NDIA Aircraft Survivability Workshop

Applying the Tenets of Aircraft Combat Survivability to Achieve Cyber Resilience



Mr. Tom Barnett

Cyber Integration Lead, APEO Engineering & Technology
Program Executive Office, Aviation

17 March 2022

DISTRIBUTION STATEMENT A: Approved for Public Release; Distribution is Unlimited



Today's Talking Points

- Misconception: Cybersecurity is an Aircraft's Achilles' Heel
- How do we Solve the Cyber Problem?
- Cyber Considerations in a Survivability Context
- Designing in Resiliency
- Traceability of Requirements to Cyber Survivability
- Closing Comments and Questions



Misconception: A Cyber Vulnerability is an Aircraft's Achilles' Heel

"Superstition: a belief or practice resulting from ignorance, fear of the unknown, trust in magic or chance, or a false conception of causation."
~ Merriam-Webster

- **Today's Military Aircraft were not Designed with Cyber Threats in Mind**
  - But they were designed to be Safe, Airworthy, Reliable and Survivable
- **DoD's Cyber Policies and Practices are Heavily Biased toward the Information Technology (IT) Paradigm**
  - Cybersecurity is about Protecting **INFORMATION** (C-I-A)
  - Access to the System is **ASSUMED** (*Likelihood* = 1)
  - Once Compromised, Impact is assumed to be **CATASTROPHIC** (Thus the misuse of the word ***Vulnerability***)
- **In the Operational Technology (OT) world, Criticality and Timing matter**
  - Functions may be Mission Critical and/or Safety Critical (or not)
  - Not all functions are Critical in all System Configurations or during all Mission Types/Phases
  - Susceptibility to Cyber Attack varies significantly depending on Operational Environment and Connectivity
  - Cyber Effects may or may not cause Mission Impacts
- **Aircraft DO NOT Fight in the Cyber Domain, but in the Physical Domain…*in the presence of* a Cyber Threat**
  - Discussions of the 'Cyber Domain' usually refer to Offensive/Defensive Cyber Operations (OCO/DCO)
  - A Cyber Threat to an Aircraft is simply a Non-Kinetic Lethality Mechanism that is part of the Operational Environment
  - We must determine both Probability of Hit (P_H) and Probability of Kill given Hit ($P_{K|H}$) to analyze Cyber alongside other Threats to Survivability

Simply Stated, we can't Prioritize Survivability Risk from a Cyber Threat until we Quantify it in Terms of Traditional Lethality



How Do We Solve the Cyber Problem?

"If we keep doing what we're doing, we're going to keep getting what we're getting." ***~ Stephen Covey***

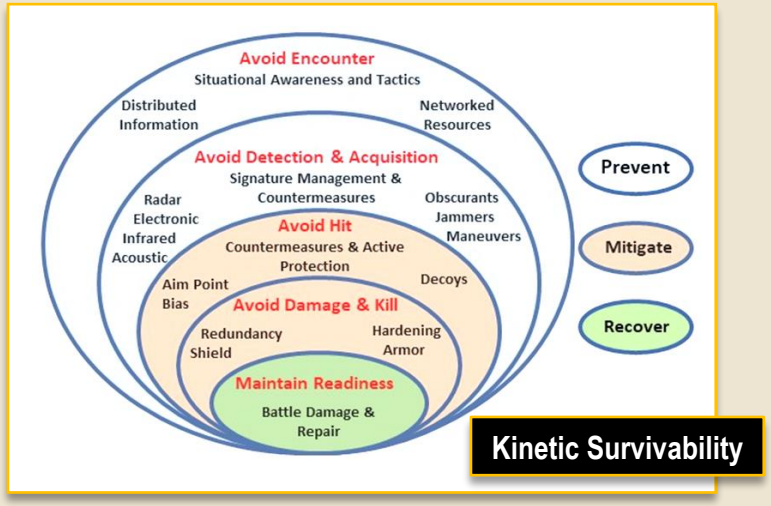
- **Cyber Resiliency is a System Engineering Problem, Not a Computer Problem**
  - Cyber is evaluated under the System Survivability KPP
  - Compliance ≠ Security
  - Assurance ≠ Survivability
  - RMF Controls ≠ Requirements
  - You can't 'Test Security into a System' (plus it's too late by then)
- **The PEO Aviation Cyber Strategy is rooted in the three System Survivability Pillars: Prevent, Mitigate, Recover**
- **We must use the same System Engineering Processes as when considering Safety, Reliability and Survivability**
  - Design in Resilience
  - Derive Cyber Requirements from Performance, Safety/Airworthiness and Other "-ility" Requirements
  - Use common Mitigate and Recover Capabilities, regardless of cause, where possible
  - Test the System *against* a Cyber Threat but **Evaluate** Impacts alongside Performance and Survivability Requirements

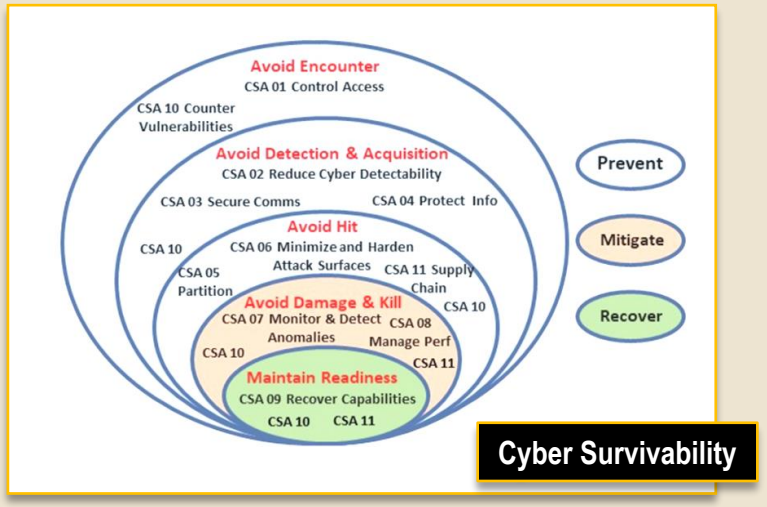
Cyber Problems aren't necessarily best solved with MORE Cyber

Cyber Considerations in a Survivability Context

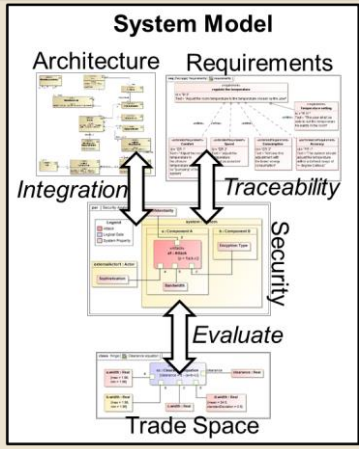
As with any Threat, the conditional 'Pillars' of Survivability must be considered

- **Prevent (Prior to the Attack)**
  - Secure Design and Configuration to avoid the Threat (Susceptibility = 0)
  - Due Diligence through Hardware, Software, and Information (Cybersecurity) Assurances
  - Protect Ground Systems (Mission Planners, Software/Data Loaders, Maintenance Devices, ...)
  - Utilize Mission Planning and TTPs, where appropriate
- **Mitigate (During the Attack)**
  - Monitor Mission Critical Functions (MCF) to maintain Mission Effectiveness
  - Utilize Countermeasures consistent with Kinetic and EW Effects
  - Detect Anomalies and Manage at the Cyber Level, when possible (i.e. Component Resilience)
  - Must be Performed in ***Tactically*** Relevant Timeframe
  - Fail Safe: Graceful Degradation and Adaptability **Must be 'Baked In'**
- **Recover (After the Attack)**
  - Incident Response at the Fleet Level
  - Reconstitute/Repair/Replace
  - Must be Performed in ***Operationally*** Relevant Timeframe



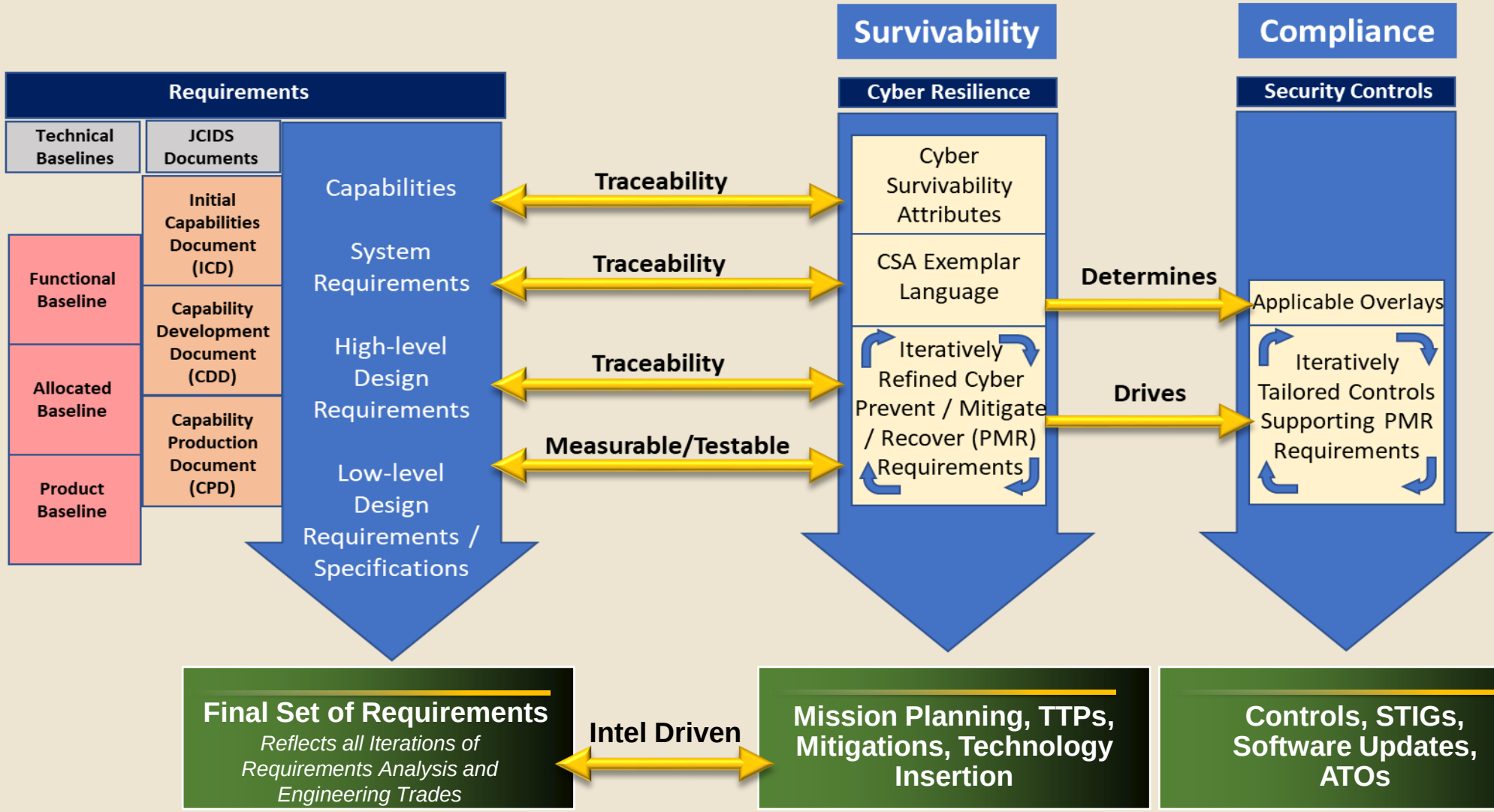


Designing in Resiliency



- **For every Cyber Effect, there is a corresponding System Effect**
  - Loss of Functionality or Capability
  - Quantify these System Effects the same as any other Failure/Damage
  - The goal of Mitigation should be to mitigate *System Effects*, not just Cyber Effects
  - Unmitigated **System Effects** lead to **Mission Impacts**
- **Translate back into 'Engineering Space,' and use existing Processes**
  - Align Cyber efforts with Program Protection processes and do things once
  - Engineering approaches such as MBSE and STPA-Sec provide excellent models to address potential Impacts
  - The Safety community has well-established processes (FMECA/FMEA/DMEA/Hazard Analysis) to ensure robust designs
  - Reference the Survivability 'Onion' to see the entire problem
  - Follow the DOTMLPF order of precedence
    - Redundancy: Have to design for It
    - TTPs: Have to train for It
    - Big changes require full DOTMLPF considerations
- **Develop Cyber Requirements alongside Performance and Airworthiness-related Requirements**
  - Leverage the SS KPP Cyber Survivability Endorsement (CSE) for alignment
  - Cyber requirements must be Measurable and Testable
  - CSE Implementation Guide offers Exemplar Requirements Language
  - Select the minimum number of RMF Overlays and Controls based on derived Cyber Requirements for compliance purposes

Traceability of Requirements to Cyber Survivability





Closing Comments and Questions

Website	http://www.army.mil/peoaviation
Facebook	http://facebook.com/peoaviation
DVIDS	https://www.dvidshub.net/unit/PEO-A
LinkedIn	https://www.linkedin.com/company/peo-aviation



Backup Slides