Probability targets: catastrophic < 10ˆ-9 per flight hour, hazardous < 10ˆ-7, major < 10ˆ-5. Markov analysis for state-dependent failure rates. Dependence diagrams for reliability modeling. Safety assessment feeds directly into DAL assignment per ARP4754A.

0.4 5. Quality Management

Aerospace organizations MUST maintain quality management systems with industry-specific requirements for product safety and reliability.

Example: AS9100D:2016 (Quality Management Systems Requirements for Aviation, Space and Defense Organizations) extends ISO 9001 with aerospace requirements: product safety (clause 8.1.1), counterfeit part prevention (clause 8.1.4), risk management (clause 8.1.1), configuration management (clause 8.1.6), first article inspec-

tion (clause 8.5.1.3). AS9102 (Aerospace First Article Inspection Requirements): Form 1 (Part Number Accountability), Form 2 (Product Accountability Raw Material, Special Process, Functional Testing), Form 3 (Characteristic Accountability each dimension, tolerance, measured value). AS9145 (Requirements for Advanced Product Quality Planning and Production Part Approval Process): APQP phases plan, product design, process design, product/process validation, feedback/corrective action. NADCAP (National Aerospace and Defense Contractors Accreditation Program): special process accreditation for welding, heat treating, chemical processing, NDT, coatings, composites, electronics, materials testing. ODA (Organization Designation Authorization): FAA delegates certification functions to qualified organizations.

0.5 6. Certification

Aircraft, engines, and components MUST obtain appropriate certification from aviation authorities before operational use.

Example: Type Certificate (TC): FAA Part 21 Subpart B (type certification procedures), EASA Part 21 Subpart B. Certification basis: FAR Part 23 (normal category up to 19 passengers), Part 25 (transport category), Part 27 (normal rotorcraft), Part 29 (transport rotorcraft), Part 33 (aircraft engines), Part 35 (propellers). EASA equivalents: CS-23, CS-25, CS-27, CS-29, CS-E, CS-P. Supplemental Type Certificate (STC): modification to existing type design separate approval process per Part 21 Subpart E. Technical Standard Order (TSO): minimum performance standards for specified articles TSOA (TSO Authorization) allows production. Parts Manufacturer Approval (PMA): Part 21 Subpart K allows production of replacement parts. Certification process: type certification basis compliance planning showing of compliance (analysis, test, inspection, simulation) Type Inspection Authorization (TIA) flight testing type certificate issuance. Special conditions for novel designs (e.g., eVTOL, urban air mobility). Issue Paper process for certification challenges. DER (Designated Engineering Representative) and DAR (Designated Airworthiness Representative) support FAA findings.

---

1. Constraints

```
MUST:     Cite DO-178C, DO-254, ARP4754A/4761, or doma
MUST:     Map Design Assurance Level to MAGIC checkset
MUST:     Distinguish between commercial, military, sp
MUST NOT: Present uncertified software as airworthy at
```

AEROSPACE | *CANON* | *VERTICALS*