



# Software Verification under DO-178B

John Joseph Chilenski  
Associate Technical Fellow  
Airborne Software Engineering  
Boeing Commercial Airplanes

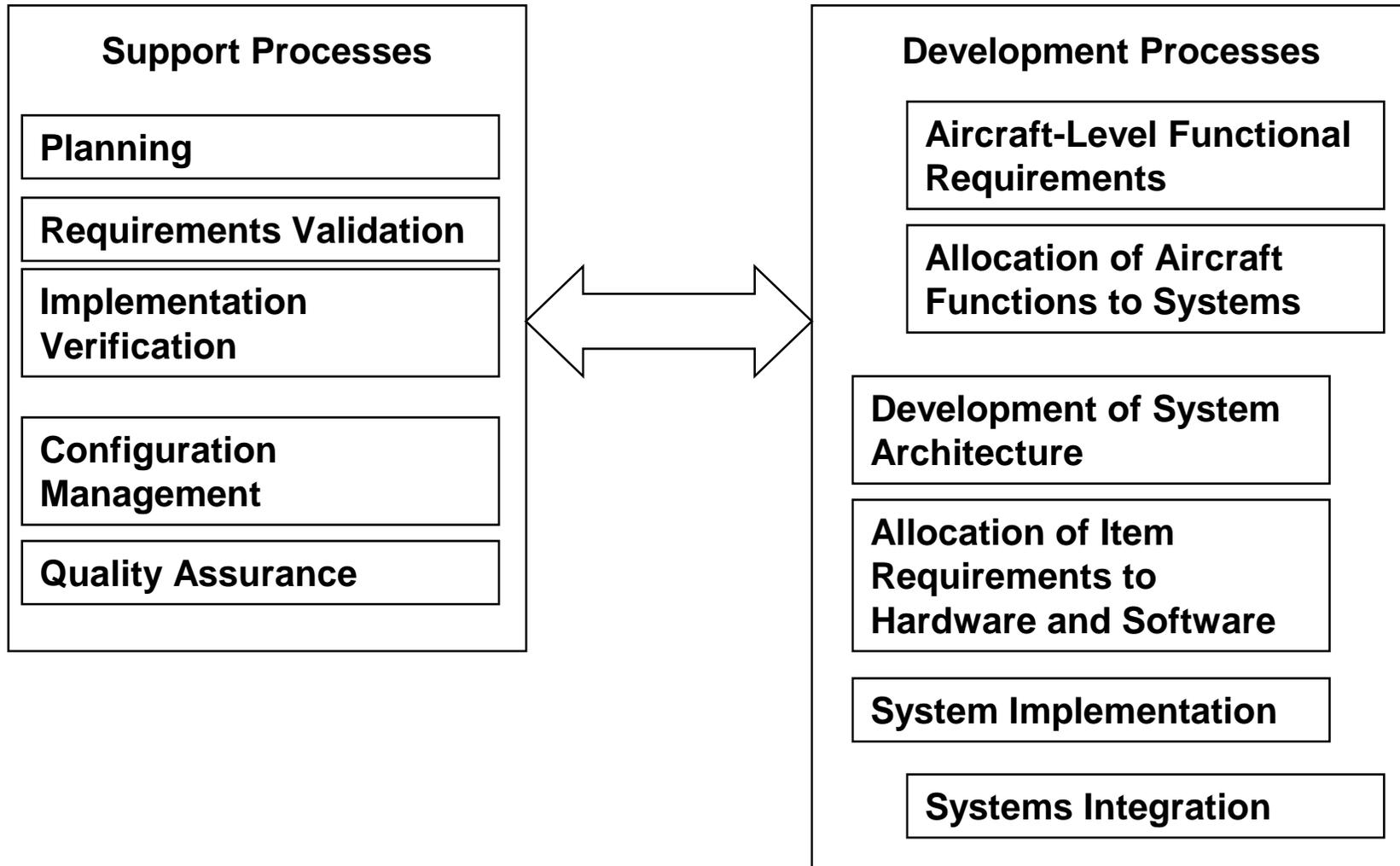
January 2002

# Agenda

- Development Process Model
- Software Lifecycle Processes
- Software Verification Process Framework
- Traceability Requirements
  - Coverage Analysis
  - Determinism
    - Predictability
    - Repeatability
- JAVA?

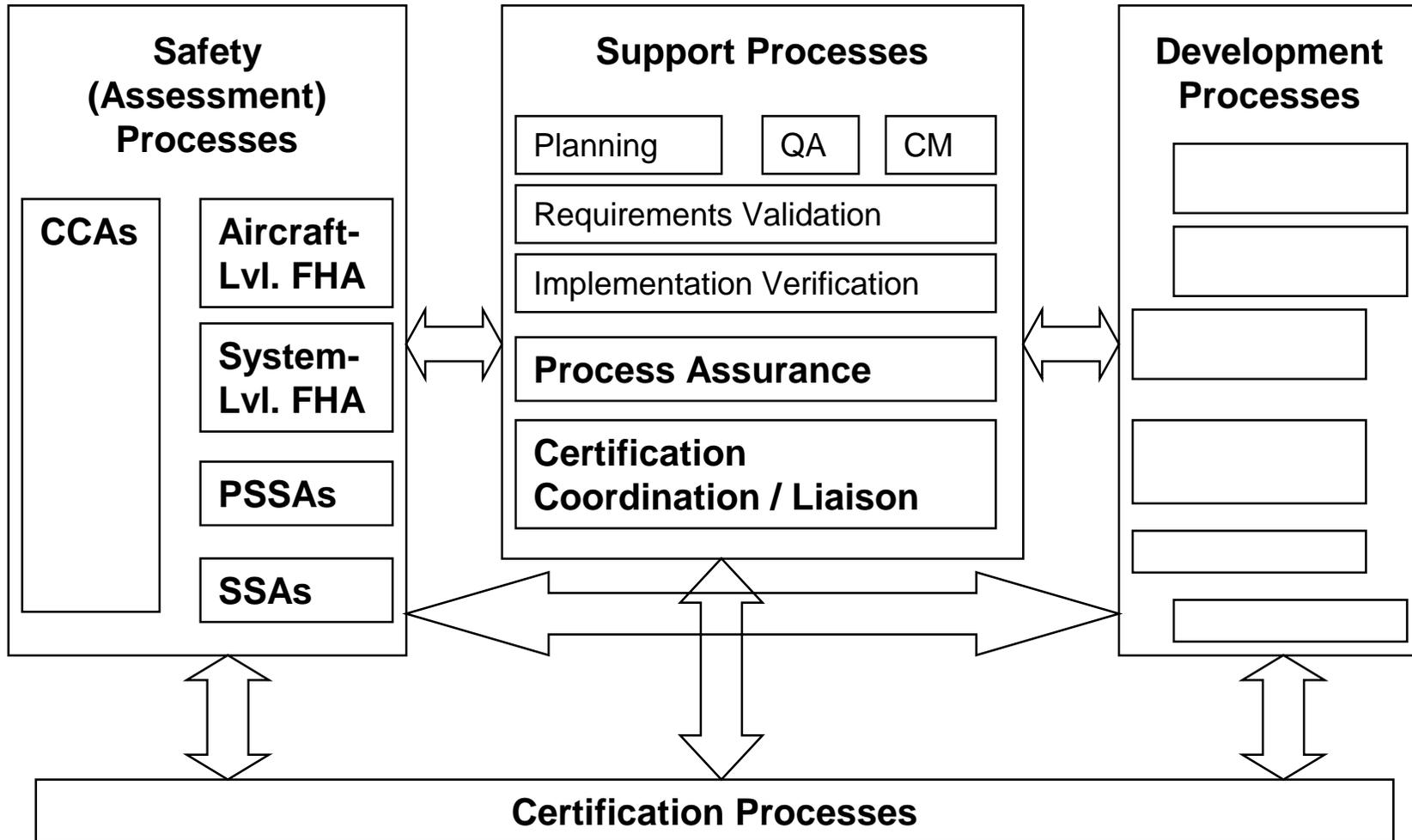
# Development Process Model

(1 of 3)



# Development Process Model

(2 of 3)



# Development Process Model

(3 of 3)

- In addition to Interaction and Feedback between Processes, some Processes impose Constraints upon other Processes
  - The Certification Process imposes constraints on all the other Processes
    - Especially the Verification Process
  - The Verification Process imposes constraints on most of the other Processes
    - Especially the Development Processes
    - If it can't be Verified, it can't be Used
      - Results in only a subset of Architectures, Designs and Implementations being Acceptable
- Traceability is very Extensive, and very Important, in the Safety Critical arena
  - Especially Traceability to Verification and the Safety Case

# Software Life Cycle Processes

Software Planning Process

Software Development Processes

Software  
Requirements  
Process

Software  
Design  
Process

Software  
Coding  
Process

Software  
Integration  
Process

Software Integral Processes

Software Verification Process

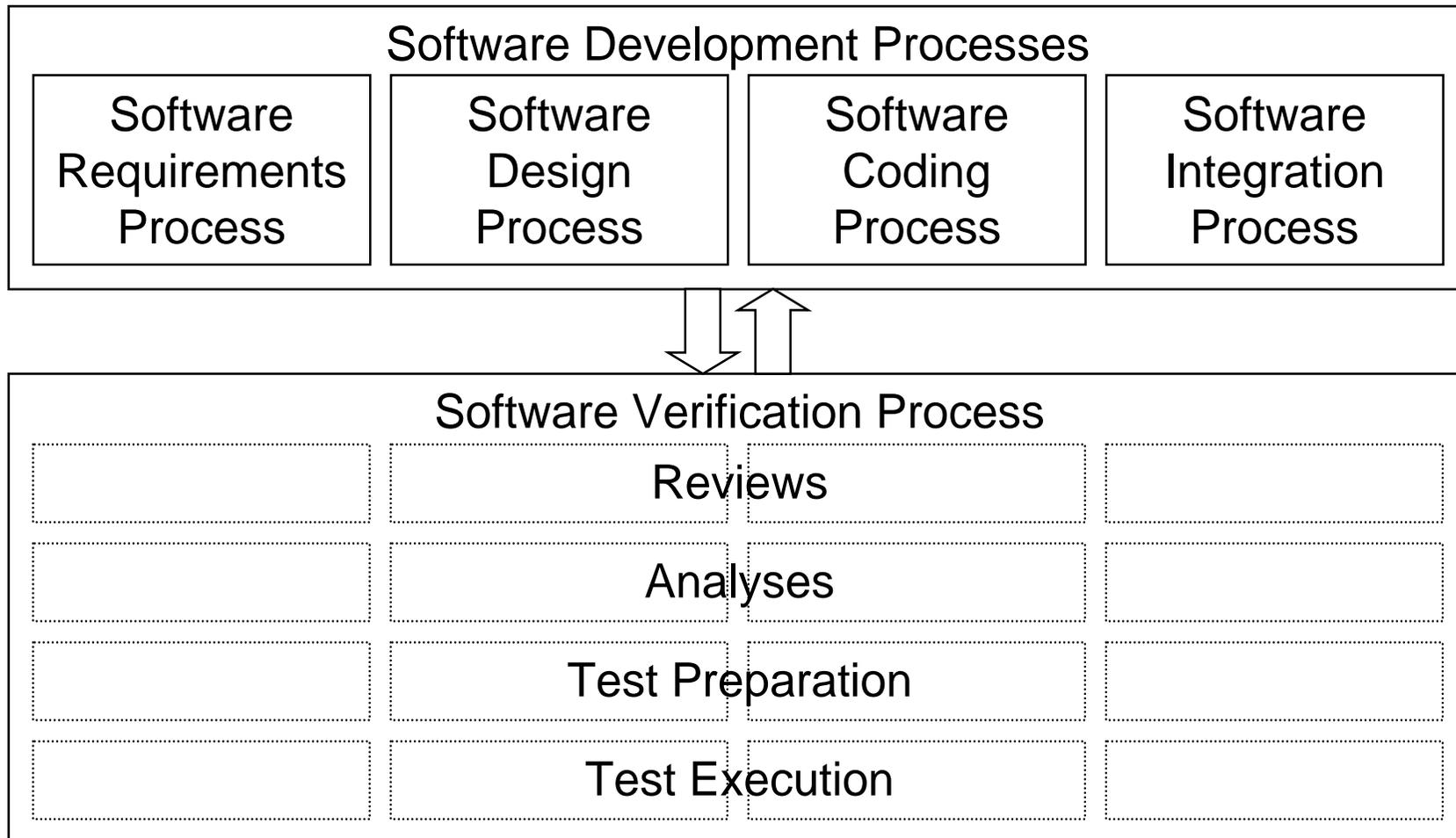
Software Configuration Management Process

Software Quality Assurance Process

Certification Liaison Process

# Software Verification Process Framework

(1 of 2)

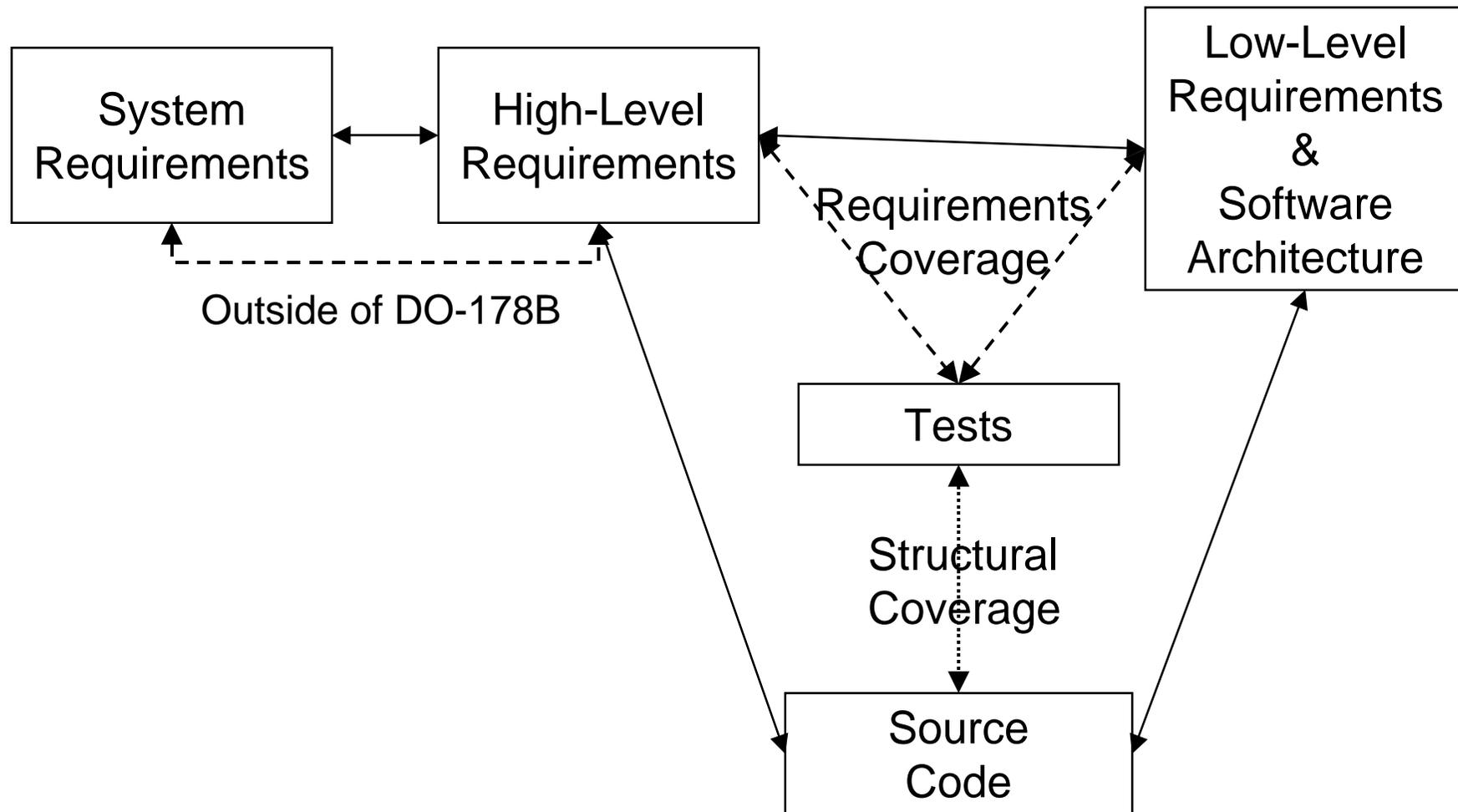


# Software Verification Process Framework

## (2 of 2)

- Reviews
  - Provide a qualitative assessment of correctness
- Analyses
  - Provide repeatable evidence of correctness
- Tests
  - Demonstrate that the software satisfies its high and low level requirements
  - Provide a high degree of confidence that errors which could lead to unacceptable failure conditions have been removed
- Extensive Verification required in the production of Safety-Critical Software

# Traceability Requirements



# Traceability - Coverage Analysis

## (1 of 2)

- Well defined way to (objectively) assess (i.e., measure) the quality of your System and Software Requirements (e.g., completeness, consistency, testability)
- Measure how well the Implementation reflects the Requirements
  - Requirements Coverage: Requirements  $\Leftrightarrow$  Tests
  - Structural Coverage: Tests  $\Leftrightarrow$  Source Code
- Objective completion criteria for the (System and Software) Testing Process
  - Determine how much Testing is enough
    - All Requirements (system and software) tested and verified
    - All Source Code exercised and verified
    - All Object Code exercised and verified (Level A only)

# Traceability - Coverage Analysis

## (2 of 2)

- Objective assessment of the adequacy of the (overall) Verification Process
  - All Requirements (system and software) implemented (satisfied) in (by) the resulting System
  - All Source Code implements the (software) Requirements
  - All Object Code implements the Source Code (Level A only)
  - Implementation of Requirements (system and software) is verified
- Helps with the identification of
  - Dead (“untest-able”) Code
  - Deactivated Code
  - Unspecified (“unintended”) Function
  - Unverified Function

# Traceability - Determinism

- Verification, Traceability and Coverage rely on Determinism
  - Every possible output for a given input can be verified correct
- Relies on Predictability and Repeatability
  - Predictability
    - Statically predict before hand what the system will do
    - Dynamically verify that the prediction is correct
  - Repeatability
    - Same thing happens every time
      - Execution
      - Memory
      - Timing

# JAVA?

- Everything is a Reference
  - Where is my data (memory location)?
  - Will it always be there?
- Garbage Collection / Dynamic Memory Management
  - When will it run?
  - How long will it take?
  - Will it compromise my data integrity?
- Dynamic Binding
  - How long will it take?
  - How much memory will it use?
  - Will I always go to the right place?