AVIONICS CYBER TEST AND EVALUATION

Joseph Nichols, PhD

Technical Advisor for Flight Test and Evaluation

Air Force Test Center

Edwards AFB CA

joseph.nichols.13@us.af.mil

OUTLINE

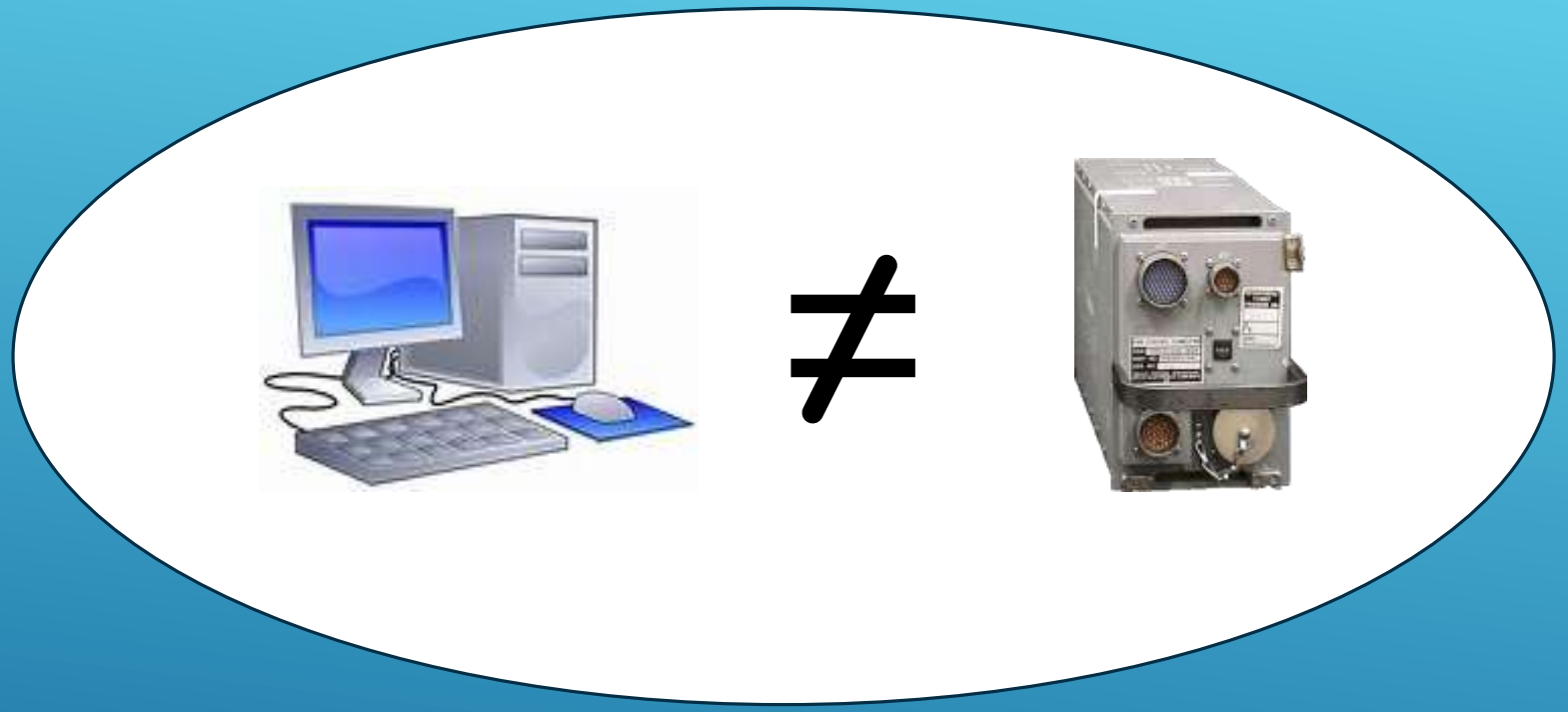
- Defining avionics cyber testing
- Cyber T&E process
- Infrastructure requirements
- Manpower requirements
- Summary

CYBERSPACE CATEGORIES

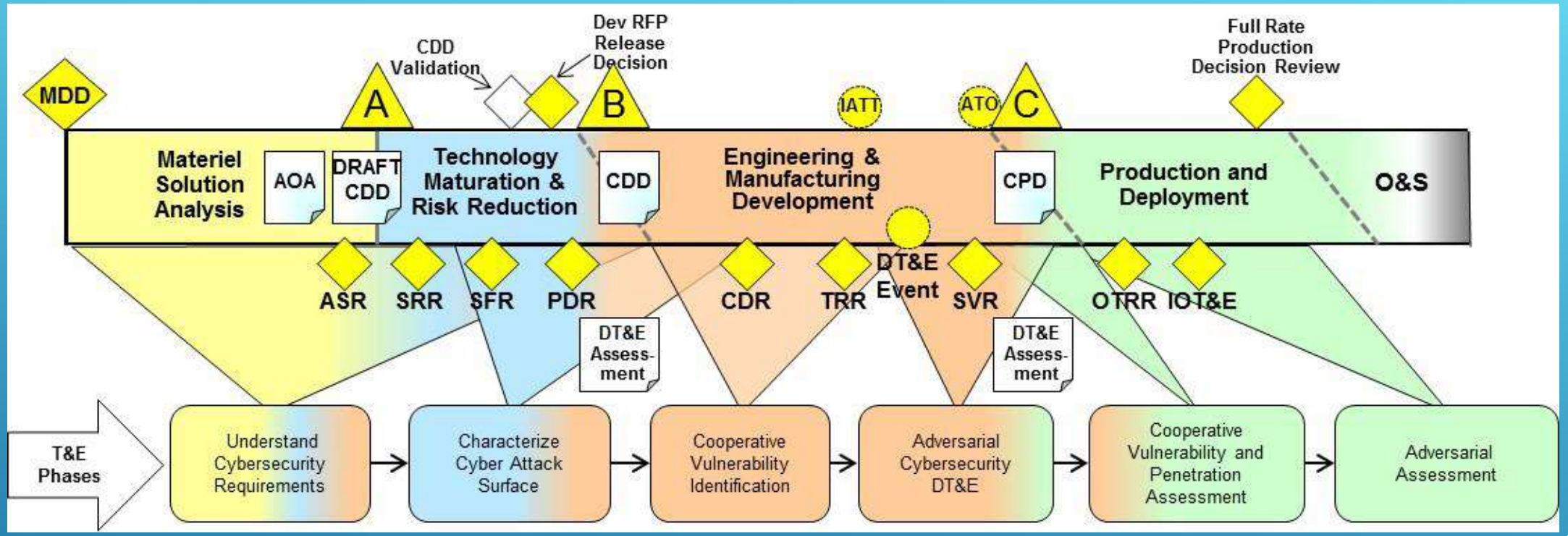
- Traditional IT
- Industrial Control Systems
- Platforms

CYBERSPACE CATEGORIES

- Traditional IT
- Industrial Control Systems
- Platforms ← Aircraft avionics and weapons



AVIONICS SYSTEMS ARE DIFFERENT FROM STANDARD PCS AND NETWORKS



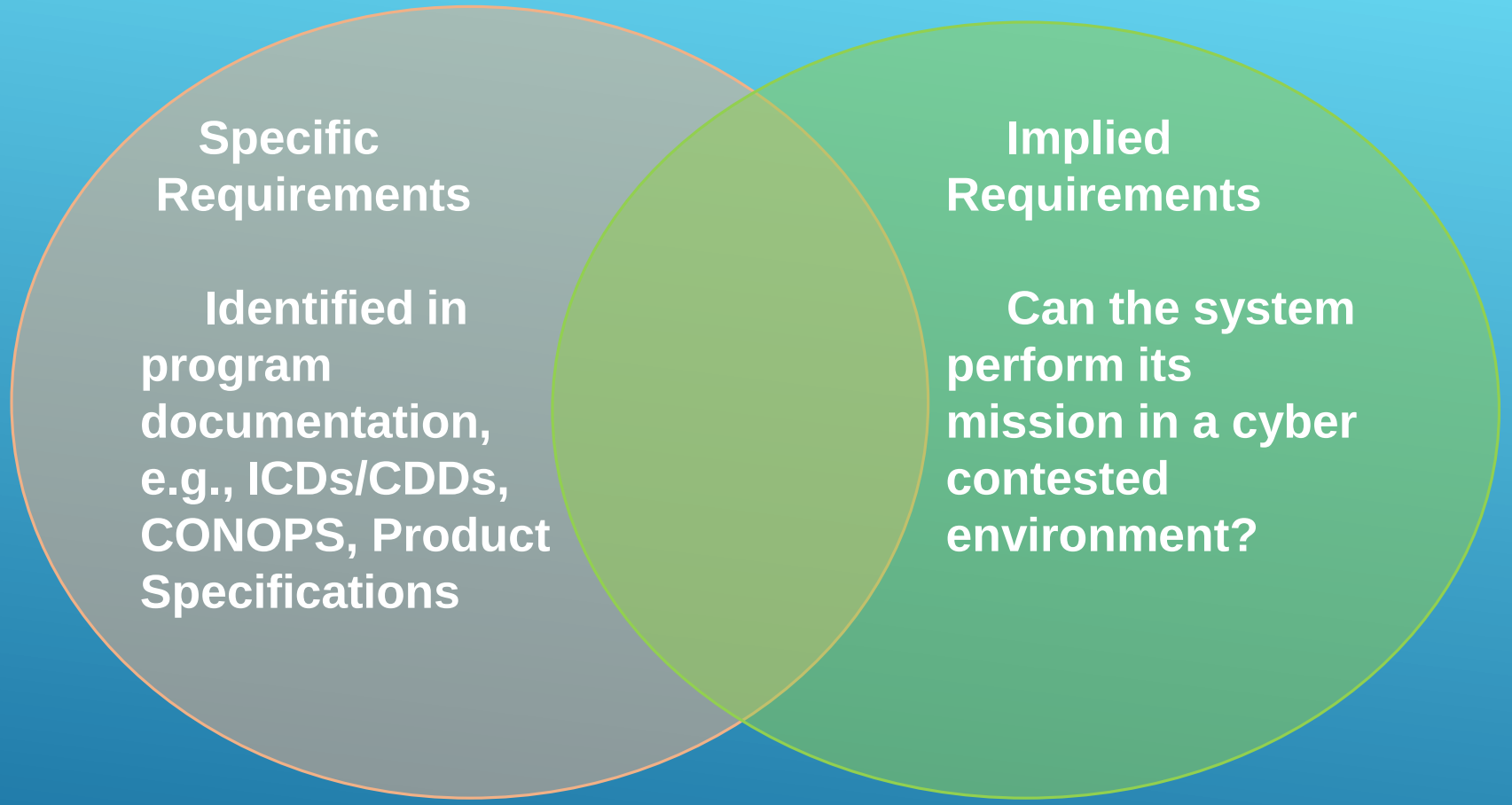
DOD CYBERSECURITY TEST AND EVALUATION GUIDEBOOK

NDAA SECTION 1647

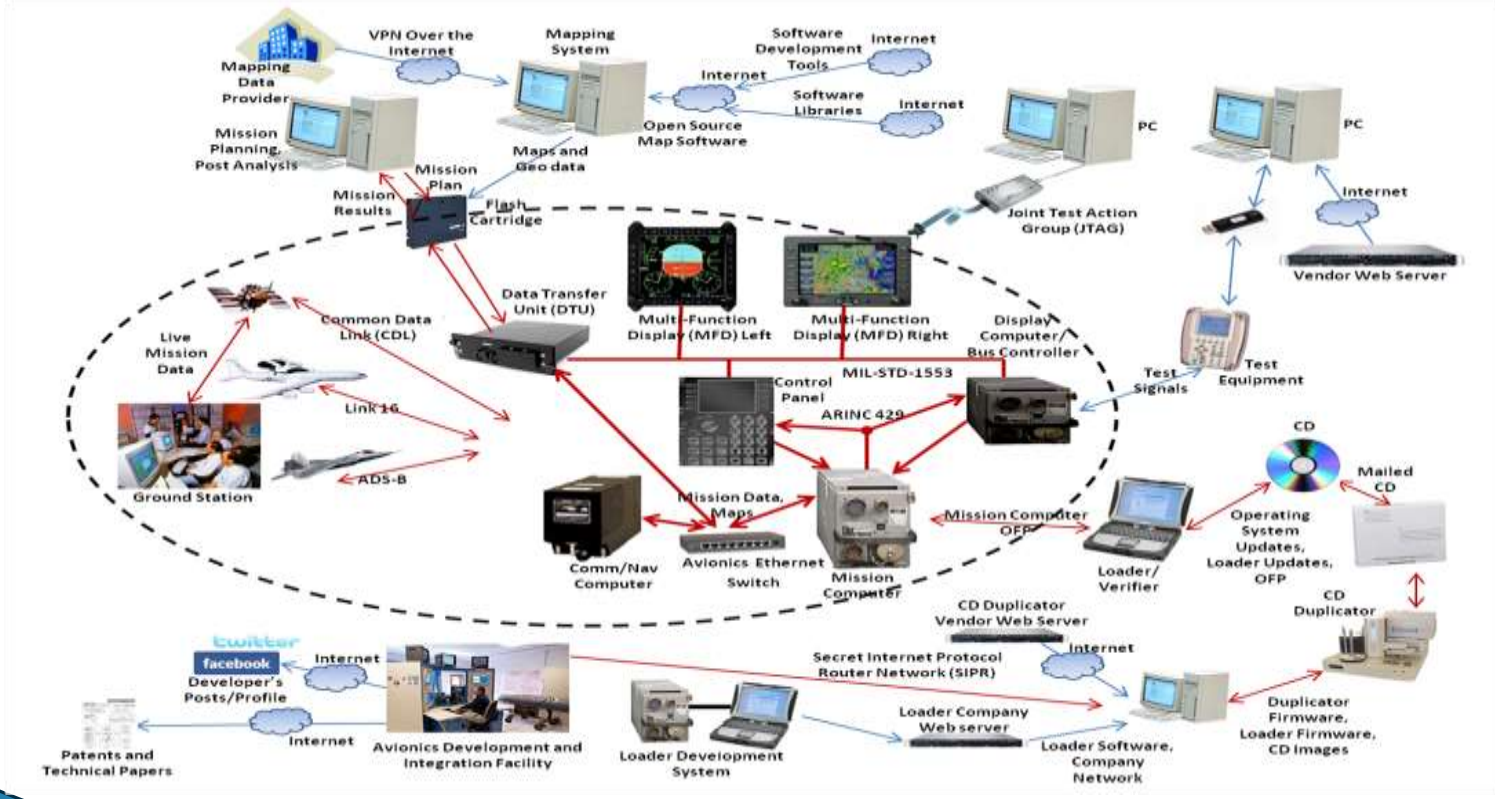
- DOD direction to conduct a cybersecurity evaluation of all major US weapon systems
- Testing must be completed by Dec 2019
- Combined vulnerability identification phase
- Planning combined DT/OT testing

CURRENT PROCESS

- Vulnerability Identification Phase (Phases 1-2)
- Cooperative DT/OT (Phases 3-5)
- Adversarial Assessment (Phase 6)



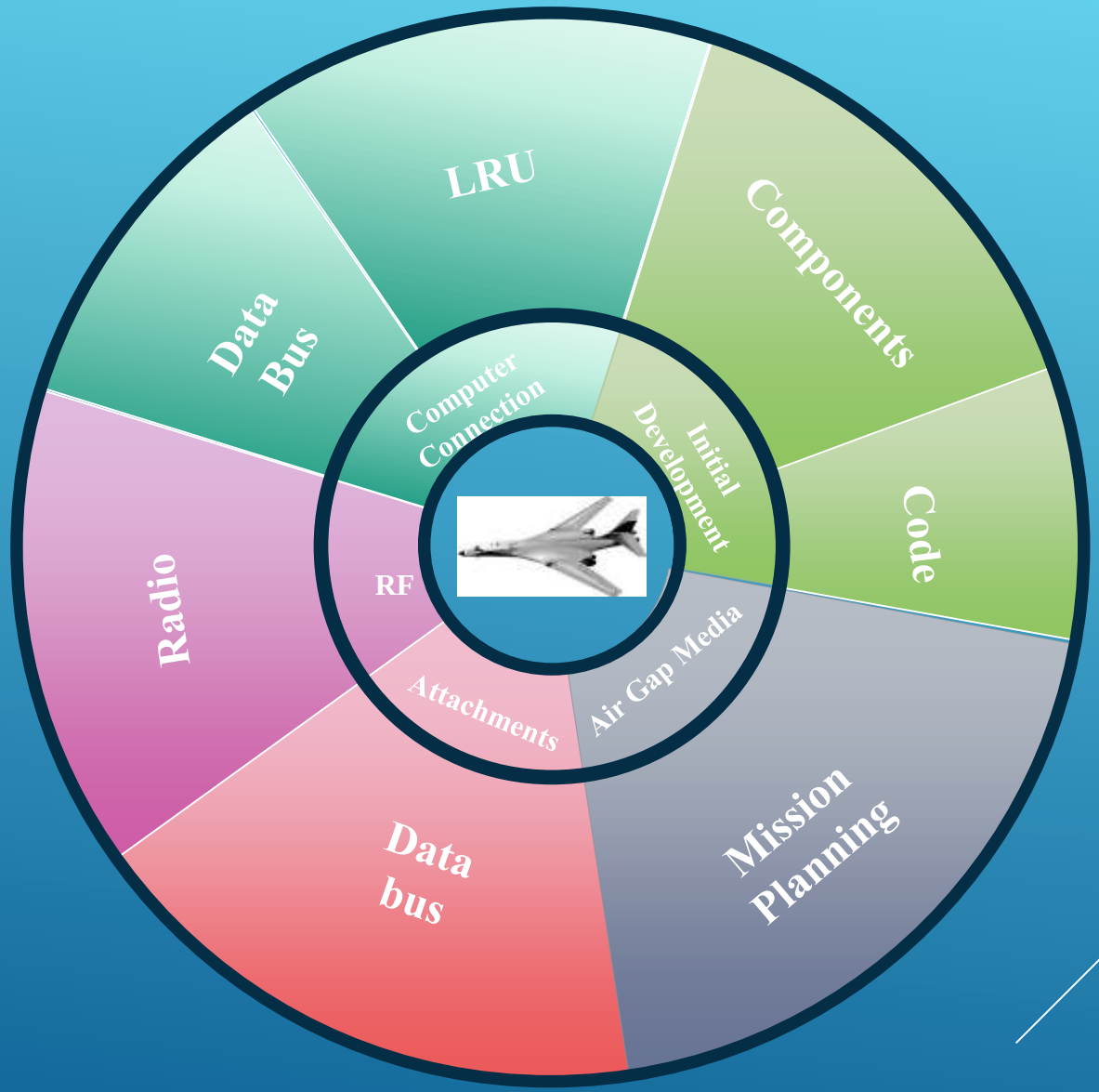
REQUIREMENTS

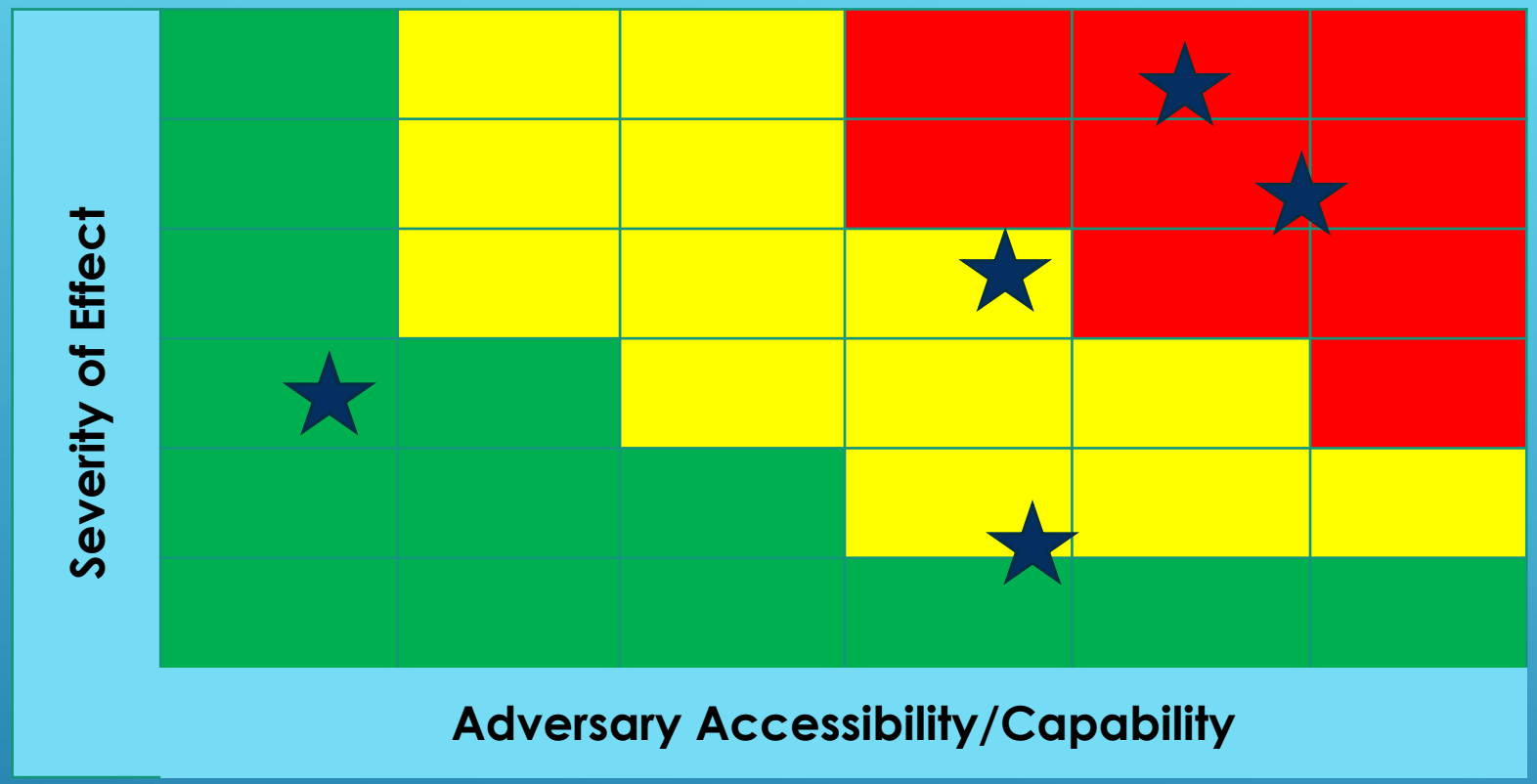


DEFINING THE ATTACK SURFACE

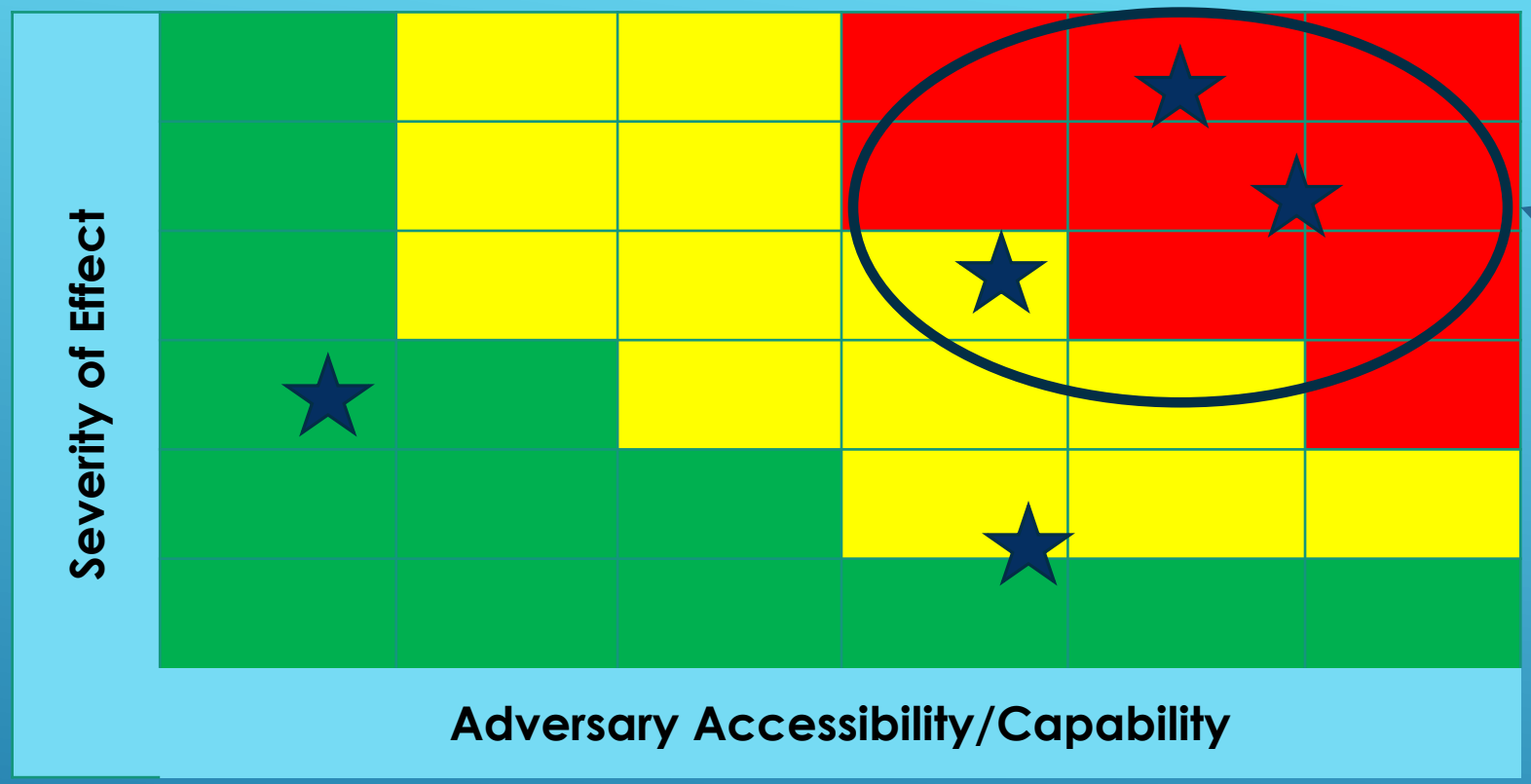
VULNERABILITY IDENTIFICATION

Avionics Wheel of Access





EVALUATING SUSCEPTIBILITY TO CYBER ATTACK



Most severe threats to be further evaluated in combined DT/OT

EVALUATING SUSCEPTIBILITY TO CYBER ATTACK

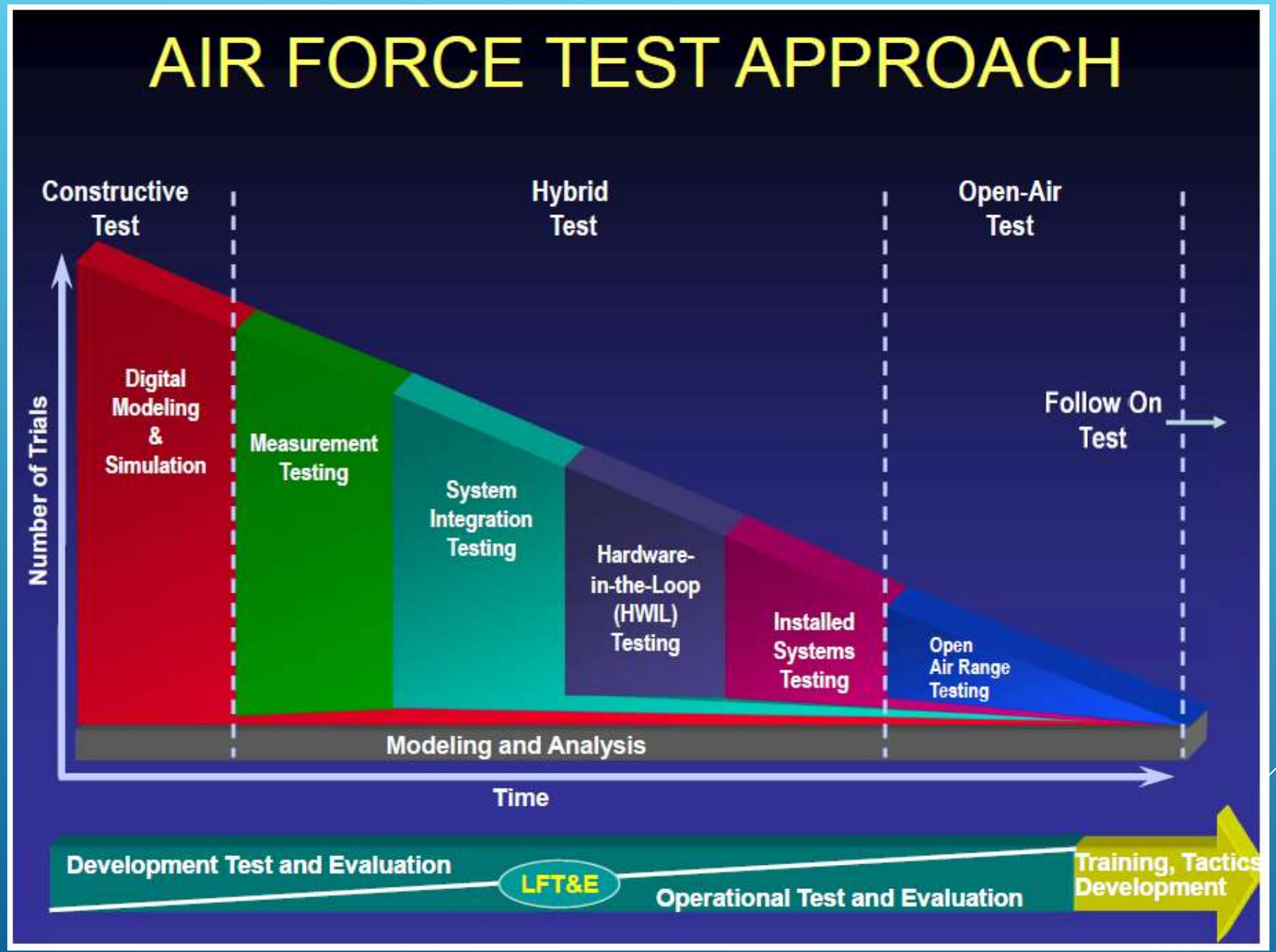
- **Evaluation of the system's cybersecurity in a mission context, using realistic threat exploitation techniques, while in a representative operating environment**
- **Characterize operational cybersecurity status and determine residual risk**

COOPERATIVE DT/OT TEST AND EVALUATION

ADVERSARIAL ASSESSMENT

- To assess the system's defensive cyberspace performance in the operational environment to withstand threat representative cyber-attacks, detect and react to those attacks, and return to normal operations in the event of a successful cyber-attack

AIR FORCE TEST APPROACH



AVIONICS CYBER TEST INFRASTRUCTURE

- DoD test facility capable of conducting cyber testing compatible with the unique features of aircraft avionics and airborne munitions
- Center of Excellence for avionics cyber T&E and developer of cyber test techniques and test tools
- Connected with the NCR and other aircraft and weapons cyber test facilities

AVIONICS CYBER RANGE REQUIREMENTS

1. Ability to stimulate avionics components to put them in flight modes
2. Ability to provide standard interfaces for avionics busses, radars, data links, radios, mission planning, software loaders, maintenance systems, weapons, sensors, etc.
3. Ability to work with actual aircraft/weapons, real subsystems, emulations, or re-hosted software (requires flight line access)
4. Ability to stimulate sensors through direct injection, or through system apertures (requires anechoic chamber)
5. Test tools capable of penetrating avionics components and returning them to pre-test conditions
6. Realistic threat emulation
7. Multi-level security environment
8. Mobile test tools/procedures for testing in other HITLs

MANPOWER REQUIREMENTS

- Cyber T&E expertise for aircraft and weapons requires a merge of traditional avionics test expertise and computer network penetration expertise
- Sending avionics test engineers to cyber training
- Developing DOD cyber training courses
- Standing up new test organization dedicated to all aspects of cyber test and evaluation – networks, aircraft, weapons

SUMMARY

- Systems becoming increasingly difficult to defend against emerging cyber threats
- Cybersecurity T&E should not be treated as a separate process. It should be integrated into the normal system development just as we test functionality and performance
- New class of test facilities and test tools must be developed to test aircraft avionics and airborne weapon systems
- New T&E discipline of avionics-cyber tester under development

QUESTIONS