

# Merging Safety and Assurance: The Process of Dual Certification for FAA and the Common Criteria

Carol Taylor, Jim Alves-Foss , Bob Rinker  
University of Idaho  
Center for Secure and Dependable Systems

<http://www.csds.uidaho.edu/~jimaf>

# Comparison/Merger Goals

- Provide mapping between FAA guidelines and the Common Criteria (CC)
  - ◆ Detailed mapping between supporting sections of RTCA DO-178B and CC assurance criteria
  - ◆ Summary of “gaps” in the mapping
- Why compare and merge?
  - ◆ Dual use of embedded systems components/controllers
  - ◆ Security related failure conditions of avionic components
  - ◆ Overlap between certifications, save effort and COST

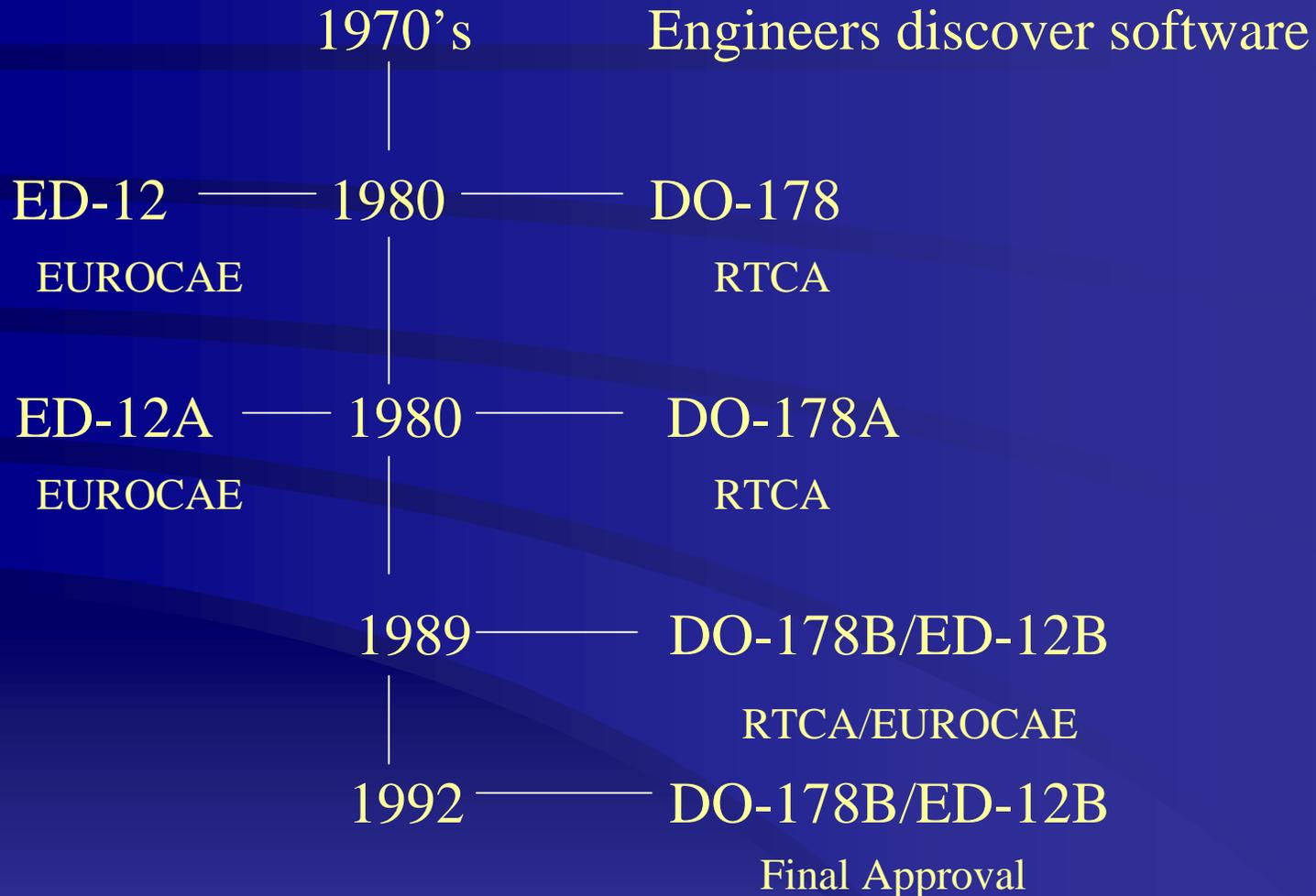
# Presentation Contents

- DO-178B
  - ◆ Overview
  - ◆ Software Failure Levels
- Common Criteria
  - ◆ Overview
  - ◆ Evaluation Assurance Levels EAL's
- Steps to Merging Certification
  - ◆ High-Level Comparison DO-178B Processes to CC Classes
  - ◆ Non-mapping CC Classes
  - ◆ FAA Certification/CC Certification
  - ◆ Merged Certification Process
- Conclusions

# DO-178B Overview

- DO-178B
  - ◆ FAA industry standard to establish software safety
  - ◆ Represents “best known” software practices
  - ◆ Compliance is done by meeting its intent since nothing is mandated
  - ◆ Other means can be used but they must conform to DO-178B standards

# DO-178B Overview



# DO-178B Overview

- DO-178B Processes for Software Development
  - ◆ *Software Planning*
    - define means of software production for system requirements
  - ◆ *Software Development*
    - requirements design, code and integrate
  - ◆ *Software Verification*
    - technical assessment of development

# DO-178B Overview

- DO-178B Processes for Software Development
  - ◆ *Software Configuration Management*
    - change control, baseline estimates and archive
  - ◆ *Software Quality Assurance*
    - assess software meets requirements, developed according to plan

# DO-178B Software Failure Levels

- Software Levels in DO-178B
  - ◆ Software level is correlated to the contribution of the software to the FAA failure conditions in aircraft.
  - ◆ The five levels range from



# DO-178B Software Failure Levels

- **Level A (Catastrophic)**
  - ◆ Failure conditions that prevent continued safe flight and landing.
- **Level B (Hazardous/Severe-Major)**
  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

# DO-178B Software Failure Levels

- **Level C (Major)**

- ◆ A significant reduction in safety margins or functional capabilities
- ◆ A significant increase in crew or in conditions impairing crew efficiency, or
- ◆ discomfort to occupants, possibly including injuries.

- **Level D (Minor)**

- ◆ no significant reduction in aircraft safety
- ◆ slight increase in crew workload, such as, routine flight plan changes
- ◆ some inconvenience to occupants

- **Level E (No Effect)**

- ◆ do not affect the operational capability of the aircraft or increase crew workload

# DO-178B Software Failure Levels

- Differences between certification requirements for the five failure levels focus on two issues:
  1. Software engineering processes that generate data/documents required to prove compliance with development standards and processes managing that data
  2. Independent vs. non-independent assessment of compliance with DO-178B requirements.

# DO-178B Software Failure Levels

- Two control processes for data classification
  - ◆ Control Category 1 (CC1)
    - More requirements
  - ◆ Control Category 2 (CC2)
    - Subset of CC1, has fewer requirements

These control processes include requirements for baselines, traceability, change control, change review, unauthorized changes protection, release and data retention

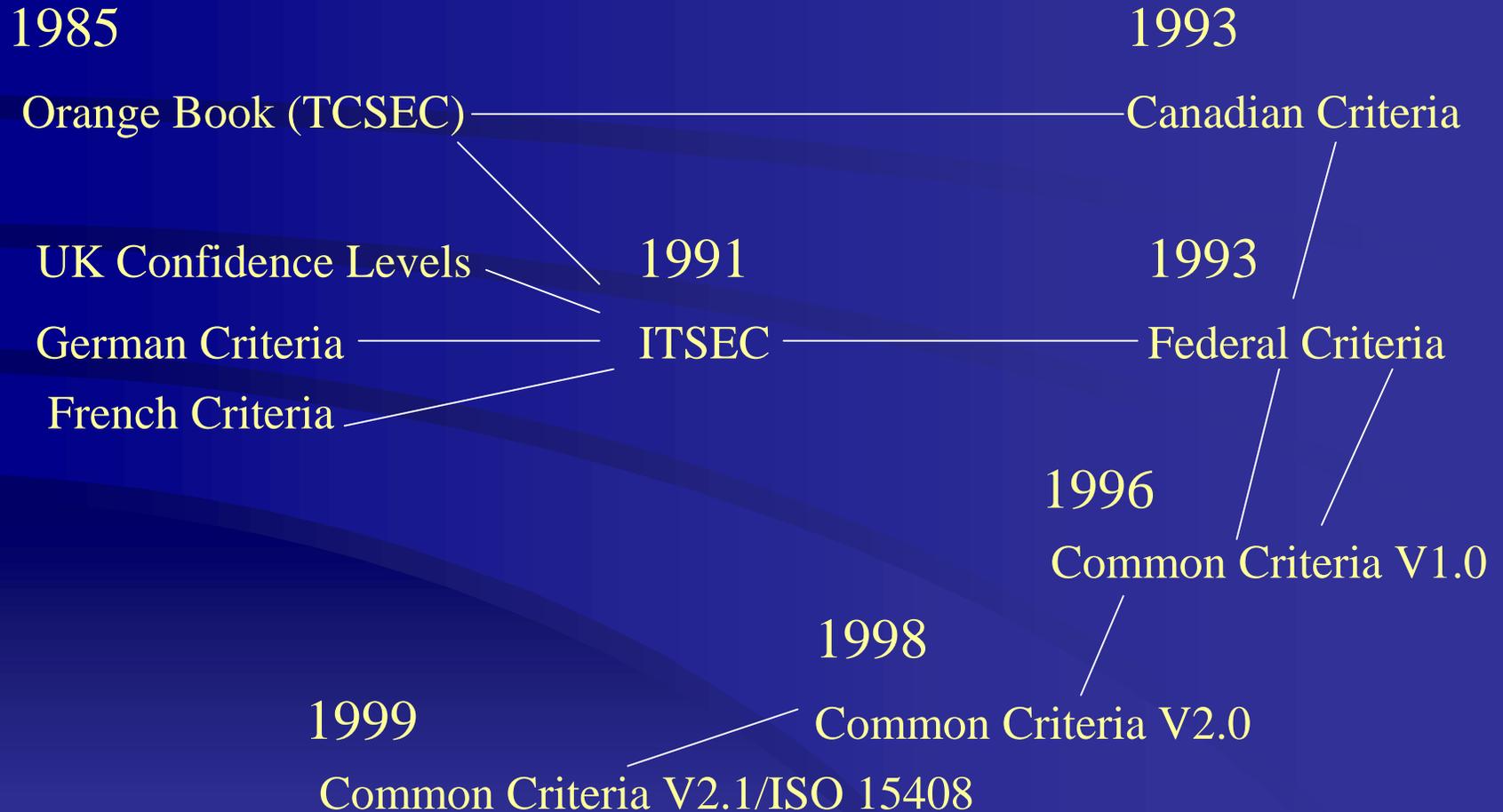
# DO-178B Software Failure Levels

- Assessment differs between five software levels
- The three types of assessment include:
  - ◆ Objective should be satisfied with independence.
  - ◆ Objective should be satisfied
  - ◆ Satisfaction of the objective is at applicant's discretion

# Common Criteria Overview

- Common Criteria
  - ◆ Replaces previous security criteria (i.e. Orange Book)
  - ◆ Is the basis of NIAP - joint activity of NIST and NSA
    - Establishes IT product security evaluation program
    - Promotes availability of tested products
  - ◆ More flexible than TCSEC
    - Can certify more types of products
    - Can pick and choose requirements
  - ◆ Is endorsed by many other countries
    - Don't need to re-certify products in supporting countries

# Common Criteria Overview



# Common Criteria Overview

- The CC organizes assurance requirements into *classes*
  - ◆ *ACM* – *Configuration Management*
  - ◆ *ADO* – *Delivery and Operation*
  - ◆ *ADV* – *Development*
  - ◆ *AGD* – *Guidance Documents*
  - ◆ *ALC* – *Life Cycle Support*
  - ◆ *ATE* – *Tests*
  - ◆ *AVA* – *Vulnerability Assessment*

# Common Criteria EALS

- Security requirements for software and systems vary depending on the purpose of the system
- Common Criteria offers different levels of assurance - Evaluation Assurance Levels (EALS)
  - ◆ Seven EAL Levels



# Common Criteria EALS

- EALS are predefined assurance packages that define a consistent set of assurance requirements
- EALS form an ordered set that is the predefined assurance scale of the CC
- EALS are hierarchically ordered in that each EAL represents more assurance than all lower EALS

# Common Criteria EALS

- **EAL1 – functionally tested**
- **EAL2 – structurally tested**
- **EAL3 – methodically tested and checked**
- **EAL4 – methodically designed, tested and reviewed**
- **EAL5 – semi formally designed and tested**
- **EAL6 – semi formally verified design and tested**
- **EAL7 – formally verified design and tested**

# Common Criteria EALS

- ◆ *EAL2* is an increase in assurance over EAL1
  - requires developer testing, a vulnerability analysis and independent testing based upon a more detailed Target of Evaluation (TOE) specification
- ◆ *EAL3* is an increase in assurance over EAL2
  - requires more complete testing coverage of the security functions, mechanisms and/or procedures that provide some confirmation that the TOE will not be tampered with during development

# Common Criteria EALS

- ◆ *EAL4* is an increase in assurance over EAL3
  - requires more design description, a subset of the implementation and improved mechanisms that provide confidence that the TOE will not be tampered with during development or delivery
  
- ◆ *EAL5* is an increase in assurance over EAL4
  - a semiformal design description is required over the entire implementation
  - more structured architecture, covert channel analysis, and improved mechanisms and or procedures that provide confidence that the TOE will not be tampered with during development

# Common Criteria EALS

- ◆ *EAL6* is an increase in assurance over EAL5
  - requires semiformal design descriptions, a structured representation of the implementation which is more analyzable
  - covert channel identification and improved configuration management and development environment controls
  
- ◆ *EAL7* is an increase in assurance over than EAL6
  - requires comprehensive analysis using formal representations and formal correspondence plus comprehensive testing

# Steps to Merging Certification

## Steps to Certification

- ◆ Step 1 - Map relevant DO-178B requirements to CC assurance requirements. High Level Comparison
- ◆ Step 2 - Document non-mapping CC classes  
Assume all DO-178B components will be done
- ◆ Step 3 - Examine separately FAA and CC certification
- ◆ Step 4 - Outline a merged certification process including steps from both sets of requirements

# High-level Comparison DO-178B to CC

## Step 1. High-level Comparison DO-178B Processes to CC Classes

### CC Assurance Class

ACM Configuration Management

ADO Deliver and Operation

ADV Development

AGD Guidance Documents

ALC Life Cycle Support

ATE Tests

AVE Vulnerability Assessment

### DO-178B Process

Software Configuration Management

*(No Correspondence) – elsewhere*

Software Development Process

*(No Correspondence) - elsewhere*

Software Planning Process

Software Verification Process

*(No Correspondence)*

# Non-mapping CC Classes

## Step 2. Non-mapping CC Classes

- Several Common Criteria classes deal only with security issues, do not map to any DO-178B processes
- These include
  - ◆ *AGD* – *Guidance Documents*
  - ◆ *ADO* – *Delivery and Operation*
  - ◆ *AVA* – *Vulnerability Assessment CC*

# Non-mapping CC Classes

## Step 2. Non-mapping CC Classes

- **Guidance documents class**
  - ◆ refers to documents specifically related to the security aspects of administration and operation of the software
- DO-178B does not address documentation relating to just security aspects of system operation
- DO-178B does not address user or management documentation directly

# Non-mapping CC Classes

## Step 2. Non-mapping CC-classes

- **Delivery and Operation** class
  - ◆ insures that software was delivered without interference or tampering
  - ◆ insures that software is installed and initially started securely and correctly
- DO-178B process components do not address security aspects of tampering and initial start-up

# Non-mapping CC Classes

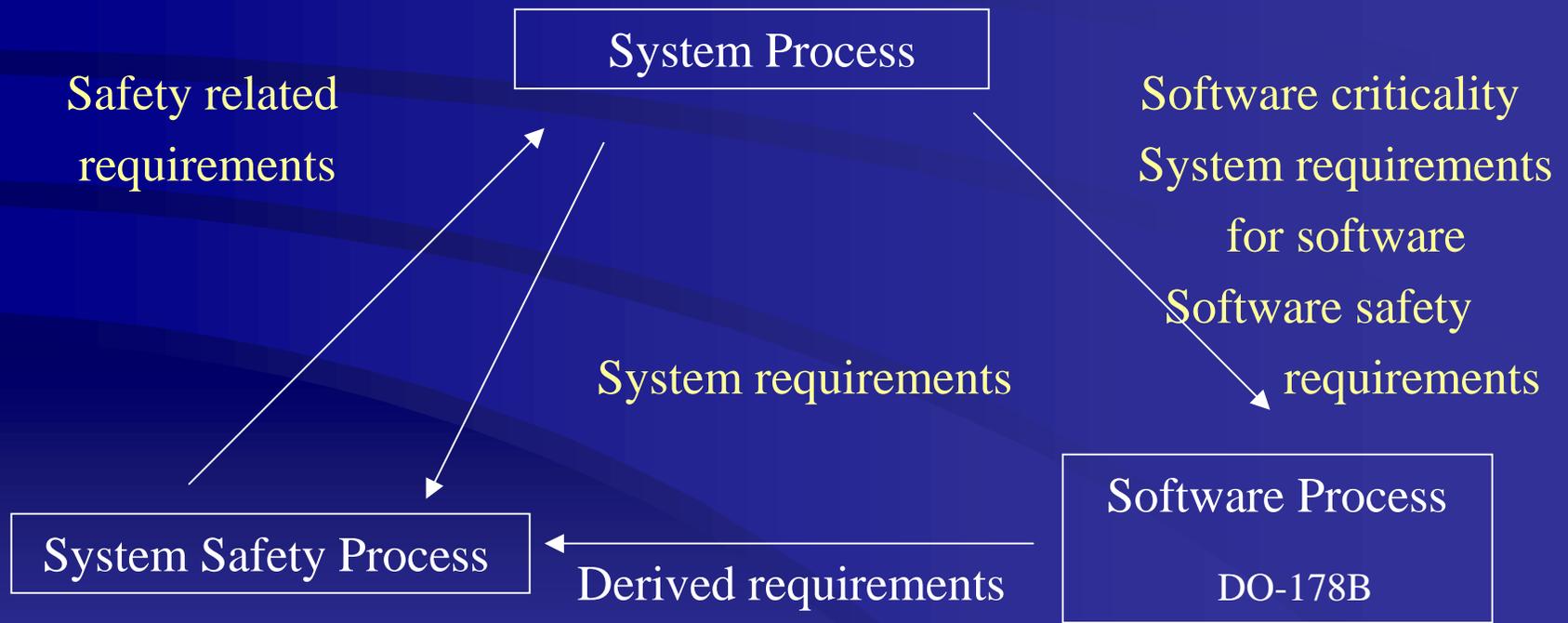
## Step 2. Non-mapping CC Classes

- **Vulnerability Assessment class**
  - ◆ Deals specifically with covert channel analysis, deliberate misuse and other security function assessments
- DO-178B requires structural coverage testing and traceability; avoiding inclusion of unspecified “features”

# FAA Certification

## Step 3. FAA Certification Process

### FAA Certification Overview



# FAA Certification

## Step 3. FAA Certification Process

### System process

- ◆ identifies system requirements, passes them to safety process
- ◆ sets software criticality level, passes this to software process

### Safety process

- ◆ sets system development assurance level, A - E
- ◆ passes back assurance level to system process

### Software process

- ◆ creates derived requirements, passes them to system safety process

# FAA Certification

## Step 3. FAA Certification Process

- Software is developed according to DO-178B requirements for the criticality level
- Certification involves the DER and the FAA
  - ◆ DER - Designated Engineering Representative
    - Represents the FAA interests at a manufacturing site
    - Typically, manufacturers have one or more DER's on site
    - Software DER's must have a software development background
  - ◆ DER either performs FAA certification or recommends certification to the FAA

# Common Criteria Certification

## Step 3. Common Criteria Certification

- ◆ For EAL 5 - 7, rigorous security requirements need to be built into the system from the beginning
- ◆ Lower level EAL's, security can be added
- ◆ Choose an existing Protection Profile (PP) if one is available
  - Protection profile is a template for a given product type, ( ie PP for a firewall)
  - No PP, security requirements can be selected from CC- Part 2
- ◆ Security Target (ST) is developed for the product
  - ◆ ST is a document that includes security requirements, the intended environment, security threats, PP requirements

# Common Criteria Certification

## Step 3. Common Criteria Certification

- ◆ Product is then built according to ST security requirements
- ◆ Evaluation is done by an accredited lab against the ST requirements
- ◆ Evaluation results are submitted to an evaluation authority for validation
  - US - NIST/NSA
- ◆ Upon passing validation, product entered in registry of CC certified products

# Merged Certification Process

## Step 4. FAA and CC Certification

- ◆ Three general phases to the process of dual certification
  - Pre-Software Development Decisions
  - Software Development
  - Evaluation and Certification

# Merged Certification Process

## Step 4. FAA and CC Certification

### Pre-Software Development Decisions

#### **FAA Certification**

- Establish system requirements
- Establish safety related requirements
- Set software criticality level

#### **CC Certification**

- Establish EAL level
- Identify applicable PP
- Incorporate security requirements
- Create the product ST

- ◆ Security requirements can merge with system safety requirements

# Merged Certification Process

## Step 4. FAA and CC Certification

### Software Development

- ◆ Software Planning
  - Configuration management, develop software plans, establish data gathering methods for both CC and FAA
- ◆ Software Development
  - High-level design, low-level design, derived requirements  
- DO-178B, code
- ◆ Software Test and Assurance
  - Both DO-178B and CC have many common areas here

# Step 3. Merged Certification Process

## Step 4. FAA and CC Certification Evaluation and Certification

### **FAA Certification**

DER either directly certifies product including software or recommends to the FAA that the product be certified

### **CC Certification**

Software is presented along with the ST to registered lab  
Lab evaluates the ST and recommends certification  
Submits it to evaluation authority for final validation

# Conclusions

- Considerations in Mapping CC to DO-178B
  - ◆ Differences exist between the intended purposes of the two documents important to the final outcome of merging requirements from both
  - ◆ DO-178B insures that software used in aircraft is developed with "best known" practices, does not contribute to aircraft safety hazards

## **Emphasis in DO-178B**

- outlining general policies and procedures to produce safe software in terms of airworthiness requirements
- produce documentation to substantiate that the development requirements have been met

# Conclusions

- Consequently, language and content is high-level and abstract
  - ◆ Most compliance decisions are left up to the developer
  - ◆ Expected that software process will be linked to an external process
- CC higher EALs require more formalism in product requirements, development and analysis.
  - ◆ This formalism is not required by DO-178B, but can be added to specific product requirements

# Conclusions

## Emphasis in CC

- The Common Criteria (CC) is intended to specify that a system, hardware or software, has met certain security assurances
  - ◆ CC only deals with security functionality of systems and does not address overall development issues except where they affect security
  - ◆ CC can be considered guidelines for a subset of the system

# Conclusions

## Emphasis in CC

- The CC is more detailed in terms of specifying **how** compliance is achieved for an intended product
  - ◆ Each component of each assurance class has specific action elements and evidence of compliance for both developers and evaluators
- Expectation of accredited independent evaluation of the product

# Conclusions

- Merging CC security requirements into DO-178B will need to address these differences in detail so that none of the CC functionality is lost
- Integrating security functionality into the FAA certification process needs to be addressed for the total system being evaluated, not just the software since the CC's scope encompasses entire systems
  - ◆ This involves other FAA regulations and documents

# Conclusions

- Consequently, mapping between DO-178B and the CC will only constitute part of the process for FAA certification NSA/NIST for a high-level assurance system.
- Mapping and integration of CC requirements will need to be extended beyond DO-178B to satisfy CC certification

# Questions?

<http://www.csds.uidaho.edu/~jimaf>