Aircraft Systems Information Security / Protection (ASISP) R&D

NextGEN

7 October 2020

Presented to:

Research, Engineering and Development (RE&D) Advisory Committee (REDAC)

By Isidore Venetos

Manager, Cyber R&D

ANG-E2, Isidore.Venetos@faa.gov

609-485-5207

FAA

Purpose Of Brief

- **Brief the REDAC a high-level overview of the <u>aircraft cyber security research efforts</u>**

Initial Research Problem Statement:

How to assess aircraft cyber risks and determine appropriate mitigations?

FAA

NextGEN

Briefing Outline – Two Parts

1) **High level brief of FAA Cyber-R&D Safety Risk Assessment methodology**

- A Cyber Risk-Based Decision-Making (RBDM) Approach

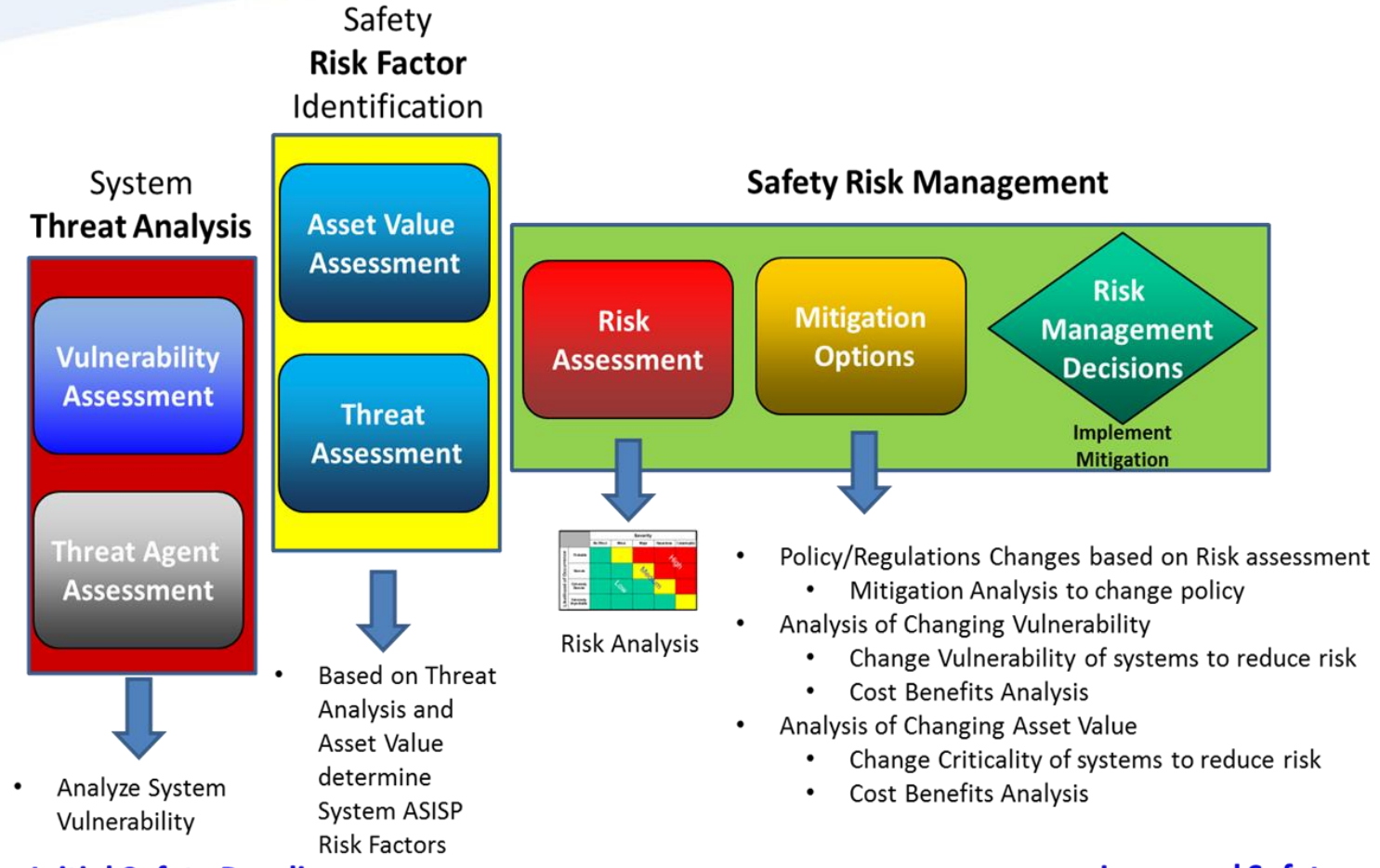
2) **Industry use of methodology & Future R&D**

- Cyber Safety Commercial Aviation Team (CS CAT)
- Foundational Cyber Risk Assessment process for CS CAT

PART I

High level brief of FAA Cyber-R&D Safety Risk Assessment methodology

ASISP Safety Risk Assessment Research Framework



FAA NextGEN

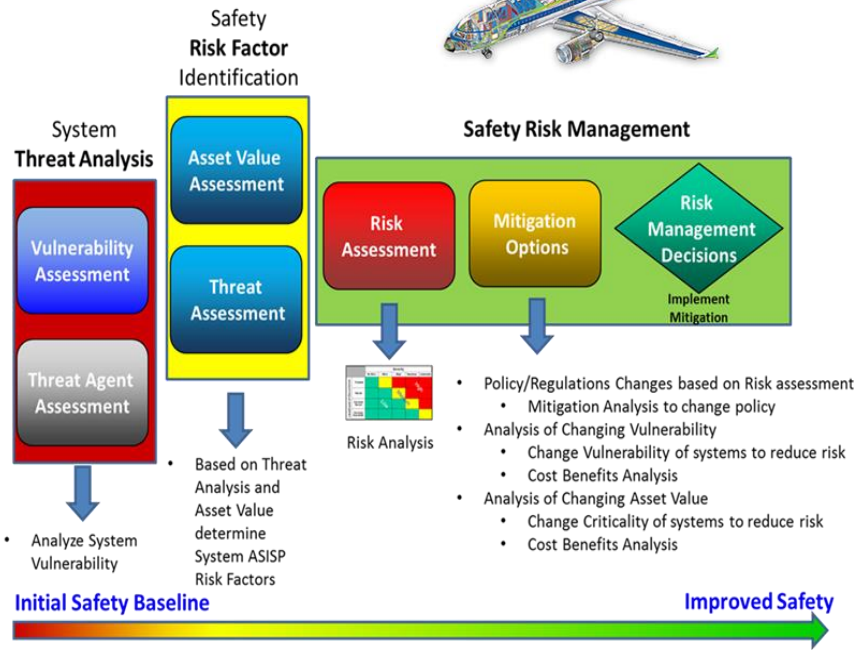
Analytical risk-based decision-making (RBDM) approach

NOT a regulatory-based approach;

Aircraft Systems Information Security Protection (ASISP) Goals

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



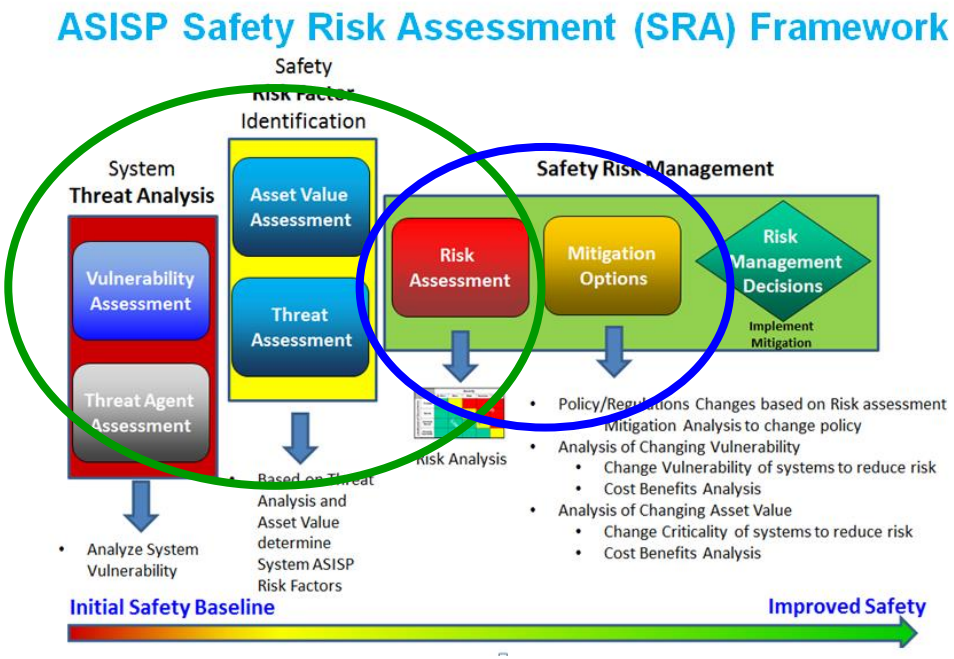
Supports collaborative team approach to drive a consensus -based approach to risks and mitigations

FAA

NextGEN

ANG Sep 2015 SAS Brief
Three-Phase Approach: **2016-2020**

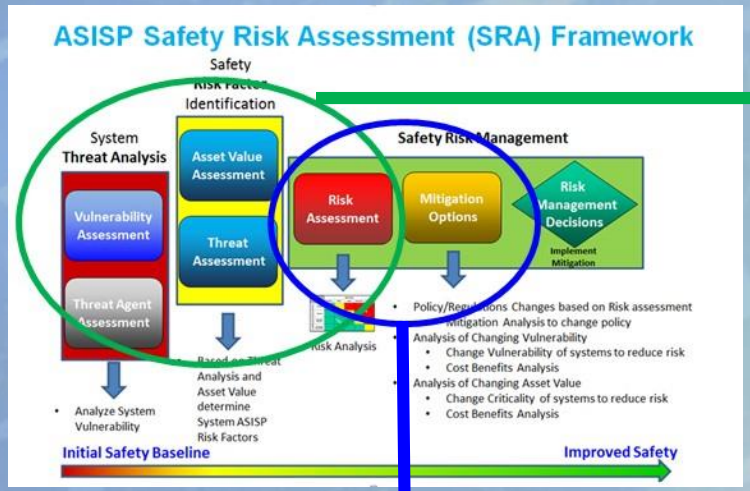
- PHASE I: Identify ASISP Interfaces and conduct Risk Assessments FY16-FY17 (Risk Characterization)
- PHASE II: Extend the Risk assessments to the development of Mitigation Techniques FY18-FY20 (Mitigation ID)
- PHASE III: Identify Recommended ASISP Community Strategies for aircraft certification, maintenance and continued operational safety FY19-FY20 (Industry/Other Gvmt)



ORIGINAL INTENT: ***Support AVS decision-making*** **related to ASISP policy and regulation to promote aviation safety by** ***reducing risk*** **from deliberate attempts to corrupt or usurp** ***aircraft information systems***

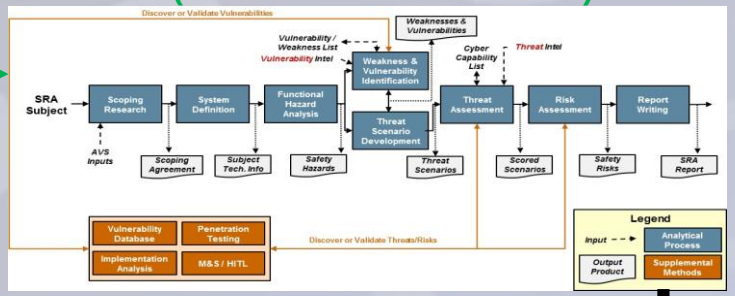
Primary Research Question

How can a methodology be developed and applied to aircraft aviation systems to assess "cyber" risks and understand effective mitigation strategies that will enable promotion of safety from cyber threats to commercial aviation in the NAS?



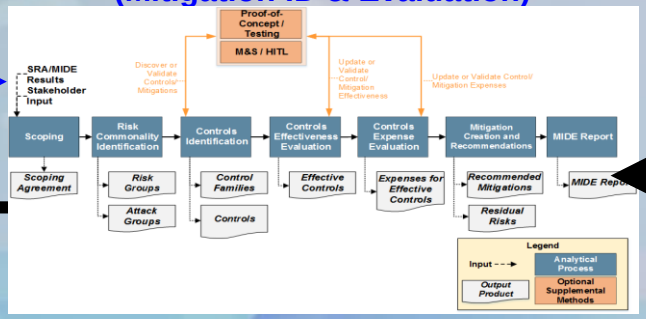
Part 1 SRA Methodology, V1.1

(Risk ID & Characterization)



Part 2 SRA Methodology

(Mitigation ID & Evaluation)



ASISP SRA Report with Initial Risk

ASISP SRA Report with Residual Risk

ASISP Cyber SRA Development

- **Apply sound system engineering principles** and work with various agencies to understand the risks
- Cyber Safety Risk Assessments (SRAs) based on a repeatable methodology
- Partnering with federal research organizations and industry

MIT LINCOLN LABORATORY

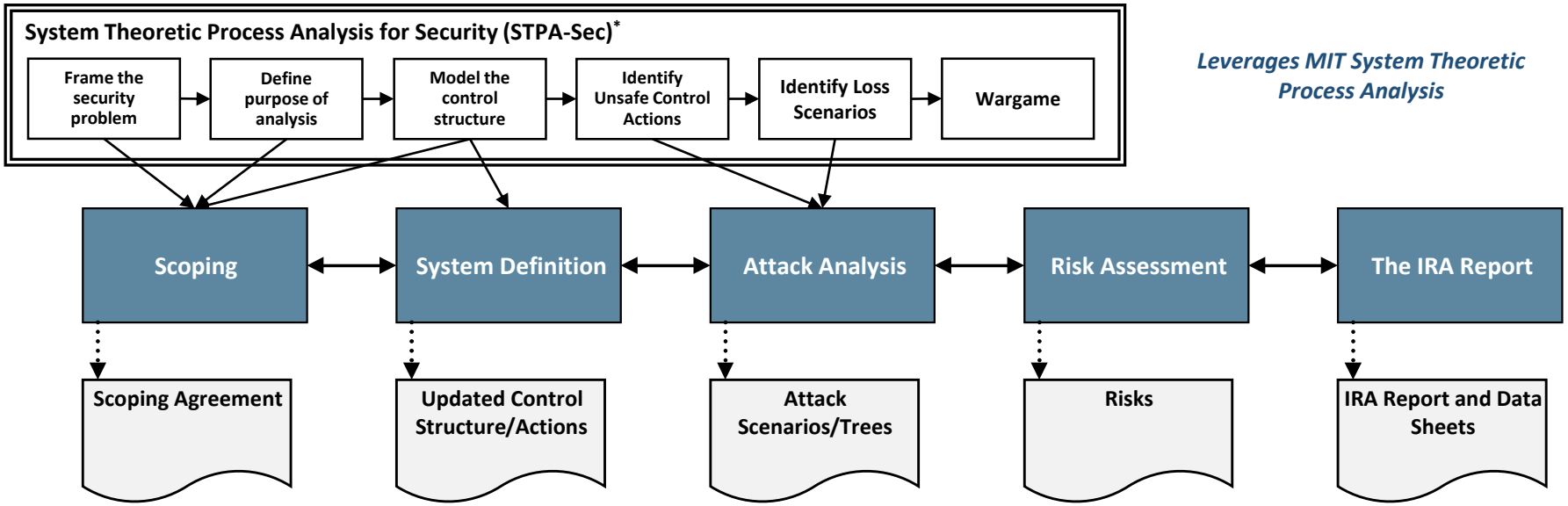
APL JOHNS HOPKINS APPLIED PHYSICS LABORATORY

Astronautics Corporation of America

FAA

NextGEN

STPA-Sec to Initial Risk Assessment (IRA) Methodology



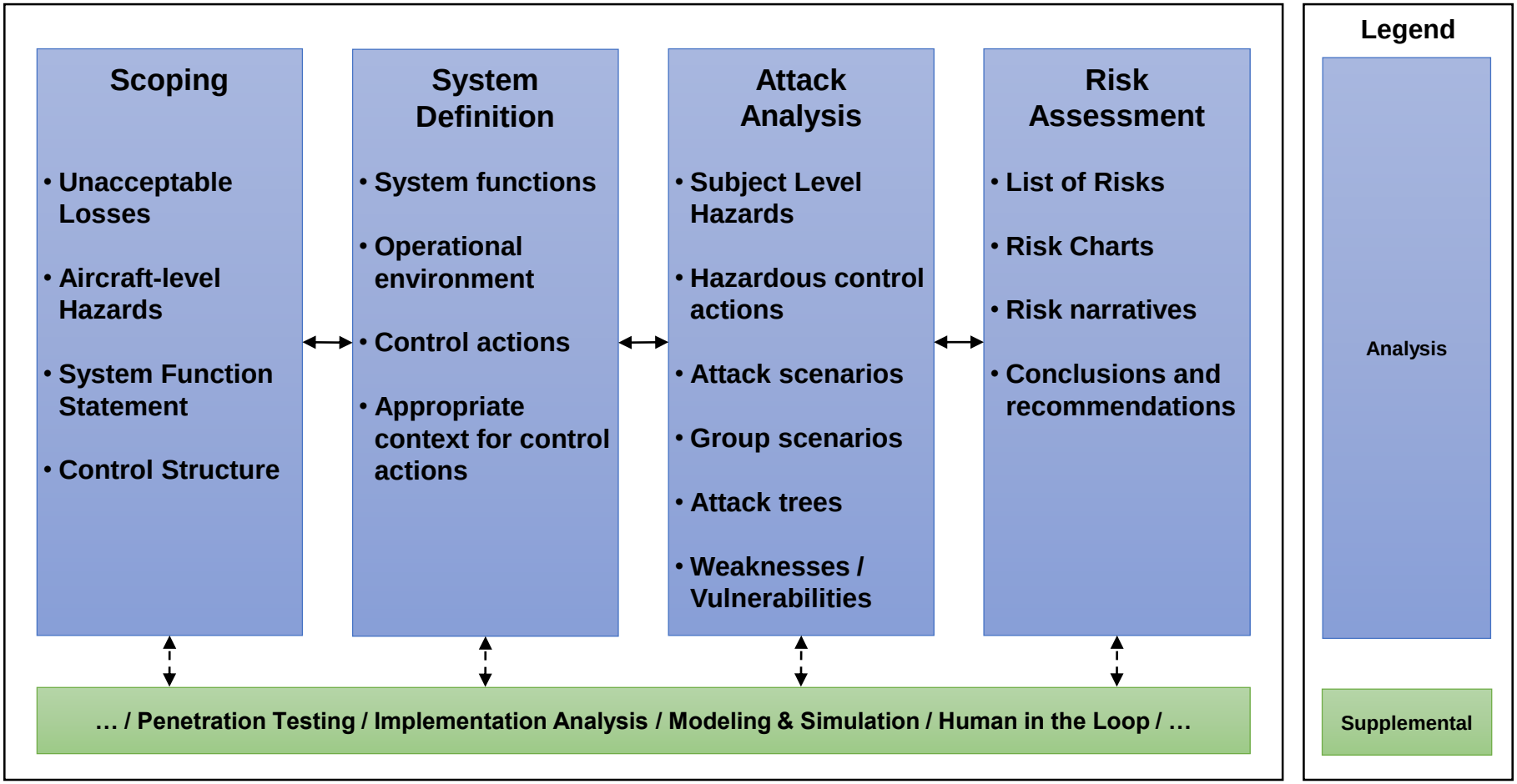
Leverages MIT System Theoretic Process Analysis

- STPA-Sec provides
  - Qualitative formal process
  - Analysis of whole system
  - Top-down approach
- Why not traditional tools?
  - Focused on reliability
  - Do not handle complexity of modern systems well
  - Bottom-up approach

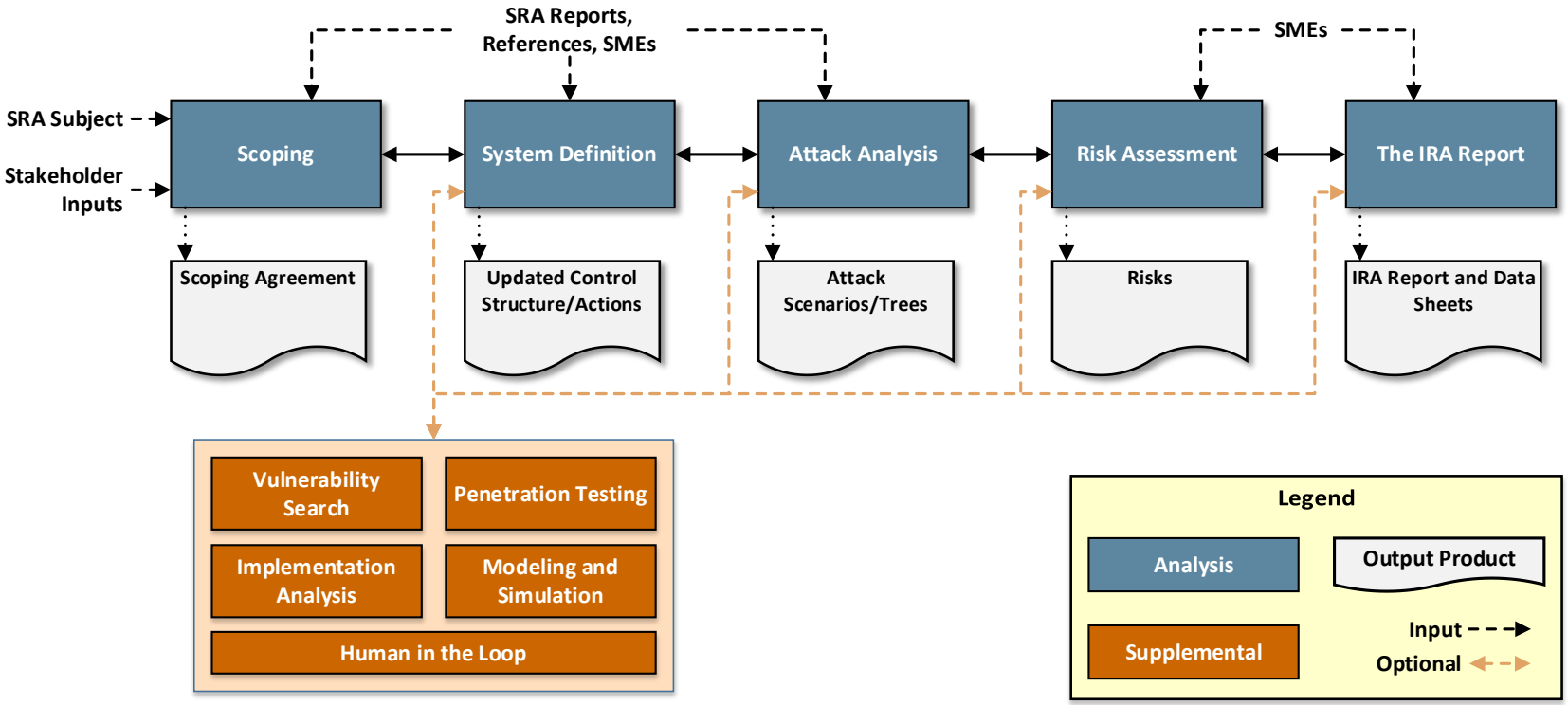
*STPA-Sec process from STPA-Sec Overview, STAMP 2019 Workshop, Slide 22

Safety Risk Assessment (SRA) Methodology

Part 1 – Initial Risk Assessment

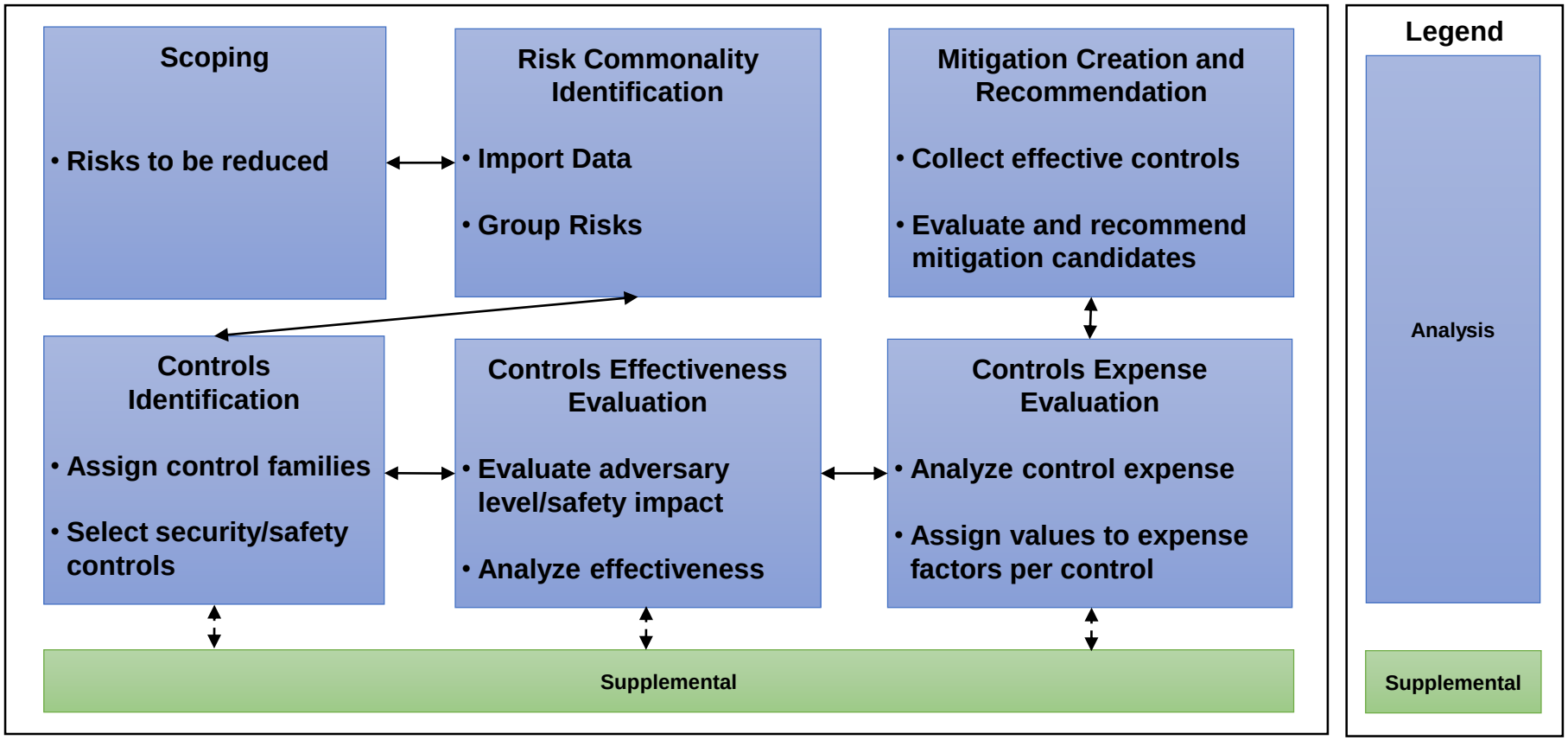


SRA Process Overview
Initial Risk Assessment (Part 1)

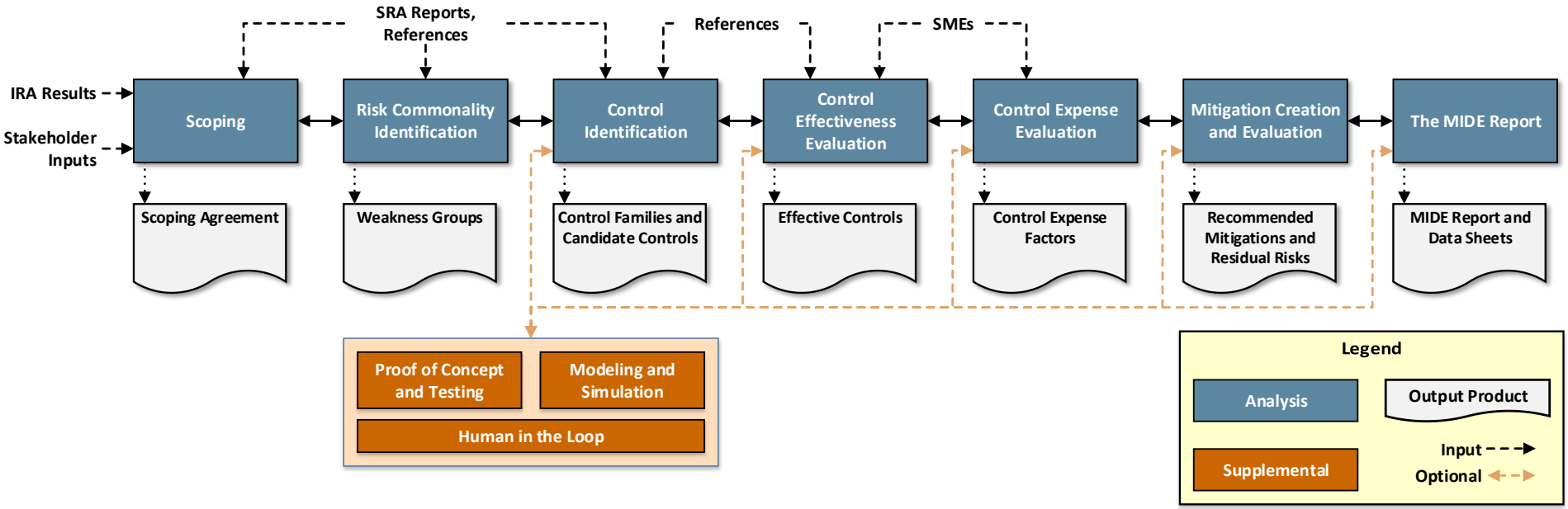


Safety Risk Assessment (SRA) Methodology

Part 2 – Mitigation Identification and Evaluation

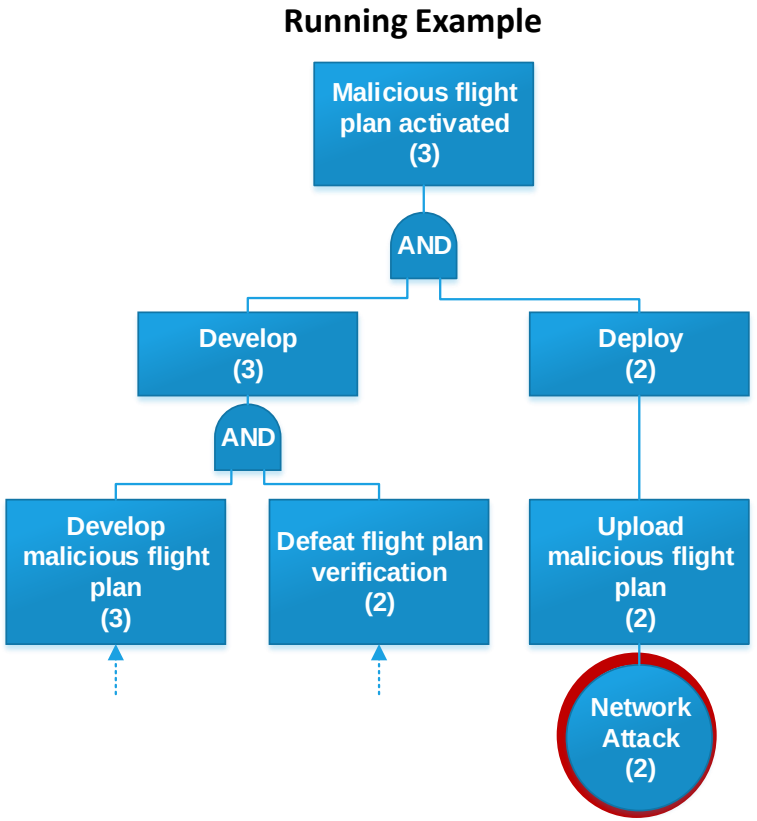


SRA Process Overview Mitigation Identification and Evaluation (Part 2)



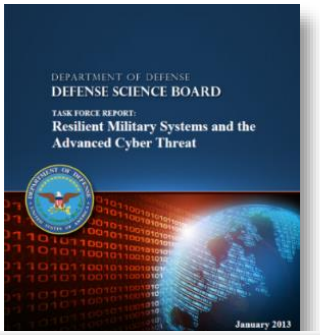
Attack Tree Generation

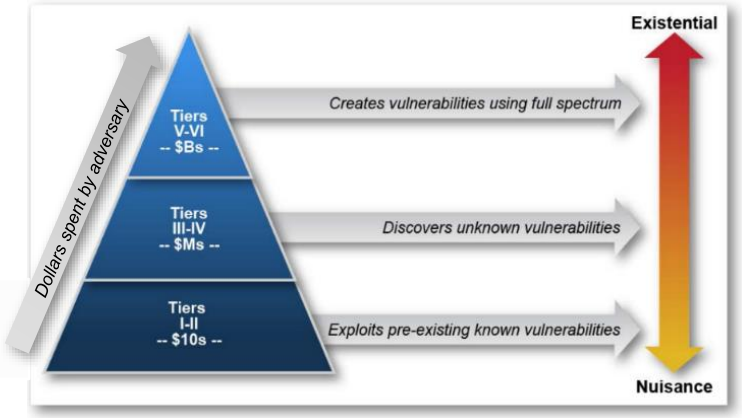
- Group attack scenarios by attack type, scenario end effect, and safety impact
- Develop attack tree for each scenario group that represents
  - Steps necessary to execute the HCA
  - Adversary capabilities required to execute the steps
- Assign capability scores to leaf nodes and propagate upward
  - AND is max
  - OR is min



Threat Assessment

- Conventional risk (evaluation of threat) requires two items
  - Safety Impact (Catastrophic, Hazardous, Major, Minor, No Effect)
  - A probability of occurrence
- Adversarial levels provide proxy for probability (inspired by resource pyramid)
  - 1: Novice/Intermediate
  - 2: Proficient
  - 3: Organized Group
  - 4: Lesser Nation State
  - 5: Greater Nation State





Evaluate Mitigations

- Select Mitigations Alternatives
  - Do the mitigations meet stakeholder objectives?
  - Which mitigations are most effective?

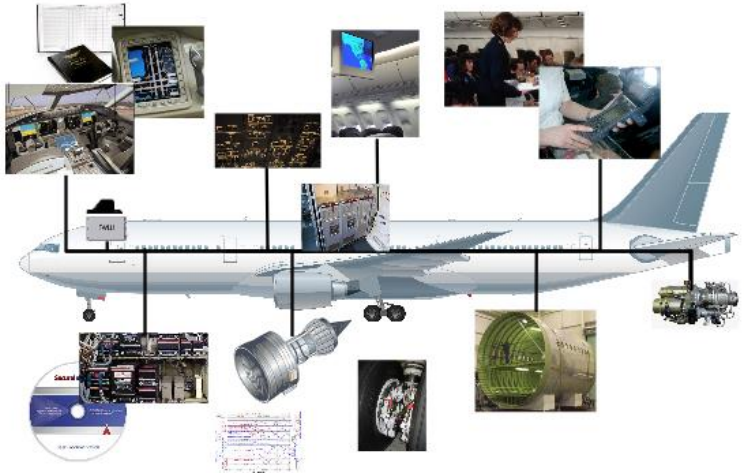
Risk ID	Mitigation ID	Selected Controls	Residual Safety Impact	Residual Individual Adversary Level	Total Mitigation Cost	Total Mitigation Time	System Impact Expense
…	…	…	…	…	…	…	…

- Create Risk Chart(s)
  - Show the residual risk after different mitigations have been applied to a Risk

NOTIONAL	Safety Impact: Minor	Major	Hazardous	Catastrophic
Required Adversary Level: Novice/Intermediate			CR5	
Proficient				
Organized Group			M4	
Lesser Nation State		M5	M2	
Greater Nation State				

Cyber SRA Subjects Researched

Aircraft Communications Addressing and Reporting System (ACARS)



Aircraft Interface Device (AID)

Field-Loadable Software (FLS)

Flight Management Systems

FAA

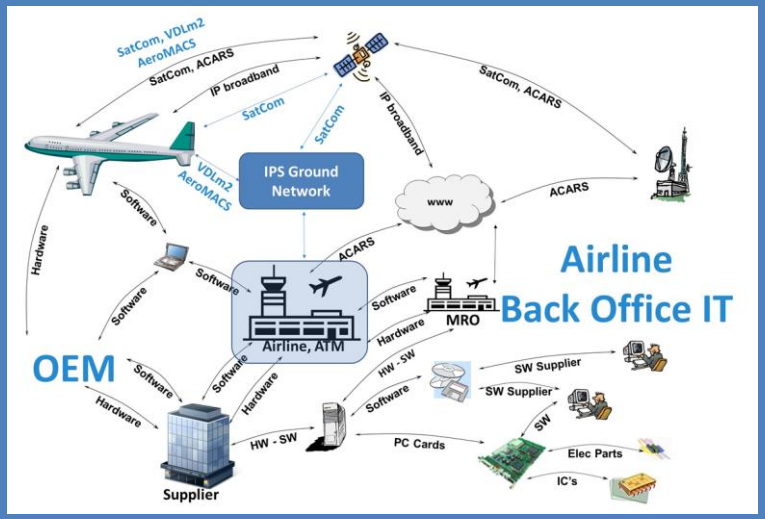
NextGEN

Cyber SRA End-to-End System Analysis

Aircraft Communications Addressing and Reporting System (ACARS)

Field-Loadable Software (FLS)

FAA



Air Traffic Services (ATS) Internet Protocol Suite (IPS)

AEROSPACE INDUSTRIES ASSOCIATION

ICAO

November 2020 completion

Electronic Interface Device (EID)

Flight Management Systems

NextGEN

The Aviation Ecosystem: Phases of Flight

FOR OFFICIAL USE ONLY (FOUO)

O FAA Oversight | R FAA Responsibility | sR FAA Shared Responsibility | FAA No Involvement

	Plan the Flight	Before the Flight		During the Flight			After the Flight
		At the Terminal	On the Tarmac	Take Off	Enroute	Landing	
Aircraft	O Engineering Design O Manufacturing O Flight Test O Electronic Flight Bags	Electronic Flight Bags	O Avionics				
Airlines	O Modifications (WiFi, USB Ports, etc) Reservation Systems Financial Systems sR Scheduling/Planning Airlift/Air Freight Systems Airline Websites	Reservation Systems Check-In Counters Baggage Systems Boarding Systems	Airline Operations Center (AOC) Comms sR Flight Plans Ground Support Systems Electronic Flight Bags	O Avionics O Cabin Systems sR Cabin Crew Automation (POS devices, In-flight manual, etc.) O Passenger Devices sR Continued Operation Safety (FAA, TSA)			Baggage Systems Ground Support Systems O Maintenance O Modifications Airlift/Air Freight Systems
Airports	sR Scheduling/Planning	Passenger Screening (TSA, CBP) Physical Security (Inside & Outside Terminal) Infrastructure: Buildings, Lighting, Signage, Comms Baggage Systems	sR Infrastructure: Lighting, Radar sR Ground Control O Ground Support Systems	O Airline Operations Area (AOA) Access			Baggage Systems Ground Support Systems sR Ground Control Infrastructure: Buildings, Lighting, Signage, Comms
Aviation Operators	sR Scheduling/Planning & Flight Plans R Certification R Inspection		sR Ground Control R Certification R Inspection	R Terminal Control	R Enroute/Oceanic Control	R Terminal Control	sR Ground Control R Certification R Inspection
Actors	Passengers Airline Staff Original Equipment Manufacturer (OEM) Staff TSA, CBP Airlift/Air Freight Staff	Airport Staff	Airport Staff sR Air Crew (FAA, TSA) sR Inspectors (FAA, TSA)	Airline Staff (Non-Rev) sR Air Crew (FAA, TSA) R Controllers Airlift/Air Freight			Airline Staff / CTRs Airport Staff / CTRs sR Inspectors (FAA, TSA) O Technicians / Mechanics
Dependencies			Telecommunications (FCC) GPS (DoD) sR NavAids (FAA, Airports, DoD) sR Passenger Devices (FAA, TSA, PHMSA)				

18.AUGUST.2017

Methodology can be applied across ecosystem – have begun discussion with airports

Primary ASISP Research Products

Phase 1

1. Problem-Space report (MSAG & LL)
2. SRA subjects report with suggested prioritization (MSAG & LL)
3. Four independent SRA methodologies (MSAG, LL, ACA, APL)
4. Four independent ACARS SRA reports (MSAG, LL, ACA, APL)
5. Initial EFB SRA report (ACA)

Phase 2

6. Integrated ASISP Part 1 (risk characterization) **SRA Methodology v1.1** (LL & ACA)
7. **FLS Part 1** SRA report (LL)
8. **EIF Part 1** SRA report (ACA)
9. **ACARS** Summary **Part 1** SRA report (ANG w/team)
10. Two independent Part 2 (mitigation) Methodologies (LL & ACA) [First Draft]
11. Integrated Part 2 Methodology (LL & ACA)
12. **EIF Part 2** SRA report (ACA)
13. **ACARS Part 2** SRA report (LL)

Phase 3

14. **CRADAs** with Collins Aerospace and GE Aviation; **multiparty agreement** w/Boeing, GE, Collins
15. Joint FMS SRA Scope Agreement (6 parties; no Boeing concurrence)
16. Integrated Parts 1&2 **SRA Methodology v 2.0** (LL & ACA)
17. **Joint FMS Part 1** SRA report (includes supplemental evaluation)
18. **Joint FMS Part 2** SRA report
19. **Joint ATS over IPS SRA** Scope Agreement (multiple parties through CS-CAT)
20. **Joint ATS over IPS Interim Part 1** SRA report (multiple parties through CS-CAT)
21. SRA Methodology tool requirements

FAA Benefits and Success
Aircraft Cyber R&D

- Developed an aviation-specific **Cyber Safety Risk Assessment (SRA) methodology**
  - Assess cyber risks on complex cyber physical systems and applied the SRA methodology to aircraft systems
  - SRA Methodology is compliant with FAA Order 8040-4b with potential for integration into Safety Management Systems(SMS) SRA processes
  - Helped address some of the Aircraft Systems Information Security/ Protection (ASISP) Aviation Rulemaking Advisory Committee (ARAC) recommendations

FAA Benefits and Success
Aircraft Cyber R&D

- **Provided industry the Cyber SRA methodology and facilitated transition** for initial industry-led cyber Safety risk assessments
- Supporting the establishment of the **Cyber Safety Commercial Aviation Team (CS CAT)**
  - Methodology provides top down approach conducive to industry & government collaboration
  - Analytical and system analysis
- CS CAT is targeting integration of CS CAT into the **Commercial Aviation Safety Team** (CAST)

FAA

NextGEN

PART II

ASISP Safety Risk Assessment methodology leading to the development of Cyber Safety Commercial Aviation Team (CS CAT)

FAA

NextGEN

Cyber Safety
Commercial Aviation Team

Vision

- Data driven risk based collaborative cyber safety decision making
- US-based response to EASA European Strategic Coordination Platform (ESCP) to address end-to-end aviation cybersecurity and develop actionable plans.
- Partnership amongst aviation industry stakeholders to address evolving aviation environment and new cyber threats to safety.

Mission

- Proactive identification & mitigation of aviation ecosystem cyber safety risks

Goals

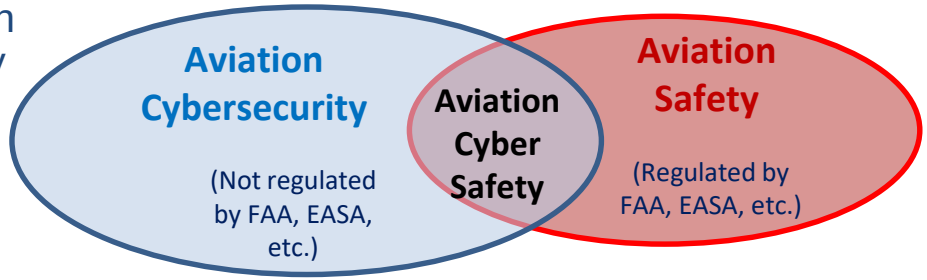
- Reduce U.S. commercial aviation cyber safety risk
- Work with international partners to reduce cyber safety risk world-wide

Outcomes

- Identification of risks & actionable ecosystem mitigation recommendations for:
  - Best practices, standards & technology development
  - Aviation cyber safety incident communications & response plans
  - EASA/ESCP Harmonization & ICAO Influence
  - Guidance & policy as needed

What is Aviation Cyber Safety Within The Aviation Ecosystem

Cyber Safety hazards include all threat vectors from interconnectivity of the aviation ecosystem that can impact aircraft safety. This includes interoperability and efficiency related safety impacts to air/ground resources that have:

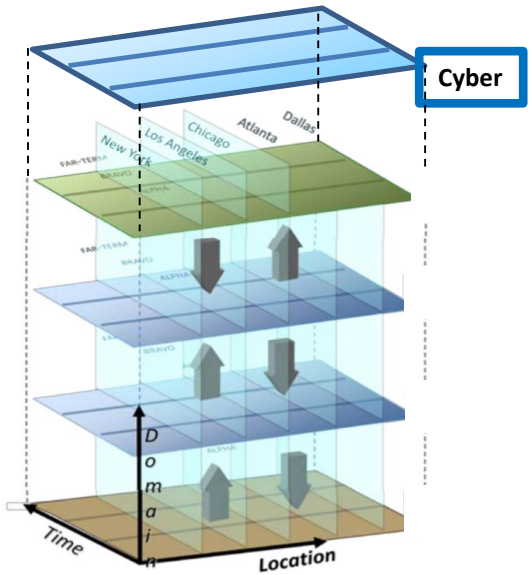


- An ability to directly effect ATM services
  - Pilot decision making or aircraft control systems
  - Air-to-Ground Voice and Data
- Direct impact to the interoperability between ATM stakeholders responsible for providing critical and safety services
  - Aerodrome (airport connections to NAS/Airplane)
  - Air Navigation Service Providers (ANSP)
  - Communications providers (air, space and ground)
  - Aircraft and Avionics manufacturers
  - Aircraft Operators
- An effect on airspace capacity and efficiency

International Coordinating Council of Aerospace Industries Associations

Aviation Safety provides a Robust Framework to Leverage

Cyber Safety Overlay and Integration



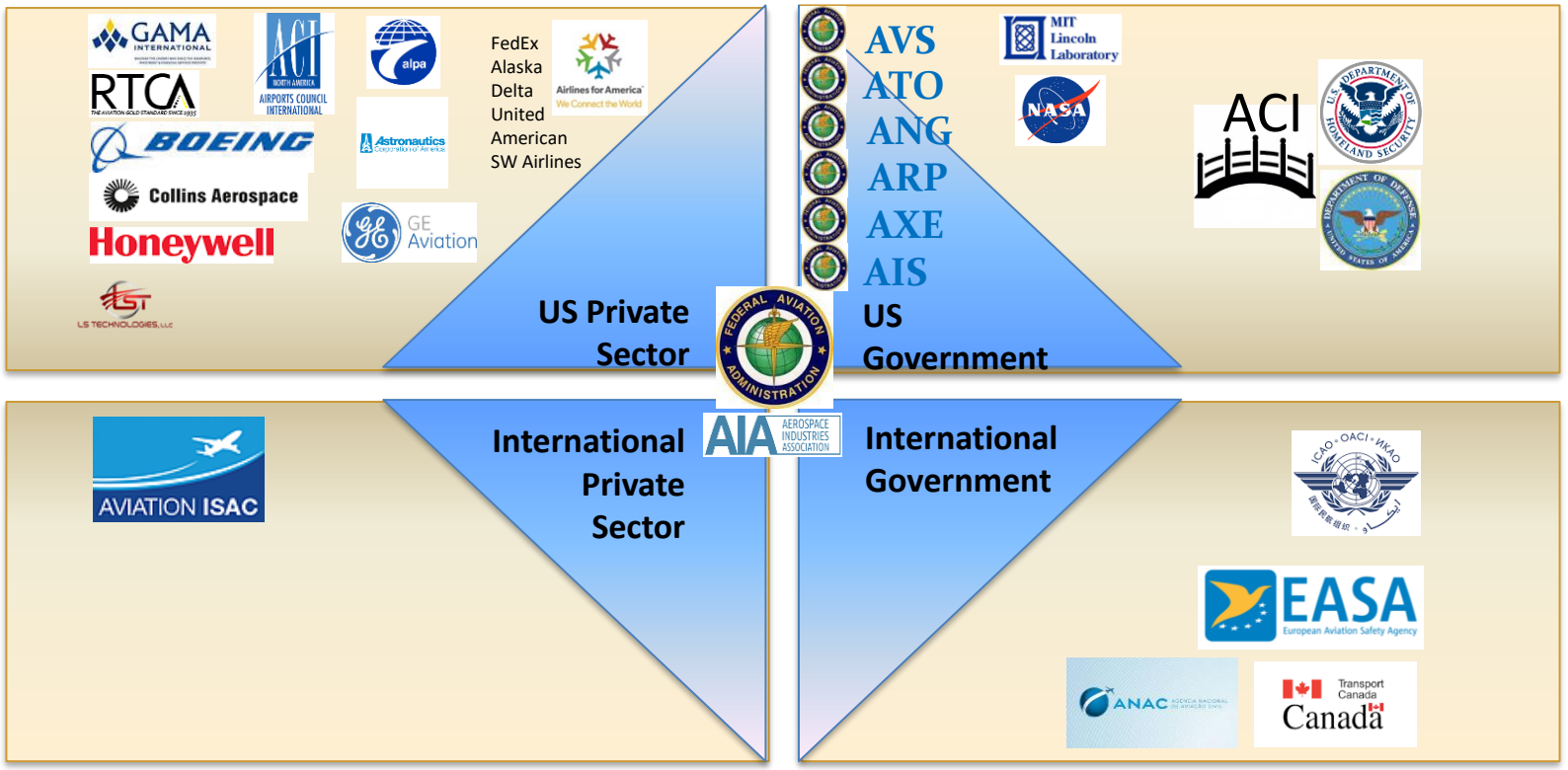
The Complex Integration Aspects of a Capability

https://www.faa.gov/air_traffic/publications/media/ATO-SMS-Manual.pdf

- Cyber Safety capabilities & controls
  - Leverage Power of Aviation Safety Community
  - Complement existing Aviation organizations, processes and relationships
  - Integrate into existing Aviation Safety controls and environment
- Cyber crosses and overlays the various domains (Aircraft, Operations, Air Traffic Managements (ATM) , Airports)

Cyber needs to be assessed across all SMS Domains

Cyber Safety Commercial Aviation Team (CAT) Preliminary Partners/Structure



Industry & Government Partnership is Imperative for a Strong Safety + Security Culture.

Cyber Safety CAT Data Management Model

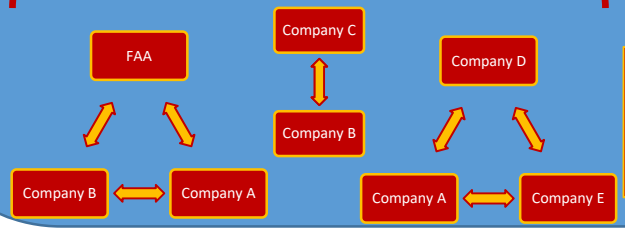
Cyber Safety Commercial Aviation Team

Data Handling Model

Information Detail & Sensitivity

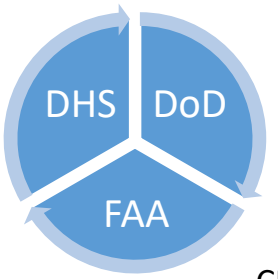
Data Sharing levels

- **Open**
  - Shared Openly
  - Final Outcomes / Recommendations (US, ICAO, EASA, …)
- **Sector**
  - Targeted Aviation Sector Sharing
  - High level results
- **Members**
  - CS CAT Members
  - Working Level Security Data
- **Limited**
  - CS CAT Sub-set Only
  - Very Limited sharing



Participant Multi way Limited Proprietary Data

Partners / Data Sharing



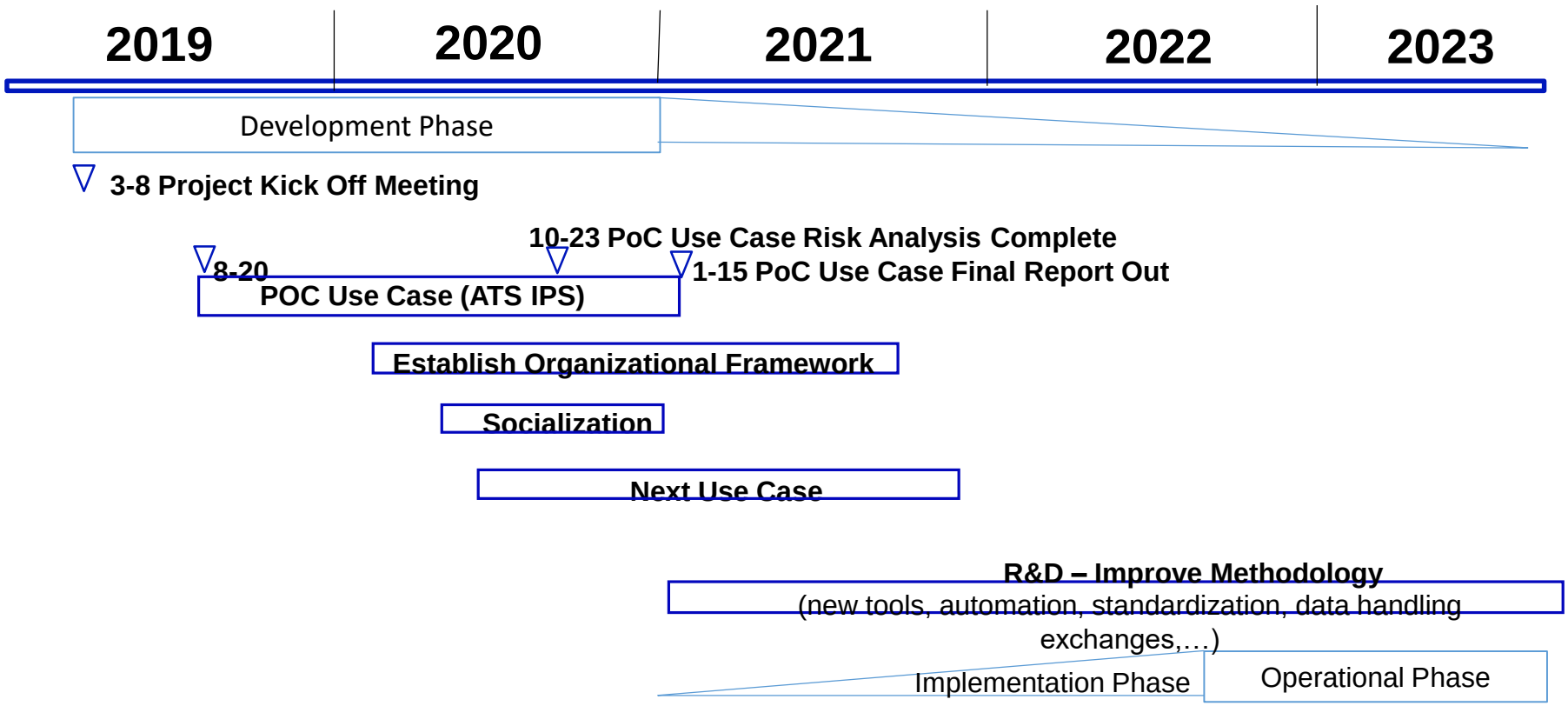
ACI Tri-Chair

CISA Central

Unclassified Data Only

AVIATION ISAC

Cyber Safety CAT Proposed Timeline



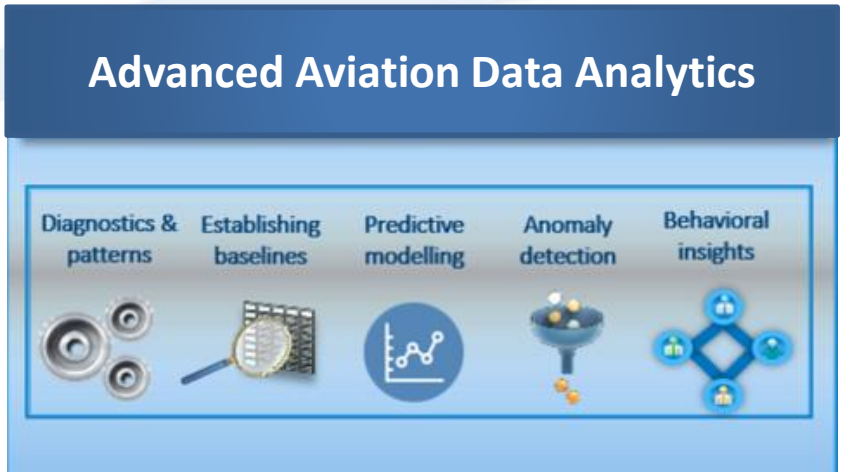
Contacts
(Cyber Safety Commercial Aviation Team)

Dan Diessner
Boeing Commercial Airplanes – Product Cybersecurity Senior Manager
AIA Civil Aviation Cybersecurity Subcommittee Chair
daniel.j.diessner@boeing.com

Susan Cabler
Federal Aviation Administration
Aviation Safety Organization (AVS)
susan.cabler@faa.gov

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

Future Research: Cyber Security Data Science



- Extend research for CS CAT to also utilize Cybersecurity Data Science (CSDS) principles
- CSDS to use Artificial Intelligence and Machine Learning in the data rich Aviation Ecosystem (NAS 2035 Vision)
- CSDS offers a path forward to utilize data rich environments besieged by unknown-unknowns

FAA

NextGEN

CSDS CONCEPT IN PLANNING PHASE

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

FAA

NextGEN