Avionics Certification

Dhruv Mittal

Motivation

- Complex Avionics systems have been regulated for a long time
- Autonomous systems are being researched and built in avionics right now
- Research in avionics is often driven/overseen by the US Air Force, and confronts the problems of certification directly
- There's not an analogous organization for automotive, so we can look to avionics for a model

Current Certifications & Process

- Focus on safety critical hardware and software
- Focus on development processes
- Standards provided by organizations like SAE International and RTCA

SAE International

- Society of Automotive Engineers
- Coordinates the development of technical standards based on best practices
  - Task forces of engineering professionals create the standards
  - Since 1915, when they standardized the different lock washers and steel tubing used in the automotive industry

ARP4754

Guidelines for Development of Civil Aircraft and Systems

- Whole lifecycle for systems that implement aircraft functions aka communications, navigation, monitoring, flight-control, collision-avoidance

- “This document discusses the certification aspects of highly-integrated or complex systems installed on aircraft, taking into account the overall aircraft operating environment and functions. The term "highly-integrated" refers to systems that perform or contribute to multiple **aircraft-level functions**. The term "complex" refers to systems whose safety **cannot be shown solely by test and whose logic is difficult to comprehend without the aid of analytical tools**.”

ARP4761

Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment

- Guidelines for conducting a safety assessment
    - Functional Hazard Assessment - Determine possible failure conditions & severity (probability bounds and assurance levels)
    - Preliminary System Safety Assessment - Determine how failures can arise
    - System Safety Assessment - Verify that failure conditions are acceptable (probability bounds)

ARP4761 SSA Chart

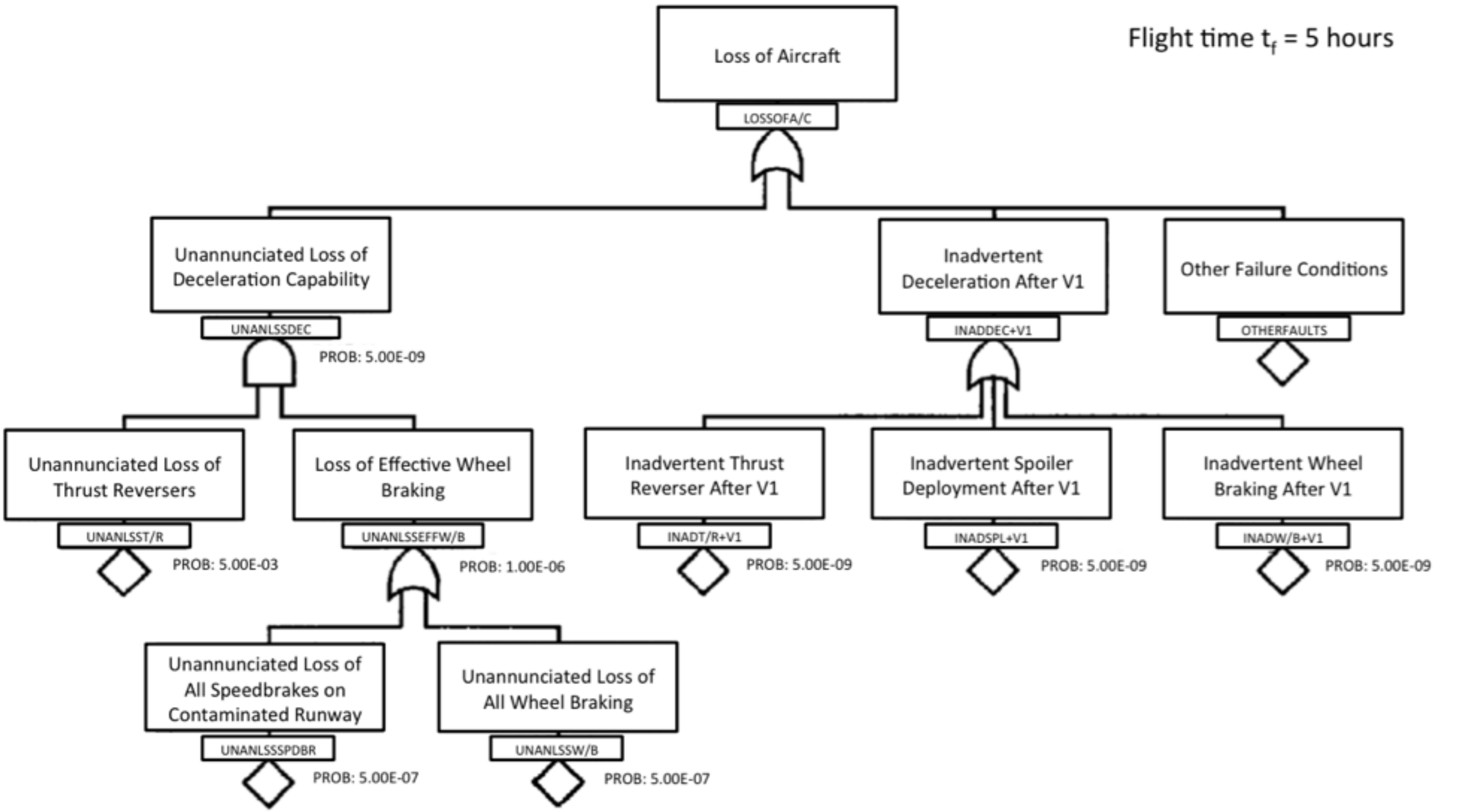
Probability (Quantitative)	1.0 1.0E-5	1.0E-5 1.0E-7	1.0E-7 1.0E-9	1.0E-9
Probability (Descriptive)	Probable	Improbable		Extremely Improbable
Failure Severity	Minor	Major	Severe Major	Catastrophic
Failure Effect	• Slight reduction in safety margins • Slight increase in crew workload • Some inconvenience to occupants	• Significant reduction in safety margins or functional capabilities • Significant increase in crew workload or conditions impairing crew efficiency • Some discomfort to occupants	• Large reduction in safety margins or functional capabilities • Significant increase in crew workload or conditions impairing crew efficiency • Some discomfort to occupants	• All failure conditions that prevent continued safe flight and landing
Development Assurance Level	Level D	Level C	Level B	Level A

SAE, “ARP4761 – Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment,” 1996.

ARP4761 (tools)

- Fault Tree Analysis
- Dependence Diagram
- Markov Analysis
- Failure Modes and Effect Analysis
- Common Cause Analysis

FHA via Fault Tree Analysis

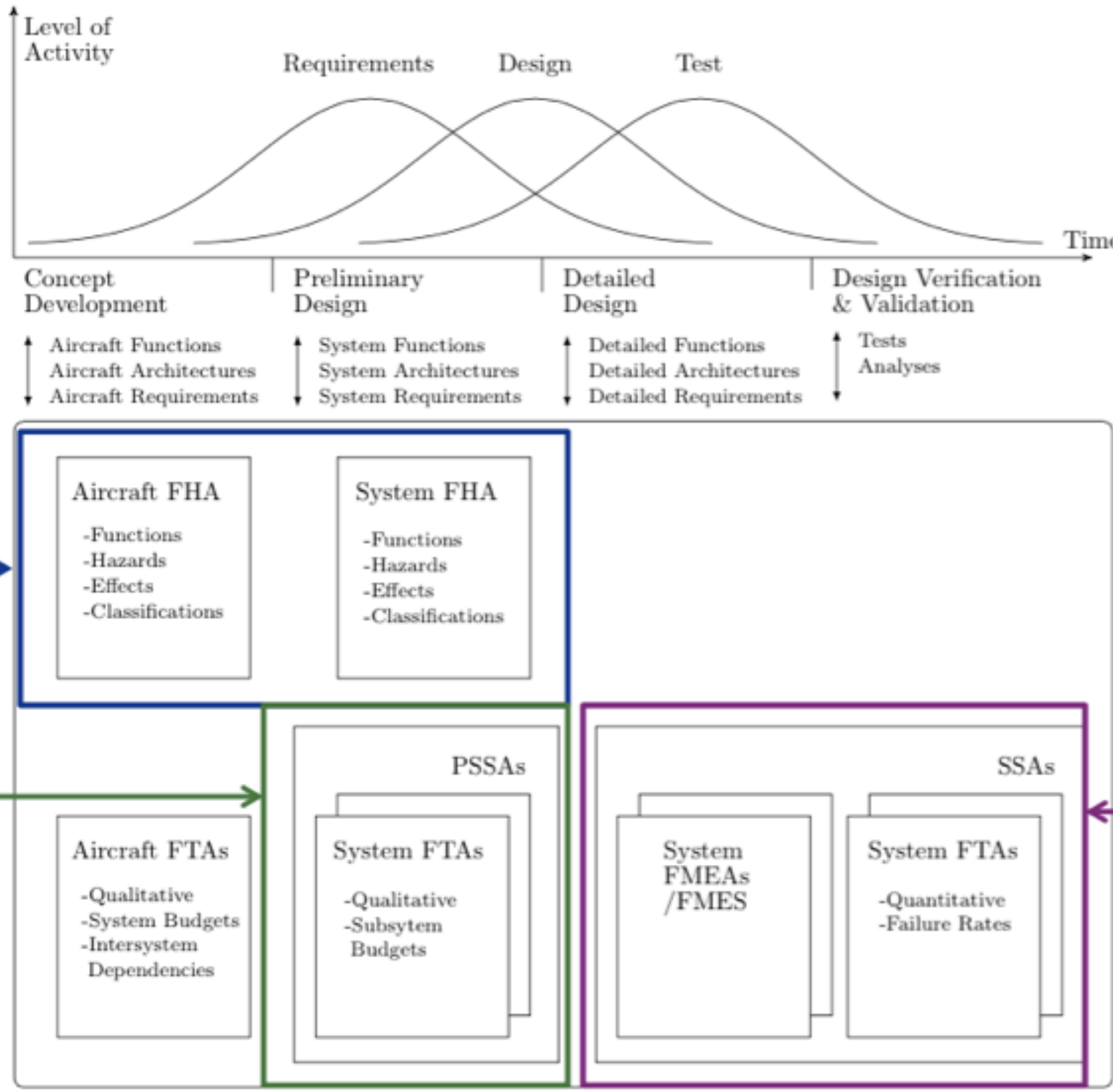


SAE, "ARP4761 – Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," 1996.

Safety Assessment Process

Functional Hazard Analysis (System level) – Identify what failure conditions are possible, classifications

Preliminary System Safety Assessment (Architecture level) – Identify how failures from FHA can arise



System Safety Assessment (Implementation level) – Show how safety objectives from FHA and PSSA are met

SAE, "ARP4761 – Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," 1996.

RTCA

- Radio Technical Commission for Aeronautics
- Private not-for-profit corporation
- develops technical guidance for use by government regulatory authorities & industry
- advisory body to the FAA

DO-178B/C

- Software Considerations in Airborne Systems and Equipment Certification
- Supplements:
  - DO-330: Software Tool Qualification Considerations
  - DO-331: Model-Based Development and Verification
  - DO-332: Object-Oriented Technology and Related Techniques
  - **DO-333: Formal Methods**

DO-178C

- Assumes that SSA has been performed on all software components
- Guides objectives for planning, development
- Explains how to
    - Develop software requirements and architecture from system requirements
    - Select processes, methods, tools, and error prevention methods for development
    - Select verification methods and test environments

DO-178C (cont)

- Sets up very specific requirements for software planning/development:
  - Defines software standards and environment
    - languages, compilers, IDEs, version control, verification tools/techniques, test environment
- Decreases subjectivity across the entire development and verification process

M.S. Reddy,“The Impact of TRCA DO-178C on Software Development”, Cognizant 20-20 insights, 2012

Current Certification Process for Avionics

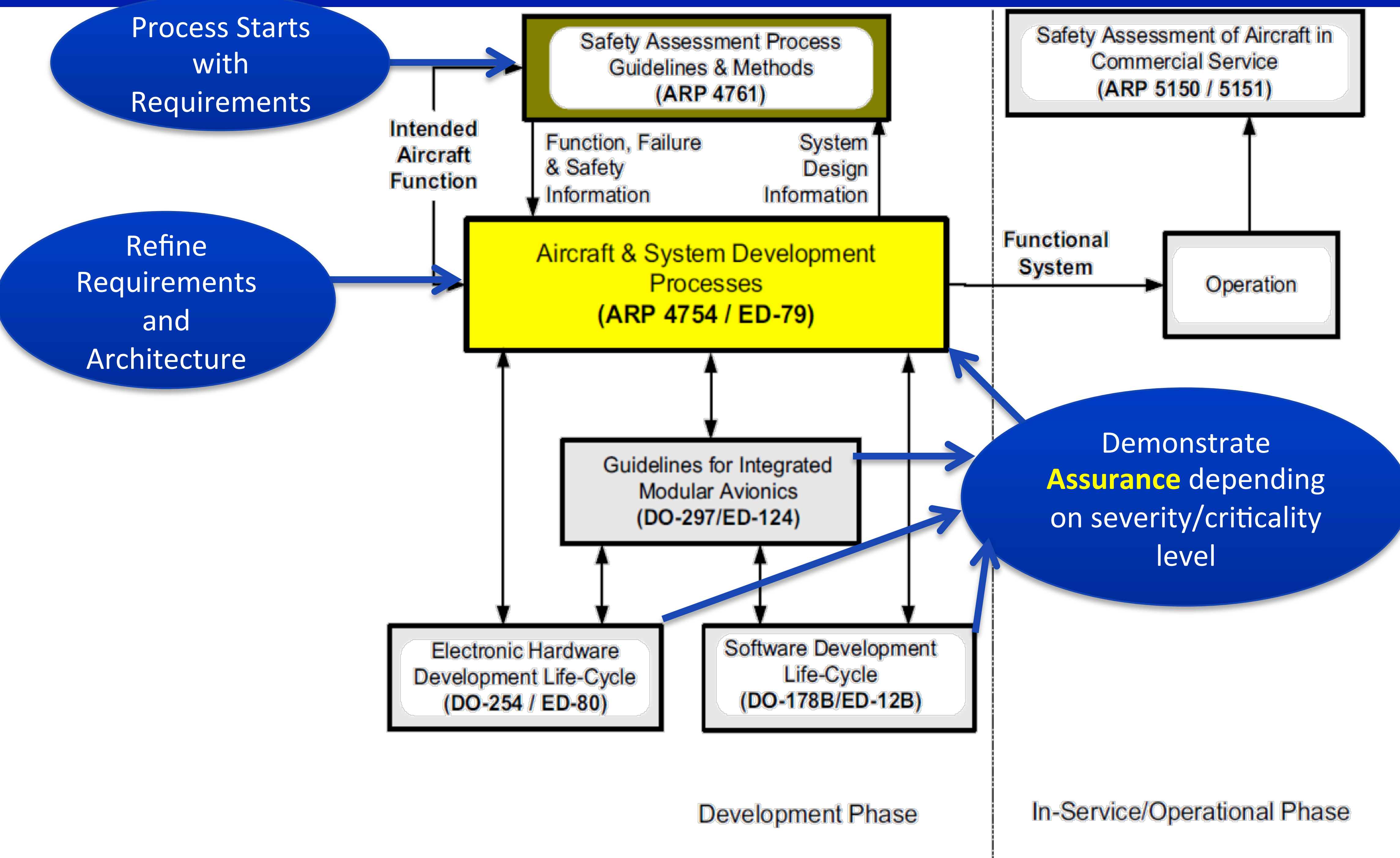


FIGURE 1 - GUIDELINE DOCUMENTS COVERING DEVELOPMENT AND IN-SERVICE/OPERATIONAL PHASES

L. Humphrey, "Certification and Design Challenges for Autonomous Systems", 2014

Autonomy

- AFRL Definition: “Systems that have a set of ‘intelligence-based’ capabilities that allow them to respond to situations in uncertain environments by choosing from a set of potential actions.”
- FAA Definition: “Autonomous operations refer to any system design that precludes any person from affecting the normal operations of the aircraft”
- Hard to certify because:
    - large state-space of system actions
    - large, potentially unknown environment
    - interactions with other autonomous systems can result in unexpected behaviors
    - testing is intractable for large state-space
    - lack of standard in design and analysis methods

Current Efforts to Certify Autonomous Avionics

- “accommodation, integration, evolution”
- Incremental fielding of autonomy - like in automotive
- human-in-the-loop for foreseeable future

FAA, “Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap”, 2013

FAA Integration of UAS into NAS Roadmap

- UAS - Unmanned Aircraft Systems
- NAS - National Airspace System
- “Although research will continue, fully certified UA-based collision avoidance solutions **may not be feasible until the long-term** and are deemed to be a necessary component for full UAS NAS integration. This will include research on safe and efficient terminal airspace and ground operations, followed by **ground demonstrations of autonomous airfield navigation** and ATC interaction.” (2013)

Key Differences between Avionics & Automotive

- Systems are often simpler wrt. safety certifications
  - Don’t have to deal with road challenges (pedestrian detection, constantly changing conditions, etc) except for airfield nav. on the ground, where it’s the same problem.
  - Radar and other detection techniques already in use are pretty effective
  - Operated by professionals, not general consumers
  - Low interest in reducing cost due to relative pricing of aircraft