

**Aircraft Electronics:
Safety Assurance in Product
Design/Development/Certification
and
Methods for Monitoring and Evaluating
Safety Performance
Aircraft Electronics**

Tom Fancy

November 16, 2010



Agenda

- Brief Biography
- Gulfstream Overview
- Critical Aircraft Systems
- Design Process – Requirements
- Criticality Definitions
- Failure Rates & Design Assurance Levels (DAL)
- Safety Related Requirements
- Requirements Flow
- Software & Complex Electronic Hardware Design
- Environmental Testing
- HIRF & Lightning
- Certification Approval

Tom Fancy

- Technical Fellow Gulfstream Aerospace
 - Responsible for all electronic, software, CEH, and Safety design for Gulfstream aircraft
- 31 years in Aerospace
- 27 years as FAA Designated Engineering Representative
 - Delegated for Systems and Equipment, Electrical, Electronics, System Safety, HIRF(EMI)/Lightning, Software, and Complex Electronic Hardware
- 19 years Gulfstream Aerospace
 - Design Build Team Lead for GV, GV-SP
 - Design Integrity Manager for GIV-X
 - Staff position for all Gulfstream aircraft

Gulfstream

- Manufacturer Business Jets
- Customers are companies, individuals, and governments
- Mid Size cabin jets
 - G150 6-8 Pass 3,000 nm
 - G200 8-10 Pass 3,400 nm
 - G250 in flight test 8-10 Pass 3,400 nm
- Large Cabin
 - G350 12-16 Pass 3,800 nm
 - G450 12-16 Pass 4,350 nm
 - G550 14-18 Pass 6,750 nm
 - G650 in flight test 14-18 Pass 7,000 nm

Critical Aircraft Systems

- Fly by Wire
- Air Data System
- Primary Flight Displays
- Electric Power System
- Engine Controls
- Monitor Warning System (CAS)

Design Process - Requirements

- Code of Federal Regulations (CFR)
 - Provides top level guidance and requirements to meet FAA standards
- Functional Hazard Assessment (FHA)
 - Used to determine system criticality and design assurance
- System Safety Analysis
 - Assures the design meets all safety requirements
- Aircraft Design Requirements
 - Defines aircraft operational and performance requirements
 - System and component level requirements are flowed to suppliers

Criticality Definitions

- Catastrophic
 - Failure conditions which would prevent continued safe flight and landing.
- Hazardous/Severe-Major
 - Failure conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be:
 - (1) a large reduction in safety margins or functional capabilities,
 - (2) physical distress or higher workload such that the flight crew could not be relied on to perform their tasks accurately or completely, or
 - (3) adverse effects on occupants including serious or potentially fatal injuries to a small number of those occupants.
- Major
 - Failure conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to occupants, possibly including injuries.

Criticality Definitions (cont.)

- Minor
 - Failure conditions which would not significantly reduce aircraft safety, and which would involve crew actions that are well within their capabilities. Minor failure conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as, routine flight plan changes, or some inconvenience to occupants.
- No Effect
 - Failure conditions which do not affect the operational capability of the aircraft or increase crew workload.

Failure Rates & Design Assurance Levels (DAL)

Hazard Level	Failure rate	DAL
Catastrophic	1.0E-9/hour	A
Hazardous/Severe-Major	1.0E-7/hour	B
Major	1.0E-5/hour	C
Minor	1.0E-3/hour	D
No Effect		E

Safety Related Requirements

- Hazards are assessed across system/systems
 - Hazard maybe mitigated by architecture
 - Reduced failure rates or DAL requirements for components or sub-systems
 - Redundancy covers failure rate requirements but not similar SW
- Safety Related Requirements
 - Tracked separately or flagged
 - Verified at various levels
 - Tracked to assure all safety related requirements are verified

Requirements Flow

SAE

ARP4754a

- 26 -

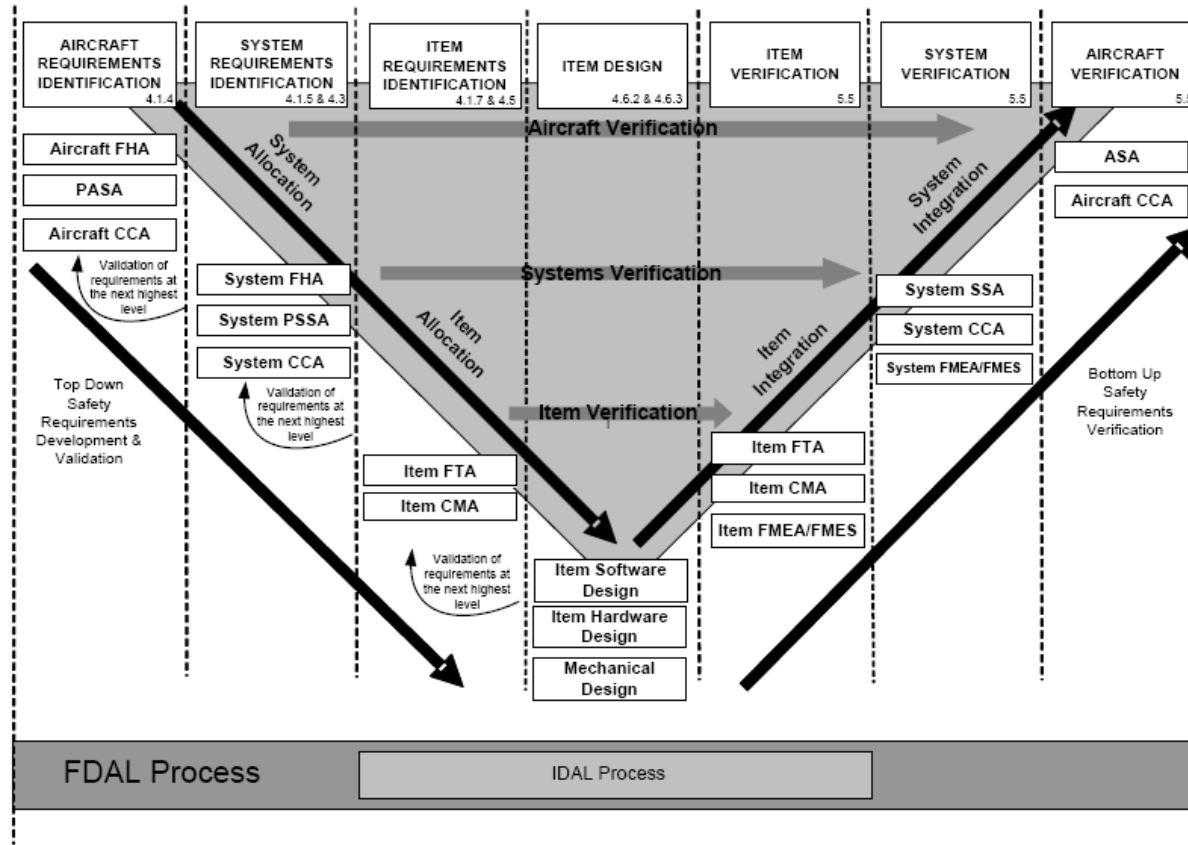


Figure 4-3 Relationship between Requirement Levels, FDAL and IDAL

Software & Complex Electronic Hardware Design

- RTCA DO-178B
 - Accepted guidance for developing SW
 - Defines process, independence, artifacts, verification, validation required for each DAL
 - Process is audited by FAA and/or DER's
 - DO-178B relies more on a rigorous process and independent reviews than testing to obtain the DAL
- RTCA DO-254
 - Accepted guidance for developing CEH
 - Similar approach used for CEH as SW
 - Different verification and validation techniques

Environmental Testing

- RTCA DO-160x
 - Accepted guidance for conducting environmental testing
 - Environment defined by categories
 - Test environment category selected by location in airplane
 - Test environment represents expected environment equipment will see
 - Temperature, vibration, humidity, altitude, etc.

HIRF & Lightning

- System and component test levels determined by aircraft characteristics
- HIRF (High Intensity Radiated Fields)
 - HIRF environments are defined by regulation for frequency vs field strength
 - Airplane is radiated at lower levels to measure the attenuation and induced cable currents
 - Each critical system is tested to the full field strength minus the aircraft attenuation plus margin in a test chamber
 - Essential systems are tested to reduced levels

HIRF & Lightning (cont.)

- Lightning
 - Waveforms and Volt-Amps are defined by regulation
 - Airplane this tested with low level waveforms to determine induced voltages and currents on cables
 - Each critical or essential system is tested to the induced full strength levels plus margin in a test chamber
 - Pass/fail criteria is different for critical and essential systems

Certification Approval

- All aircraft design, and safety related requirements are reviewed to assure each one is verified and tested
 - Includes requirement flowed down to suppliers
- Verification data is reviewed against the 14 CFR 25.xxxx to assure all FAA requirements are verified
- FAA and DER's review these results
- Any in service changes require a Change Impact Analysis to define the effort required to certify the change
 - The same process is used as for initial certification

Questions