ITEA Cyber Security Workshop

Workforce Development Panel

27 March 2019

Isidore Venetos
Federal Aviation Administration
William J. Hughes Technical Center -Aviation Research Division (ANG-E2)
Aviation Information Security Protection R&D , Manager
Atlantic City International Airport, NJ 08405
Isidore.venetos@faa.gov
HSDN: Isidore.venetos@faa.sgov.gov
609-485-5207

FAA

NextGEN

NOT your typical IT networks

Location: William J. Hughes Technical Center, ACY New Jersey

Aviation Research Division
Cyber R&D Overview

- **Aviation Research Division** Cyber R&D Programs

  Two Broad categories of FAA Cyber research:

  - **Aviation Safety**
    - Support development of policy, regulation, guidance
    - *Collaborate with the aviation community*
    - **Promote the safety culture to include information security**
  - **Innovative Cyber Capability Development**
    - Mature innovative technologies/concepts for application into the aviation ecosystem
    - Transition into NAS & MSD systems

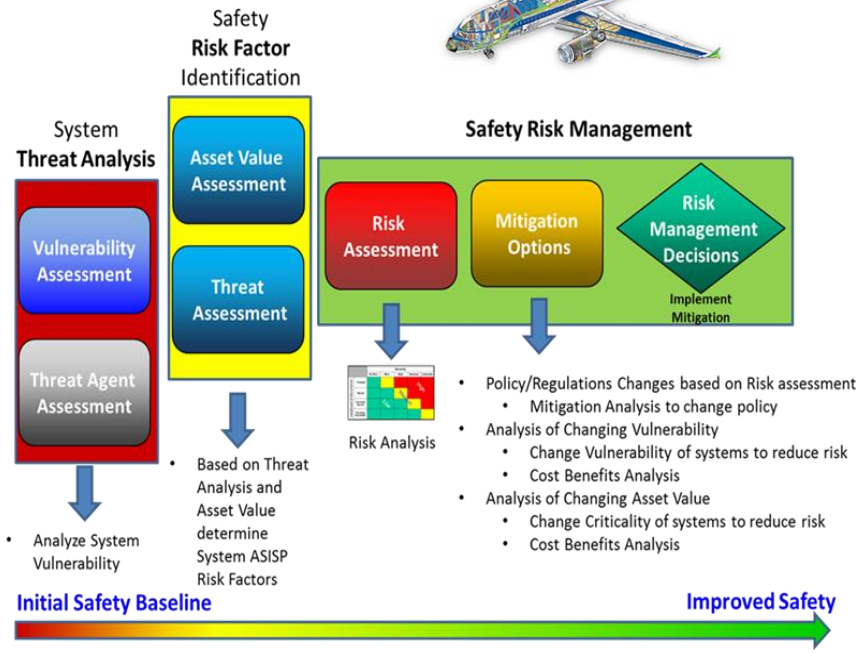
FAA

NextGEN

Aircraft Systems Information Security Protection (ASISP)

Goal: A Risk Based Decision Making Process for assessing the risks associated with cyber attacks on aircraft

- ✓ Allows consistent standard outputs
- ✓ Structured methodology
- ✓ Repeatable and Validated processes
- ✓ Removes assessment bias
- ✓ Consistent with the Safety Management Systems (SMS)- Safety Risk Management (SRM) and Risk Based Decision Making (RBDM) principles FAA strategic initiative



RBDM process can be applied to other systems beyond Aircraft to the Aviation Ecosystem

FAA

NextGEN

Safety Environment: Today

Safety

- Safety culture is very strong
  - Safety is a priority, well understood problem set of risks and solutions, proactive approach with solution sets
  - Well structured safety processes & procedures support the culture
- Outstanding historical performance record
- Commercial Aviation Safety Team (CAST)
  - Solutions based; NOT regulatory based
  - Industry coordinated solutions
- Predictable product assurance based approach
  - Likelihood is very quantitative with well documented occurrences to include outliers

Cyber Security

- Security culture is in development
  - Cyber Security is not often prioritized, not a well understood set of risks and solutions with ad-hoc approach and patch solution sets
  - Processes & Procedures being developed independently
- Sparse documented historical record
- No CAST equivalent community solution
  - Often checklist compliance based
  - Independent solution sets
- Unpredictable Cyber-based environment
  - Likelihood is not easily quantifiable since cyber security is based on vulnerabilities, actor capabilities and actor motivation

Safety Environment: Tomorrow

Safety

- Safety culture is very strong
  - Safety is a priority, well understood problem set of risks and solutions, proactive approach with solution sets
  - Well structured safety processes & procedures support the culture
- Outstanding historical performance record
- Commercial Aviation Safety Team (CAST)
  - Solutions based; NOT Regulatory based
  - Industry coordinated solutions
- Predictable product assurance based approach
  - Likelihood is very quantitative with well documented occurrences to include outliers

Cyber Security

- Security culture is strong
  - Cyber Security risks prioritized, well understood set of risks and solutions with industry wide approach
  - Well structured Processes & Procedures in place
- Historical record of threat/risks/mitigations
- CAST equivalent community solution
  - Solutions based; NOT Regulatory based
  - Consensus-based solution sets
- Managed Cyber-based environment
  - Understanding of vulnerabilities, actor capabilities and actor motivation
  - **Risk-Based Management Approach**

Industry and Government Partnership is imperative for a Strong Safety + Security Culture

ITEA Workforce Development Challenges Summary

- Aviation goes beyond standard IT systems
  - ✓ Cyber IT expertise does not equate to Cyber Aviation expertise
  - ✓ Proprietary black boxes
- Safety Culture needs to be integrated with the Cyber Security culture
  - ✓ Mature Integrated Aviation Safety/Cyber security processes and methods are imperative
- Industry and Government Expertise must be leveraged through partnerships
  - ✓ Test and Evaluation is dependent on understanding Risks and in the FAA Safety Risk is Top Priority (DOD – Mission is Top Priority)