REDAC / NAS Operations

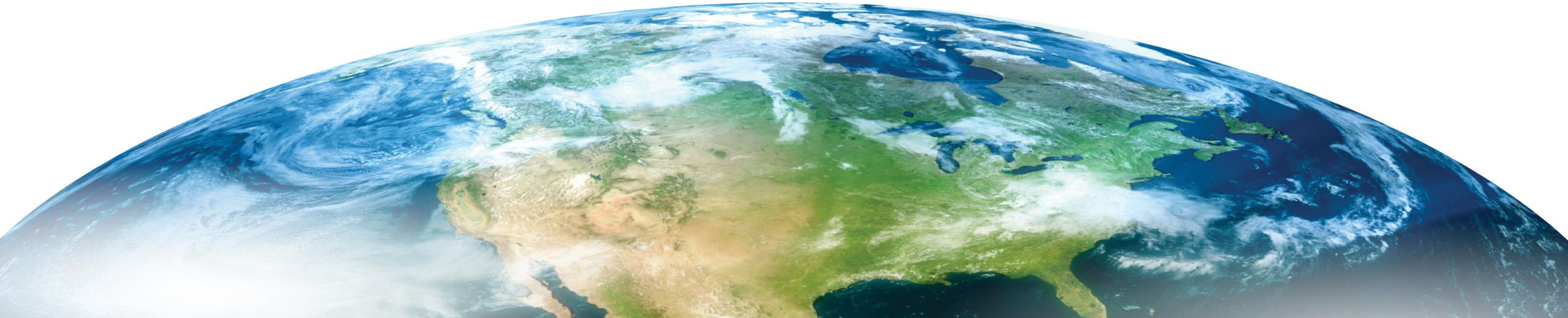
Name of Program: Flight Deck Data Exchange Requirements

BLI Number:

Presenter Name: Nouri Ghazavi

Date: Sept, 2021

Review of FY 2021 - 2023 Proposed Portfolio

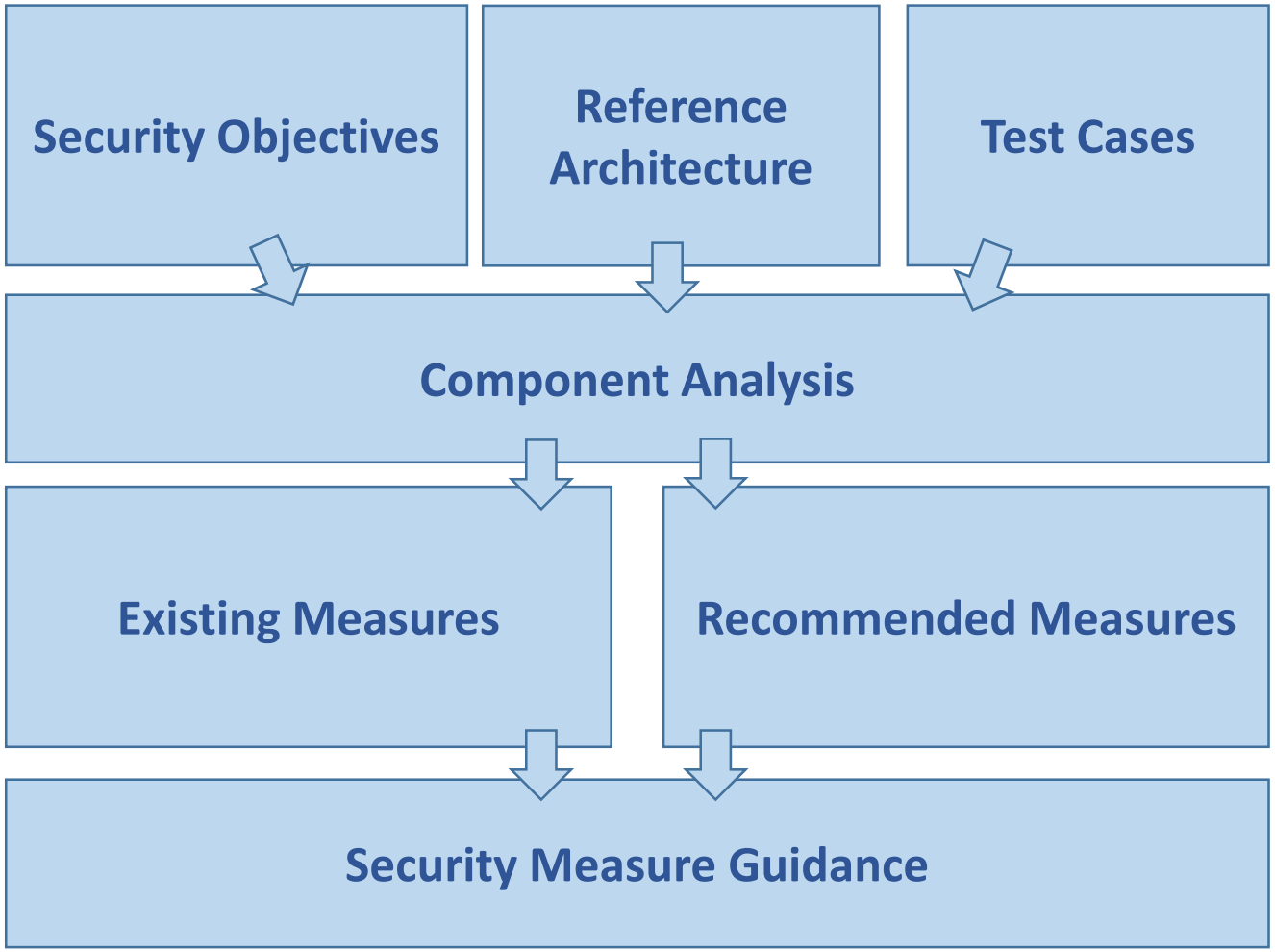


FD DER Overview

Project Description:

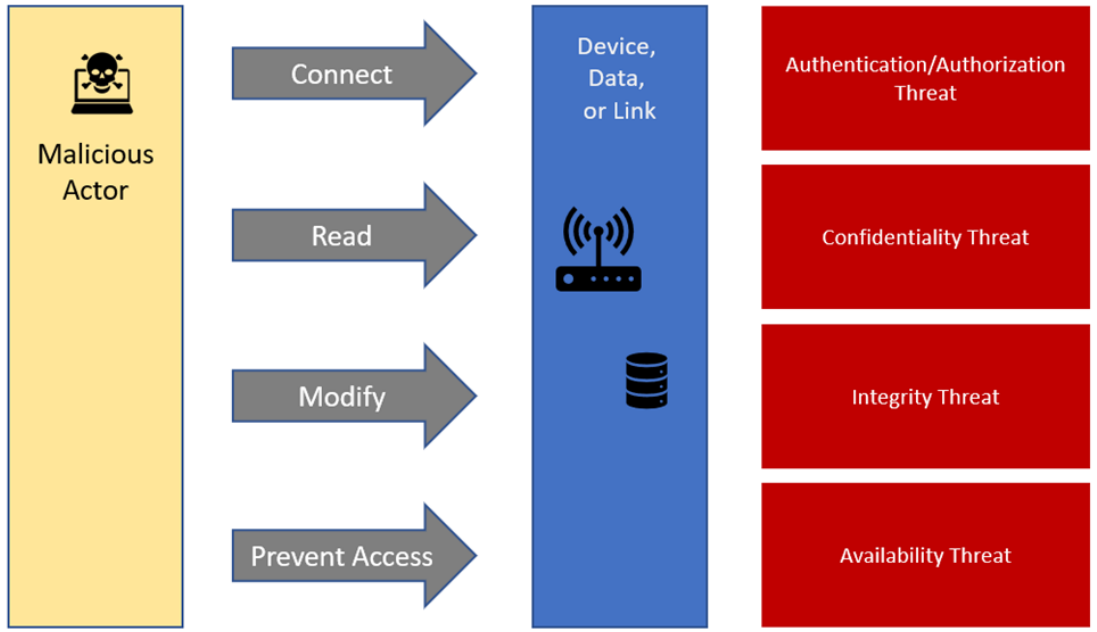
- FD DER project supports advanced exchanges of information between aircraft and ground systems by identifying and addressing cybersecurity gaps for onboard avionics with specific focus on Electronic Flight Bag (EFB) and Aircraft Interface Device (AID) as well as Internet Protocol (IP) datalinks
- Identify mitigations to guarantee data integrity, when the data is coming from
  - Untrusted sources (e.g. EFB), or
  - Untrusted networks (e.g. IP Datalinks), into the Airline Information AISD or ACD Domain
- Conduct security analysis through selected test cases of applications that support Air Traffic Management (ATM) functions.

Overall Approach



Security Objectives

- Authentication/Authorization
- Confidentiality
- Data Integrity
- Availability



Apply threat activity to each component to identify baseline threat conditions

FD DER Project Progression

Architecture Alternatives

Risk Assessments

Generalized Test Cases

Security Objectives and Measures

Validation Exercise

Gaps and Roadmap

FD DER Evaluation Approach

- These security measures may be added to an existing prototype systems:
  - Domain segregation for A/G Links
  - Application Data Encryption
  - LAN Segregation, Rate Limiting, Traffic Filtering
  - EFB & Other Hardware Protection (e.g. disabling ports)
  - EFB & Other SW Protection (e.g App testing, OS settings, anti-malware)

Requirement approach

- Identify applicable threats
- Apply controls
- Assess existing prototype system:
  - Approach:
    - Table lists the high-level controls
      - Focus is on controls that are implemented by technical means (as opposed to organizational)
      - Most controls have both aspects, but we will only be looking at technical means
    - Expectation is that FD-CDM would identify the implementation
      - Some controls may be implemented in the prototype, others may be deferred to the production system
    - Will be an iterative process

Organizational Security Controls

- These controls have some technical aspects, but are primarily implemented by policy and other administrative actions:

NIST Category	EFB	AID	A/G Links	MAS to A/C API	MAS to NAS API
2. Awareness and Training	(Outside of aircraft domain)				
3. Audit and Accountability	(Organizational requirement outside of aircraft domain but some controls such as timestamps and audit logs should be considered for future work)				
4. Assessment, Authorization, and Monitoring	(Organizational requirement outside of aircraft domain, related technical requirements are covered under other controls)				
8. Incident Response	(Outside of aircraft domain)				
10. Media Protection	(Organizational requirement outside of aircraft domain, related technical requirements are covered under other controls)				
11. Physical and Environmental Protection	(Out of scope for this project)				
12. Planning	(Outside of aircraft domain)				
13. Program Management	(Outside of aircraft domain)				
14. Personnel Security	(Outside of aircraft domain)				
15. Personally Identifiable Information Processing	(Outside of aircraft domain)				
16. Risk Assessment	(Outside of aircraft domain)				
17. System and Services Acquisition	(Outside of aircraft domain)				
20. Supply Chain Risk Management	(Outside of aircraft domain)				

Technical Security Controls

- We will be looking to identify implementations for these controls:

NIST Category	EFB	AID	A/G Links	MAS to A/C API	MAS to NAS API
1. Access Control e.g. User Accounts, Secure Logon, Domain Authentication, etc.					
5. Configuration Management e.g. Protected Software Installation, Digital Signing, Monitoring					
6. Contingency Planning e.g. Alternative Data Paths, Automatic or Manual Safe Mode					
7. Identification and Authentication e.g. Multi-factor or Out-of-band authentication, PKI authentication, etc.					
. Maintenance e.g. Restricted Tool Use, Software Patching					
*** 18. System and Communication Protection** e.g. Partitioning, Access & Flow Controls, DoS Protection, Transmission Confidentiality & Integrity, and many others…					
*** 19. System and Information Integrity** e.g. Malicious Code Protection, System Monitoring, Software Integrity, and many others…					

Accomplishments and Anticipated Research

Accomplishments

- Published "*Cybersecurity for Flight Deck Data Exchange"* for Digital Avionics Systems Conference.
- Continue assessing prototype systems and developing requirement for Validation Exercise.

Planned Research Activities

- The follow-on effort will conduct an exercise to validate effectiveness of the identified security mitigation. The exercise will be conducted in partnership with a proof-of-concept NextGen program(s), and leverage its concept prototype to implement security test components for evaluation.
- Provide recommendation for Securing Future Connected Aircraft and Flight Deck Applications
  - Identifies Key Technology, Infrastructure, and Regulatory Areas
  - Identifies Potential Gaps
  - Provides Concrete Recommendations
  - Focus Areas for Regulatory Updates
  - Focus Areas for Industry Support
  - Enablers for Air Traffic Services over Connected Aircraft

Emerging FY23 Focal Areas

- No current plan/fund beyond FY22

FD DER

Research Requirements

This program will address cybersecurity concerns around avionics and onboard IP Data Link required to enable connected aircraft concept and enhance Collaborative Decision Making (CDM) between flight deck and ground operations. The program will conduct cybersecurity assessment and evaluation exercises to identify risks and determine appropriate mitigation strategy. The findings of this research will serve as recommendations to support development of future standards and policies for connected aircraft.

Outputs/Outcomes

- The outcome will inform development of an initial security considerations for IP-based flight deck data exchanges concept

FY 2022 Planned Research

- Cybersecurity risk assessments of avionics and aircraft systems in Aircraft Control domain and Airline Information Services domain such as FMS and aircraft maintenance system
- Conduct lab exercises to evaluate security management strategy identified through the cybersecurity risks assessment exercise

Out Year Funding Requirements

RE&D

FY20	FY21	FY22
$ 1.014M	$ 1.005M	$ 0.879M

F&E

FY20	FY21	FY22	FY23	FY24	FY25
$ - M	$ - M	$ - M	$ - M	$ - M	$ - M