REDAC / NAS Operations

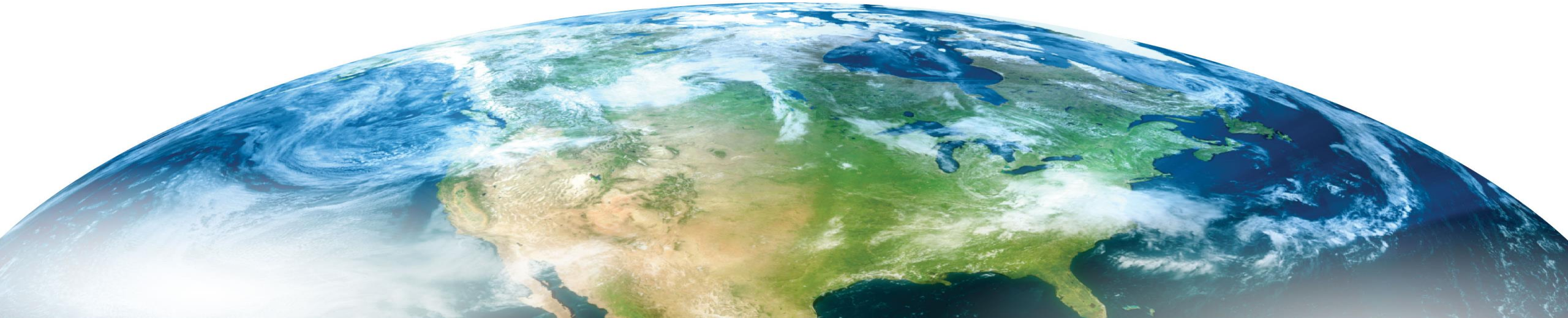
Name of Program: Flight Deck Data Exchange Requirements

BLI Number:

Presenter Name: Nouri Ghazavi

Date: March 16th, 2021

Review of FY 2021 - 2023 Proposed Portfolio

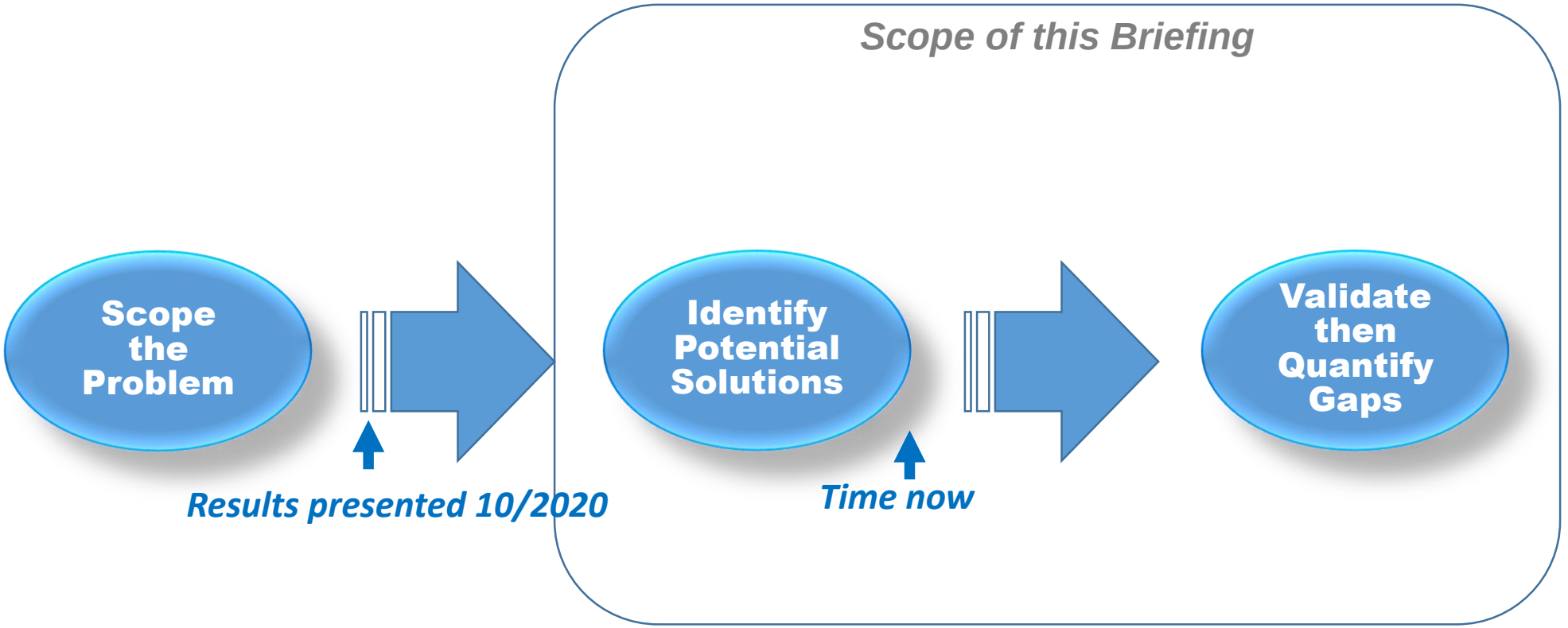


FD DER Overview

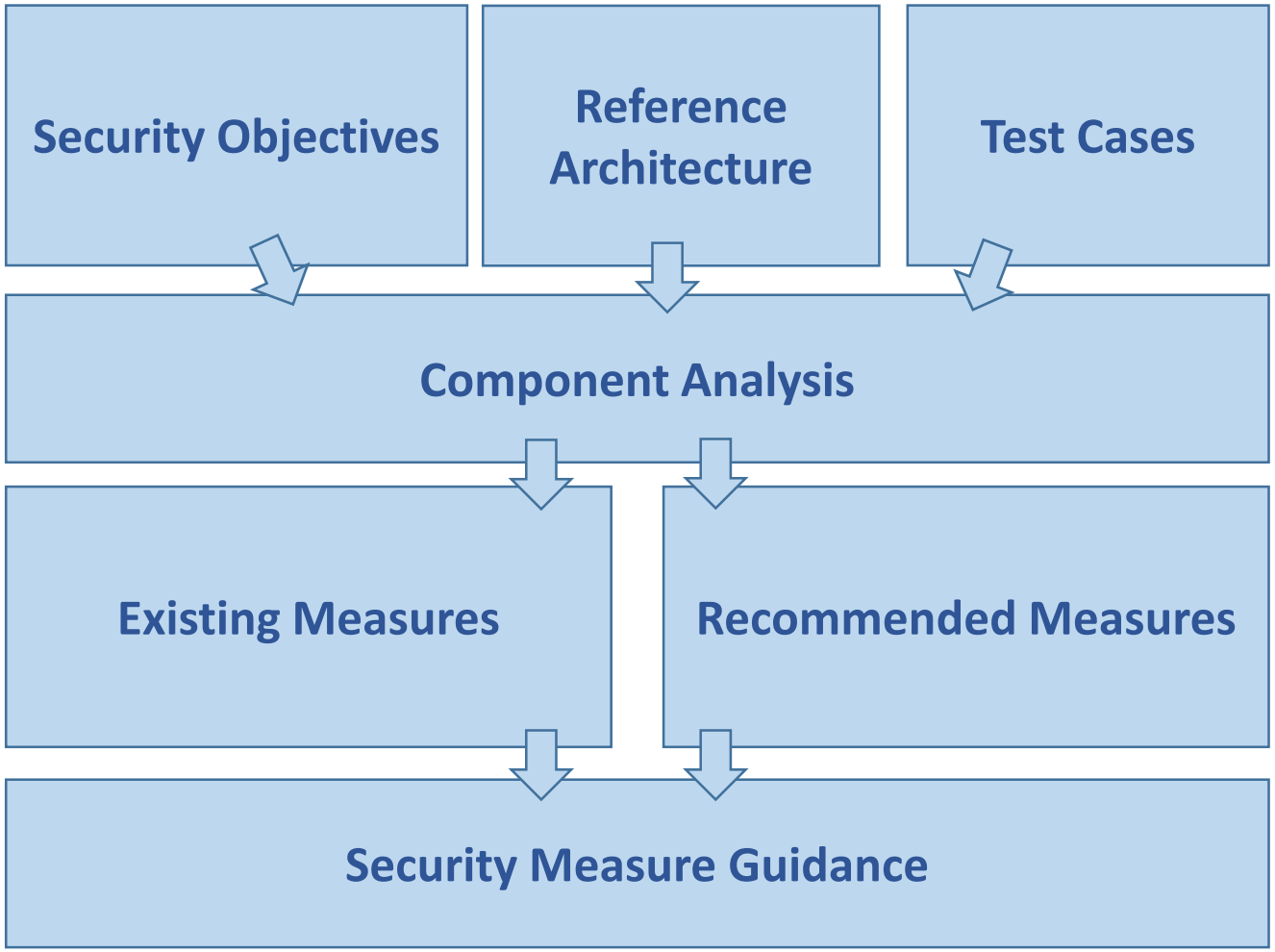
Project Description:

- 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 safety critical data and applications that support Air Traffic Management (ATM) functions.

FD DER Project Progression

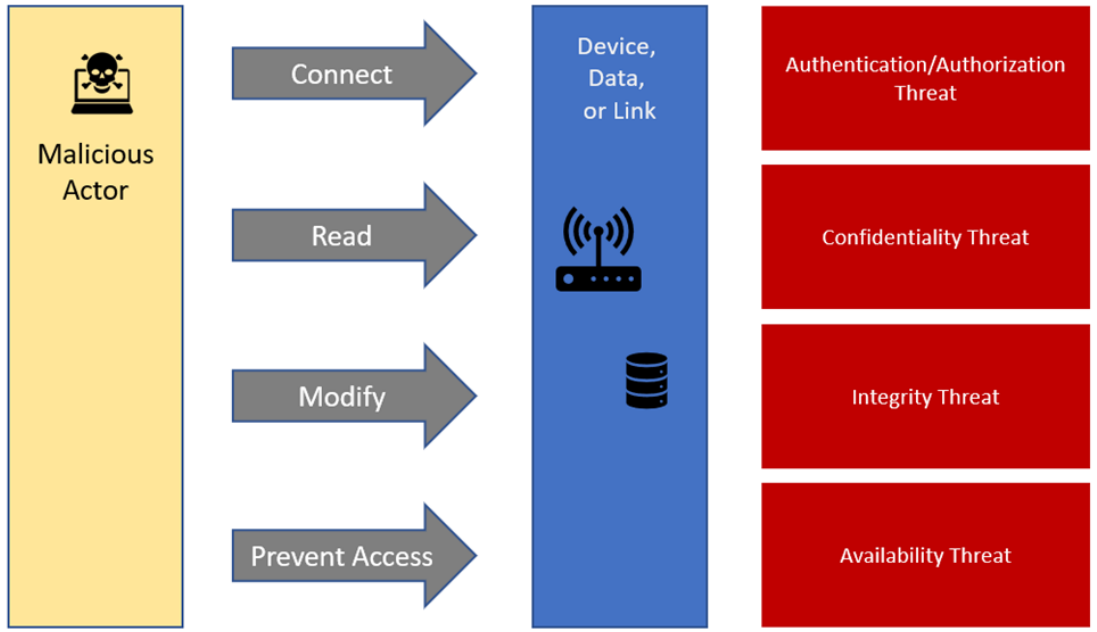


Overall Approach



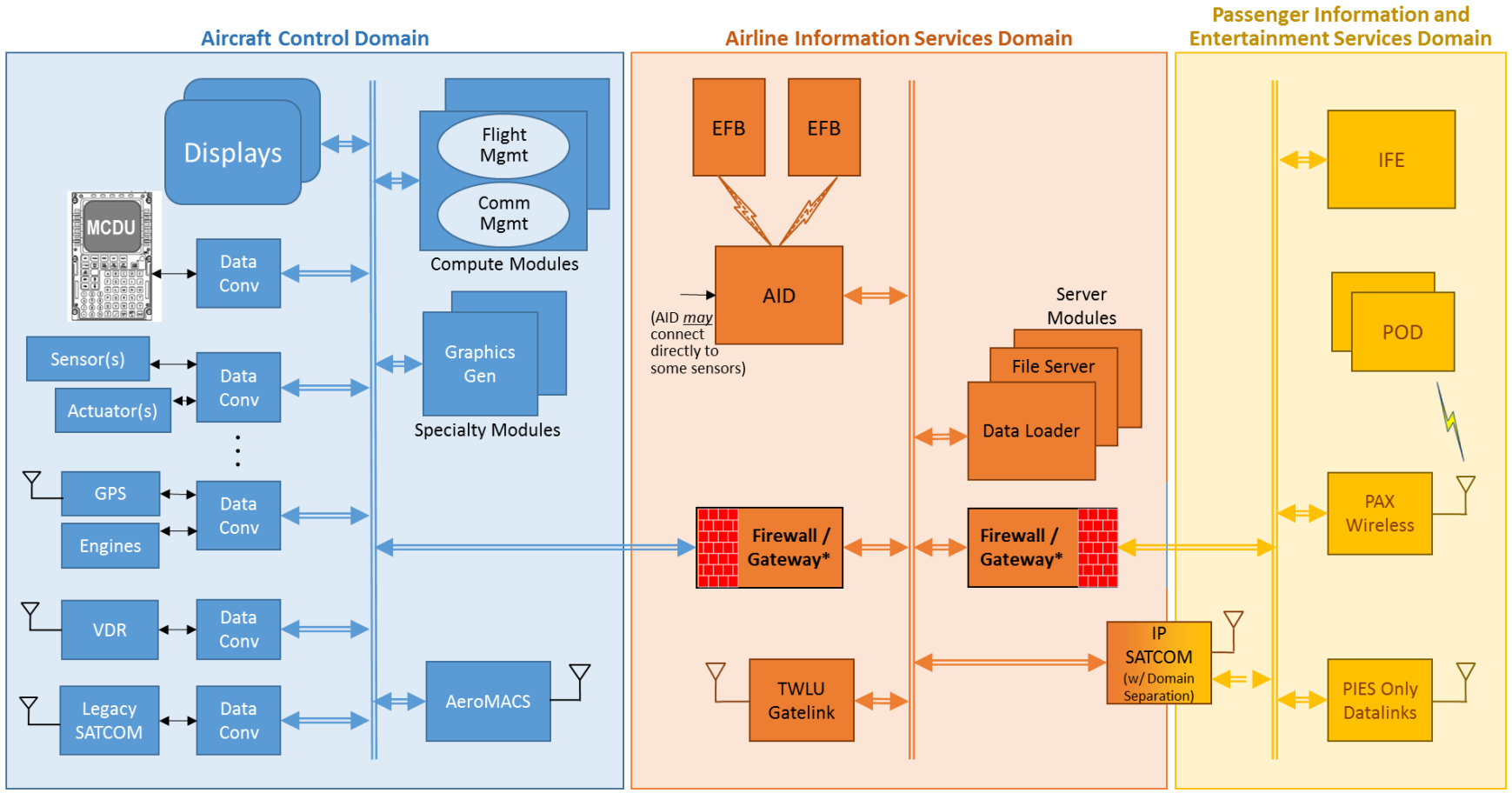
Security Objectives

- Authentication/Authorization
- Confidentiality
- Data Integrity
- Availability



Apply threat activity to each component to identify baseline threat conditions

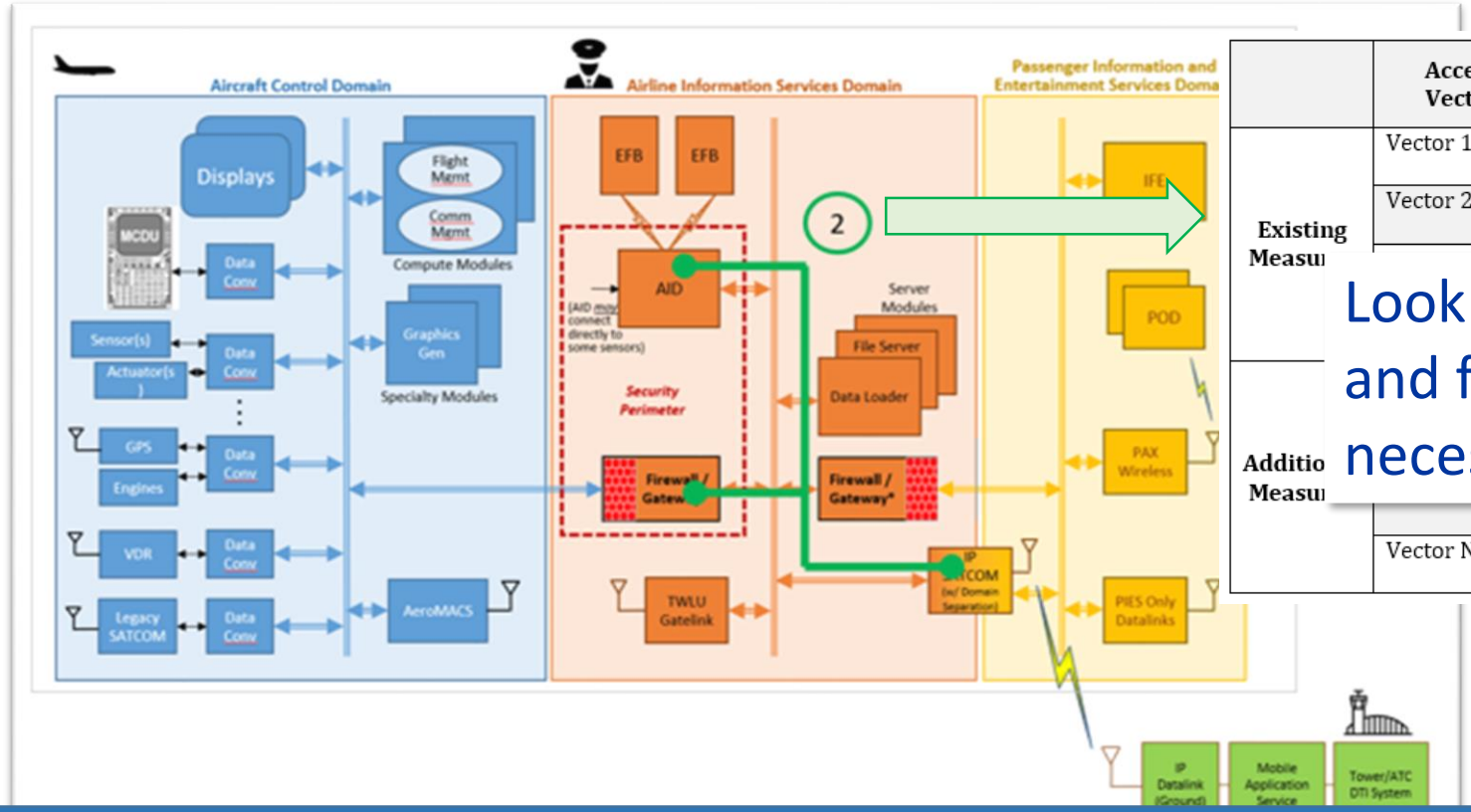
Reference Architecture



Key Architectural Assumptions

- EFB Not Fully Controlled
  - This is less restrictive than the assumptions in the previous work.
- EFB Connected Directly to the AID
  - This is our recommended approach, but discussion is provided for alternate approaches.
- Analysis is focused on “inside the aircraft skin”
  - i.e. Air/Ground Links are assumed to have link security, ground servers etc. are secure,
  - However, the importance of End-to-End security is recognized and discussed.

Component Analysis – AISD Network



	Access Vector	Confidentiality	Data Integrity	Authentication & Authorization	Availability
Existing Measu	Vector 1				
	Vector 2				
Additio Measu					
	Vector N				

Look for gaps in existing measures and fill them with new measures as necessary

AISD Network was found to be vulnerable to Denial of Service and Corruption of Data

AISD Network Additional Measures

Additional Physical Security

Domain Segregation for Shared A/G Links

Application Data Encryption

LAN Segregation (within the AISD)

Rate Limiting and Traffic Filtering

Security Measure	Description	Guidance and Security Implications
Security Measure	Description	Guidance and Security Implications
Security Measure	Description	Guidance and Security Implications
Security Measure	Description	Guidance and Security Implications
Security Measure Identifier	Description	Guidance and Security Implications
Rate Limiting	Network traffic rate limiting provides detection and volume control for defined data types and/or source and destination addresses within the network.	ARINC 664 Part 5, section 3.5.1 and others (ref 8) Also see the discussion in 5.2.2 Rate limiting provides an additional layer of protection for device availability on the network, by ensuring traffic volume falls within expected limits. Without this measure, devices on the network have increased exposure to availability threats.
Traffic Filtering	Network traffic filtering defines and enforces rules for the allowed source and destination addresses of various types of network traffic.	ARINC 664 Part 5 (ref 8) section 4.6.2 NIST Special Publication 800-41 Revision 1, Guidelines on Firewalls and Firewall policy (20) Traffic filtering provides an additional layer of protection for devices on the network, by limiting the types and sources of connections to those devices. Without this measure, devices on the network have increased exposure to

Summary

- Primary Threats
  - Denial of Service
  - Malicious and undetected corruption of assets

- Security Measures
  - Existing measures leave some gaps
  - Additional measures, such as rate limiting filters in the AISD, link security within the AISD and software protection should be applied

Analysis shows new applications are possible when appropriate security measures are applied, however this theoretical analysis should be validated and then shared with industry.

Current FY21 Accomplishments

- Completed assessment current and emerging flight deck information services technologies and architecture
  - Developed air/ground data interface alternatives technical report
- Conducted Cybersecurity risk assessment on EFB and AID, and flight deck IP Data Link
  - Developed cybersecurity risk assessment reports on
    1. EFB and AID,
    2. flight deck IP Data Link technologies and architecture
- Completed Technical Report on current and emerging technology and existing protocols for safety critical application (10/1)
- Completed two Test Cases for security analysis including (1) Negotiation, (2) Digital Taxi Instructions (11/1)
- Completed Analysis of Flight Deck Data Exchange Security for Safety Critical Data (1/20)

Anticipated Research in FY22

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. Expected research Products
- 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