Software Test & Evaluation Summit/Workshop

Mike Nicol
Software Technical Advisor
Air Force Aeronautical Systems Center
michael.nicol@wpafb.af.mil
Issues in Software Test & Evaluation

• Evolving ASC/EN Role as Independent USAF Airworthiness Authority

• Focus on safety critical systems & software
  – No longer limited to flight systems/vehicle control

• Integrated look at the computer system architecture and hardware/software components that support safety critical functions to ensure
  – Proper implementation of all safety critical requirements/functions and hazard mitigations
  – No hazardous or misleading information to crew
**MIL-HDBK-516B (Airworthiness Certification Criteria)**

**Computer Resources Requirements**

- Identification of safety critical functions and associated hazards
- Effective approaches to fault tolerance and redundancy management
- Use of mature hardware
- Disciplined application of a thorough development process
- Complete requirements traceability
- Comprehensive testing of the software
  - Unit, component, configuration item, integration, and system levels
- Full software qualification with every release
- Failure insertion testing through “extensive” Failure Modes Effects Testing (FMET)
- System qualification through lab testing
Challenge Areas

- **DO-178B as a silver bullet**
- **Development process issues**
  - Safety critical functions/requirements not tagged
  - Inadequate function/requirements traceability
  - Lack of clear understanding of how hardware and software components support safety critical functions
  - Inadequate process or lack of defined process for verification of changes
  - Inadequate test coverage for safety critical functions
  - Lack of robust FMET
- **Lack of test automation**
  - Contributes to compounded delta qualifications
Next Steps

• Develop Computer Systems and Software Integrity Program Military Standard (CSSIP)

• Continue to improve Air Force Weapon Systems Software Management Guidebook

• Update MIL-HDBK-516B

• Increase emphasis on Software Development Plans (SDPs)
Software, hardware, architecture, and integration

Criticality definitions and categories (flight/safety, mission, maintenance, lab/development, etc.)

Safety critical function analysis

Redundancy management, fault tolerance, partitioning

System architecture risk mitigation requirements

Interface requirements

Testing (software, hardware, integration, failure modes effects, coverage analysis, qualification, regression)

Discrepancy reporting and tracking

Etc.

Nicol, 16 Sep 2009
Concluding Thoughts

• We know how to do this better so,
  – What are the barriers?
  – What can we do about them?
  – Develop guidance for RFP and contract language?
  – Are current standards adequate?

• Balance zeal with reality
  – Unintended consequences of policy
  – Technical workforce limitations/resource impacts