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

2 September 2020

Presented to:
REDAC NAS OPS

By Isidore Venetos
Manager, Cyber R&D
ANG-E2, Isidore.Venetos@faa.gov
609-485-5207

Purpose Of Brief

- Brief the NAS Operations subcommittee a high-level overview of the aircraft cyber security research efforts

Initial Research Problem Statement:

How to assess aircraft cyber risks and determine appropriate mitigations?

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

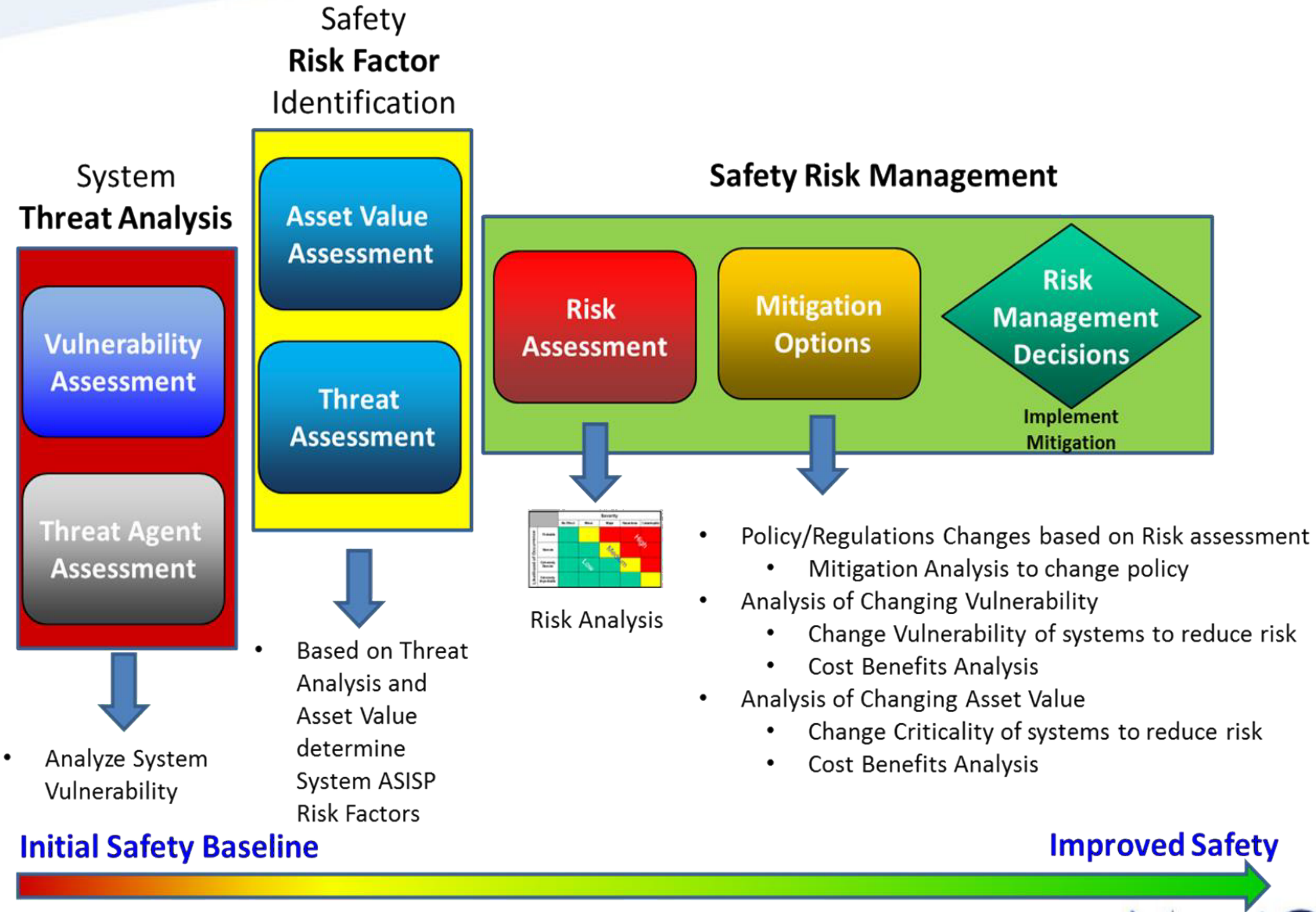
2) Industry use of methodolgy

- 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



System **Threat Analysis**

Vulnerability Assessment

Threat Agent Assessment

- Analyze System Vulnerability

Safety **Risk Factor** Identification

Asset Value Assessment

Threat Assessment

- Based on Threat Analysis and Asset Value determine System ASISP Risk Factors

Safety Risk Management

Risk Assessment

Mitigation Options

Risk Management Decisions

Implement Mitigation

Risk Analysis

- Policy/Regulations Changes based on Risk assessment
  - Mitigation Analysis to change policy
- Analysis of Changing Vulnerability
  - Change Vulnerability of systems to reduce risk
  - Cost Benefits Analysis
- Analysis of Changing Asset Value
  - Change Criticality of systems to reduce risk
  - Cost Benefits Analysis

Initial Safety Baseline

Improved Safety

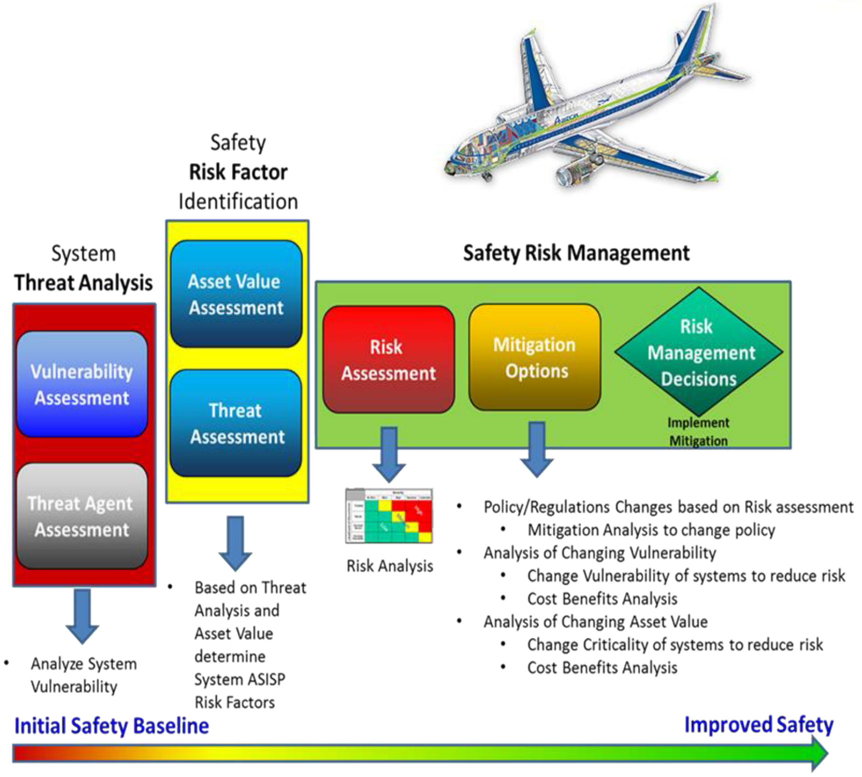
Analytical risk-based decision-making (RBDM) approach

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

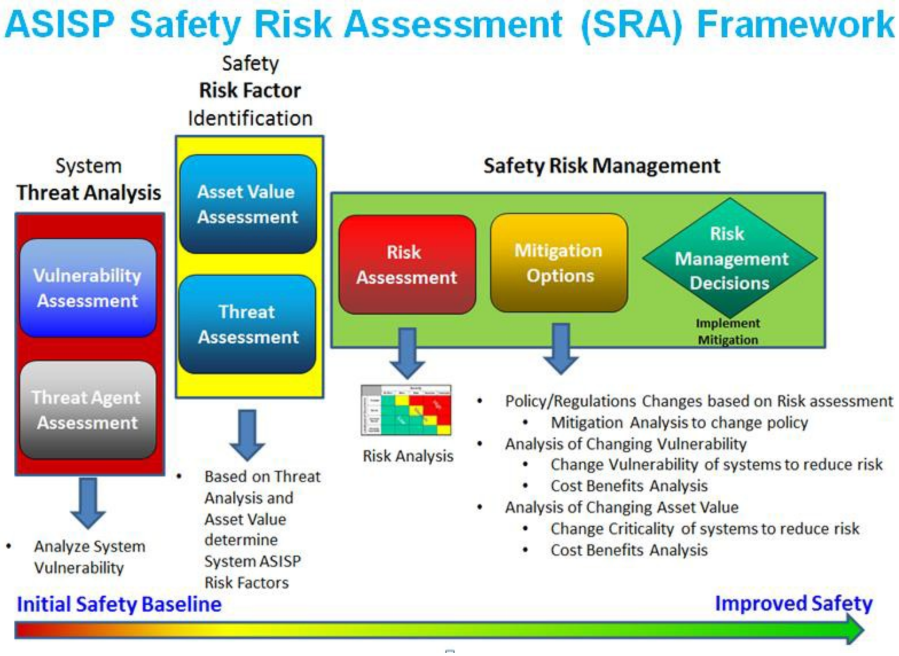
- Allows consistent standard outputs
- Structured methodology
- Repeatable and Validated processes
- Removes assessment bias
- Consistent with the Safety Management Systems (SMS)- Safety Risk Management (SRM) and Risk-Based Decision-Making (RBDM) principles FAA strategic initiative


System Threat Analysis
Vulnerability Assessment
Threat Agent Assessment
Analyze System Vulnerability
Safety Risk Factor Identification
Asset Value Assessment
Threat Assessment
Based on Threat Analysis and Asset Value determine System ASISP Risk Factors
Safety Risk Management
Risk Assessment
Mitigation Options
Risk Management Decisions
Implement Mitigation
Risk Analysis
Policy/Regulations Changes based on Risk assessment
Mitigation Analysis to change policy
Analysis of Changing Vulnerability
Change Vulnerability of systems to reduce risk
Cost Benefits Analysis
Analysis of Changing Asset Value
Change Criticality of systems to reduce risk
Cost Benefits Analysis
Initial Safety Baseline
Improved Safety

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

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)



ASISP Safety Risk Assessment (SRA) Framework

System Threat Analysis

Vulnerability Assessment

Threat Agent Assessment

- Analyze System Vulnerability

Safety Risk Factor Identification

Asset Value Assessment

Threat Assessment

- Based on Threat Analysis and Asset Value determine System ASISP Risk Factors

Safety Risk Management

Risk Assessment

Mitigation Options

Risk Management Decisions

Implement Mitigation

Risk Analysis

- Policy/Regulations Changes based on Risk assessment
  - Mitigation Analysis to change policy
- Analysis of Changing Vulnerability
  - Change Vulnerability of systems to reduce risk
  - Cost Benefits Analysis
- Analysis of Changing Asset Value
  - Change Criticality of systems to reduce risk
  - Cost Benefits Analysis

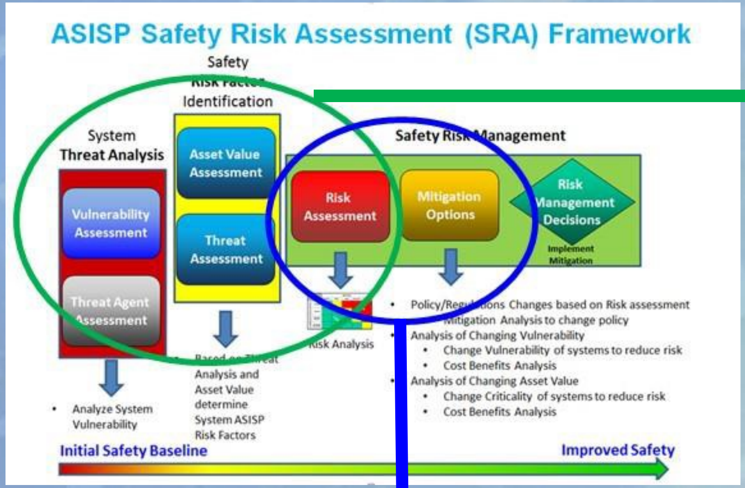
Initial Safety Baseline

Improved Safety

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



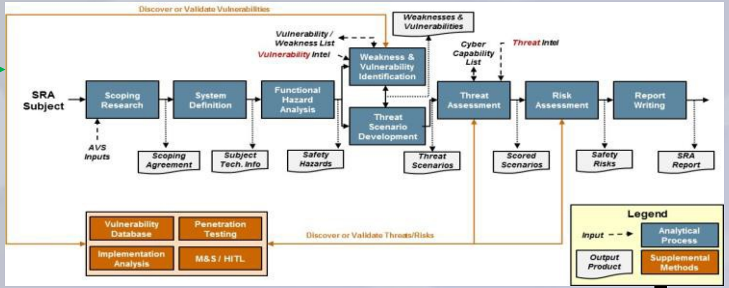
- Analyze System Vulnerability

Based on Threat Analysis and Asset Value determine System ASISP Risk Factors

- Policy/Regulations Changes based on Risk assessment
  - Mitigation Analysis to change policy
- Analysis of Changing Vulnerability
  - Change Vulnerability of systems to reduce risk
  - Cost Benefits Analysis
- Analysis of Changing Asset Value
  - Change Criticality of systems to reduce risk
  - Cost Benefits Analysis

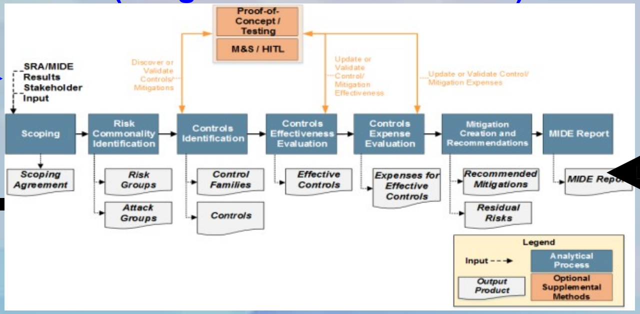
<u>Part 1</u> SRA Methodology, V1.1

(Risk ID & Characterization)



<u>Part 2</u> SRA Methodology

(Mitigation ID & Evaluation)


Proof-of-Concept / Testing
M&S / HITL
SRA/MIDE Results
Stakeholder Input
Discover or Validate Controls/ Mitigations
Update or Validate Control/ Mitigation Effectiveness
Update or Validate Control/ Mitigation Expenses
Scoping
Risk Commonality Identification
Controls Identification
Controls Effectiveness Evaluation
Controls Expense Evaluation
Mitigation Creation and Recommendations
MIDE Report
Scoping Agreement
Risk Groups
Attack Groups
Control Families
Controls
Effective Controls
Expenses for Effective Controls
Recommended Mitigations
Residual Risks
MIDE Report
Legend
Input
Analytical Process
Output Product
Optional Supplemental Methods

ASISP SRA
Report with
<u>Initial</u> Risk

ASISP SRA
Report with
<u>Residual</u> 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

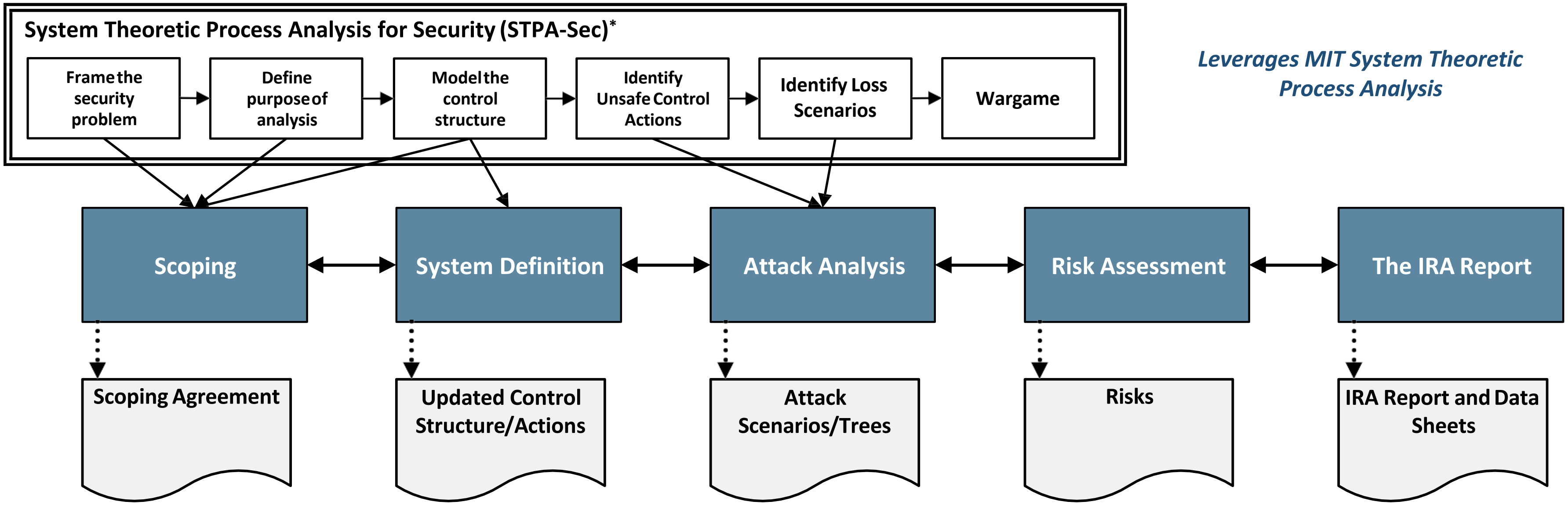
APL JOHNS HOPKINS APPLIED PHYSICS LABORATORY

Astronautics Corporation of America

FAA

NextGEN

STPA-Sec to Initial Risk Assessment (IRA) Methodology


System Theoretic Process Analysis for Security (STPA-Sec)*
Frame the security problem
Define purpose of analysis
Model the control structure
Identify Unsafe Control Actions
Identify Loss Scenarios
Wargame
Scoping
System Definition
Attack Analysis
Risk Assessment
The IRA Report
Scoping Agreement
Updated Control Structure/Actions
Attack Scenarios/Trees
Risks
IRA Report and Data Sheets

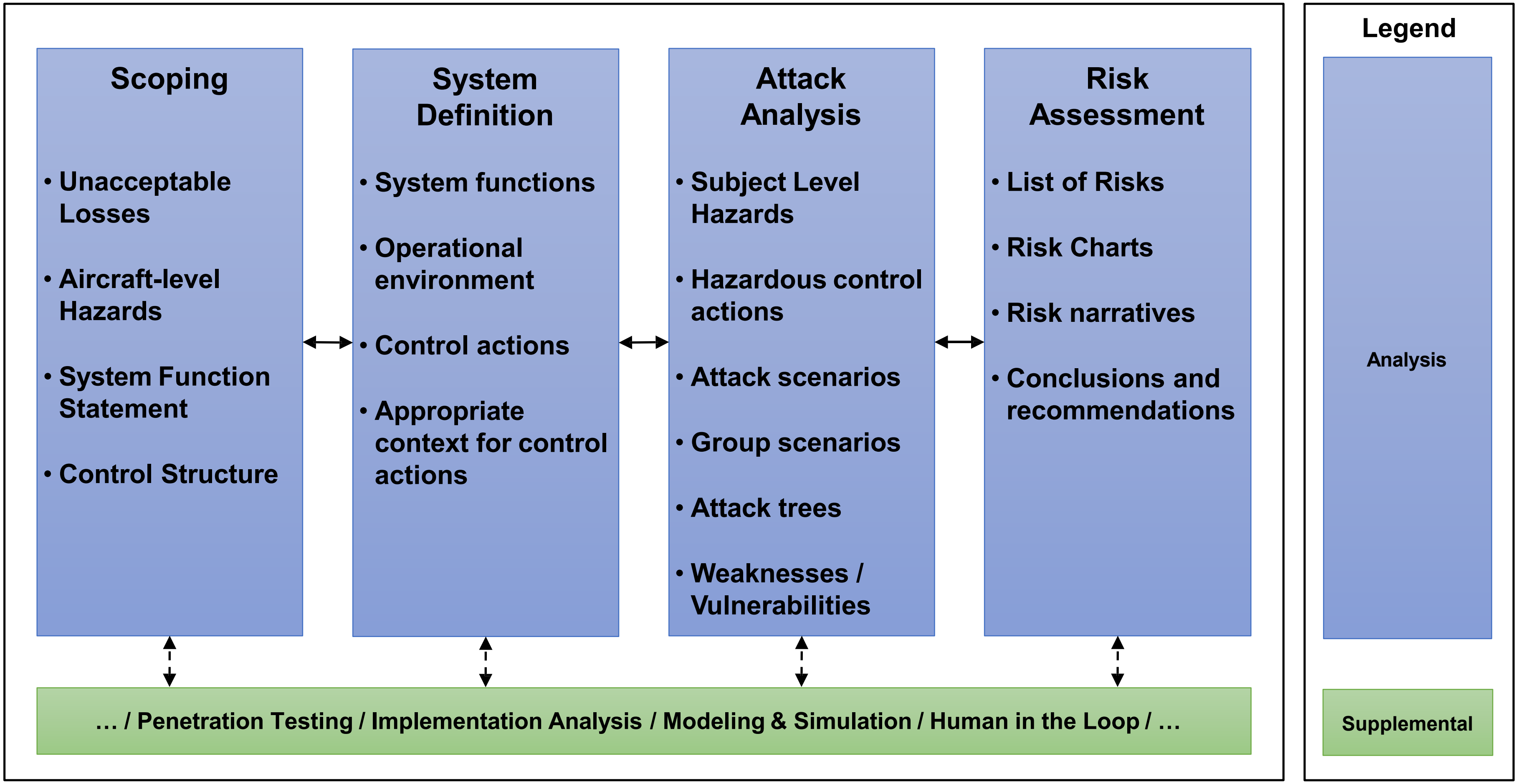
Leverages MIT System Theoretic Process Analysis

- 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



Scoping

- Unacceptable Losses
- Aircraft-level Hazards
- System Function Statement
- Control Structure

System Definition

- System functions
- Operational environment
- Control actions
- Appropriate context for control actions

Attack Analysis

- Subject Level Hazards
- Hazardous control actions
- Attack scenarios
- Group scenarios
- Attack trees
- Weaknesses / Vulnerabilities

Risk Assessment

- List of Risks
- Risk Charts
- Risk narratives
- Conclusions and recommendations

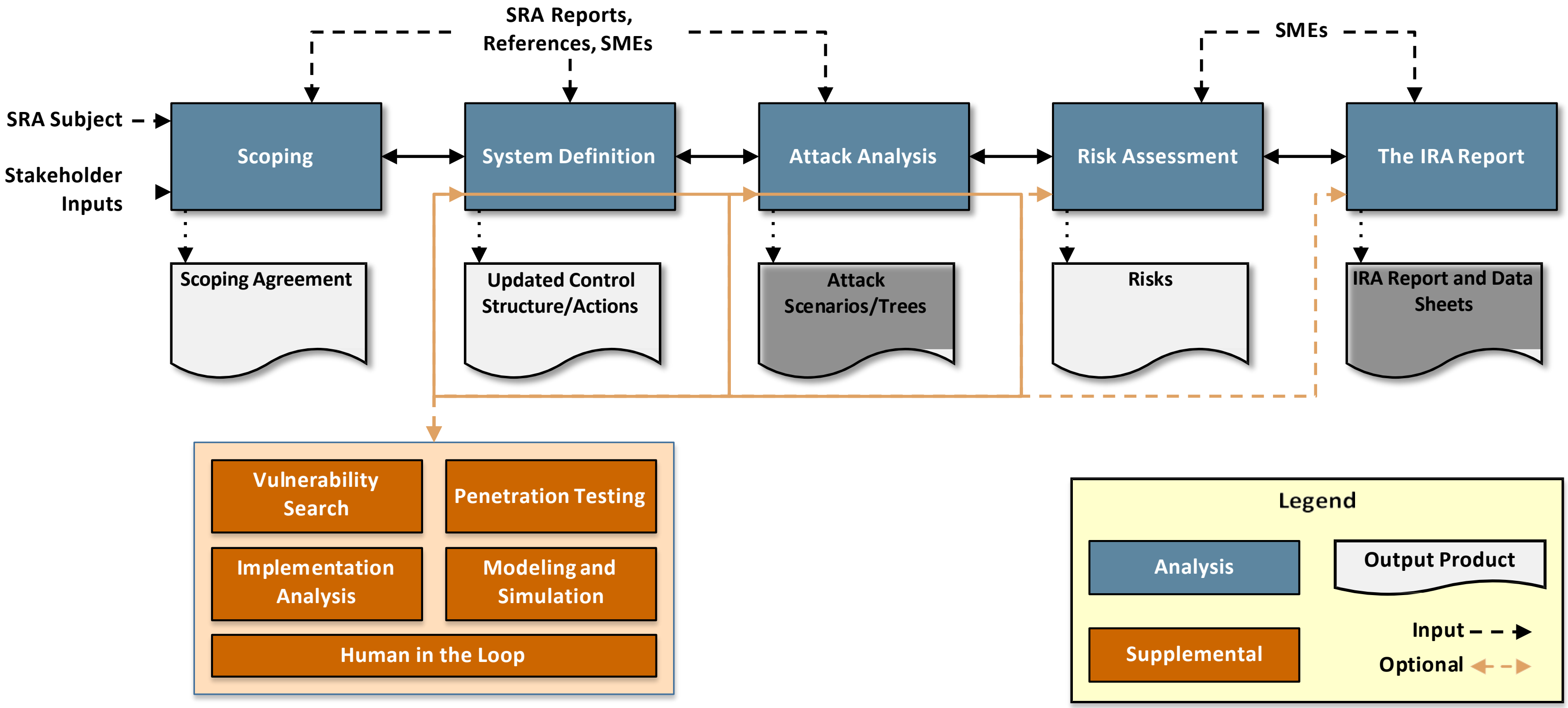
… / Penetration Testing / Implementation Analysis / Modeling & Simulation / Human in the Loop / …

Legend

Analysis

Supplemental

SRA Process Overview
Initial Risk Assessment (Part 1)



SRA Reports, References, SMEs

SMEs

SRA Subject

Stakeholder Inputs

Scoping

System Definition

Attack Analysis

Risk Assessment

The IRA Report

Scoping Agreement

Updated Control Structure/Actions

Attack Scenarios/Trees

Risks

IRA Report and Data Sheets

Vulnerability Search

Penetration Testing

Implementation Analysis

Modeling and Simulation

Human in the Loop

Legend

Analysis

Output Product

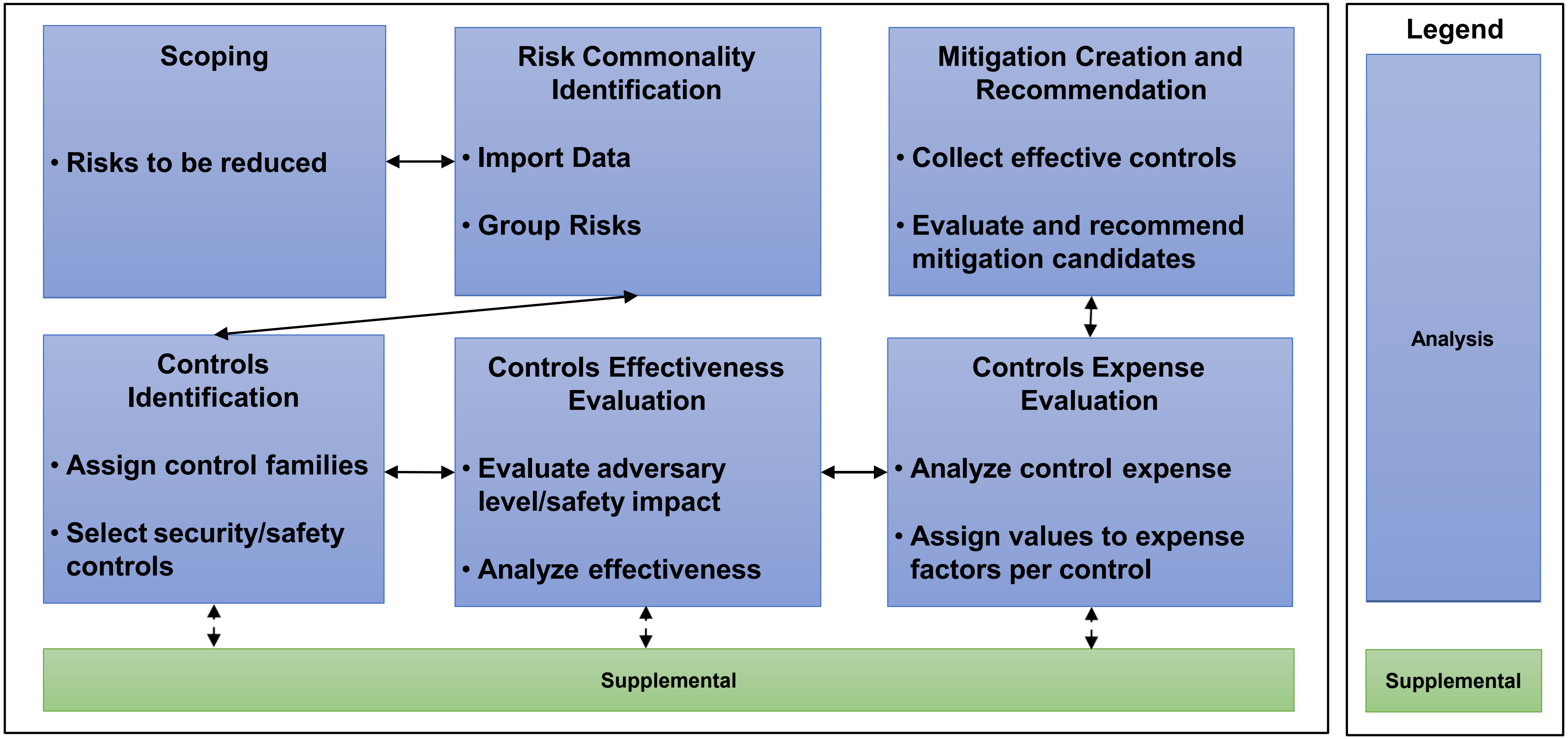
Supplemental

Input

Optional

Safety Risk Assessment (SRA) Methodology

Part 2 – Mitigation Identification and Evaluation



Scoping

- Risks to be reduced

Risk Commonality Identification

- Import Data
- Group Risks

Mitigation Creation and Recommendation

- Collect effective controls
- Evaluate and recommend mitigation candidates

Controls Identification

- Assign control families
- Select security/safety controls

Controls Effectiveness Evaluation

- Evaluate adversary level/safety impact
- Analyze effectiveness

Controls Expense Evaluation

- Analyze control expense
- Assign values to expense factors per control

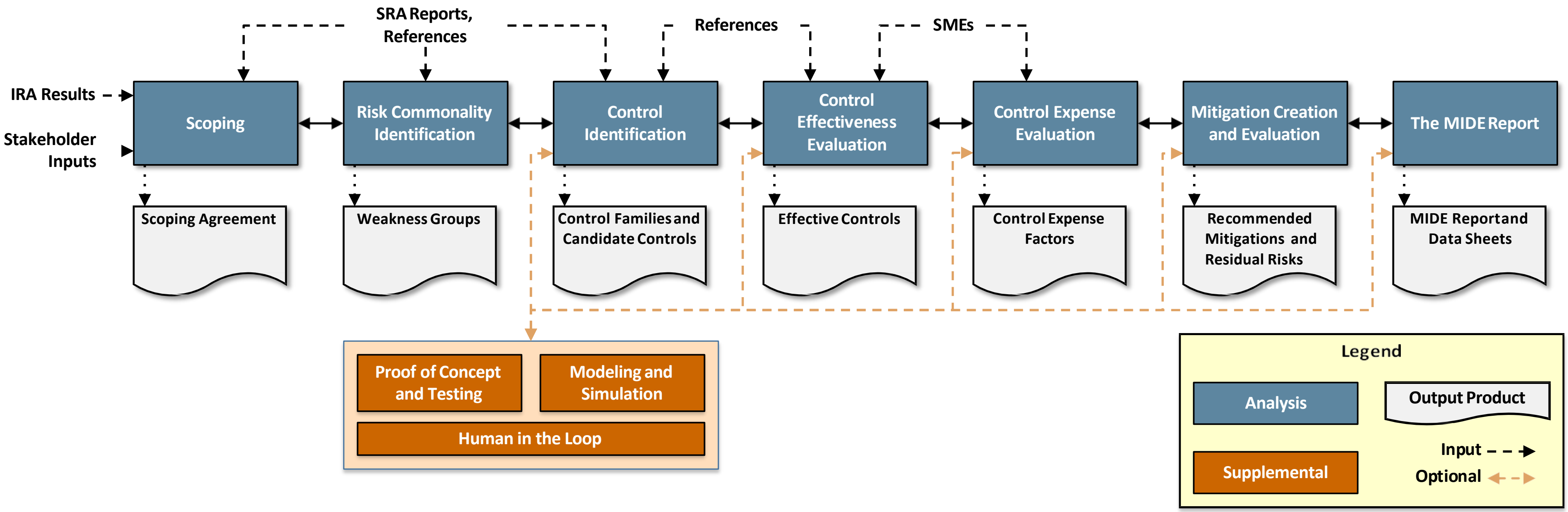
Supplemental

Legend

Analysis

Supplemental

SRA Process Overview Mitigation Identification and Evaluation (Part 2)



SRA Reports, References

References

SMEs

IRA Results

Stakeholder Inputs

Scoping

Risk Commonality Identification

Control Identification

Control Effectiveness Evaluation

Control Expense Evaluation

Mitigation Creation and Evaluation

The MIDE Report

Scoping Agreement

Weakness Groups

Control Families and Candidate Controls

Effective Controls

Control Expense Factors

Recommended Mitigations and Residual Risks

MIDE Report and Data Sheets

Proof of Concept and Testing

Modeling and Simulation

Human in the Loop

Legend

Analysis

Output Product

Supplemental

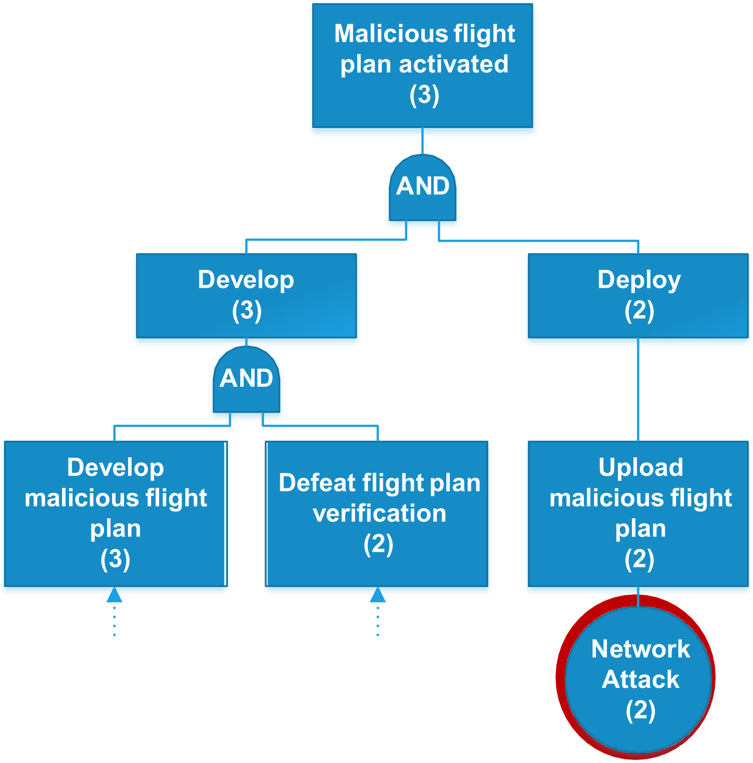
Input

Optional

Attack Tree Generation

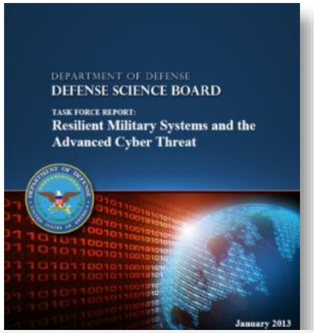
- Group attack scenarios by attack type, scenario end effect, and safety impact
- Develop attack tree for each scenario group that represents
  - Steps necessary to execute the HCA
  - Adversary capabilities required to execute the steps
- Assign capability scores to leaf nodes and propagate upward
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

Running Example

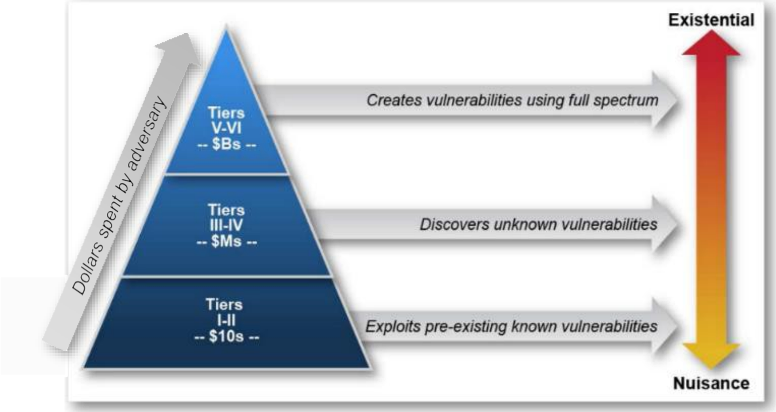

Malicious flight plan activated (3)
AND
Develop (3)
Deploy (2)
AND
Develop malicious flight plan (3)
Defeat flight plan verification (2)
Upload malicious flight plan (2)
Network Attack (2)

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



DEPARTMENT OF DEFENSE
DEFENSE SCIENCE BOARD
TASK FORCE REPORT:
Resilient Military Systems and the Advanced Cyber Threat
January 2013


Existential
Dollars spent by adversary
Tiers V-VI -- $Bs --
Creates vulnerabilities using full spectrum
Tiers III-IV -- $Ms --
Discovers unknown vulnerabilities
Tiers I-II -- $10s --
Exploits pre-existing known vulnerabilities
Nuisance

FAA

NextGEN

Evaluate Mitigations

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

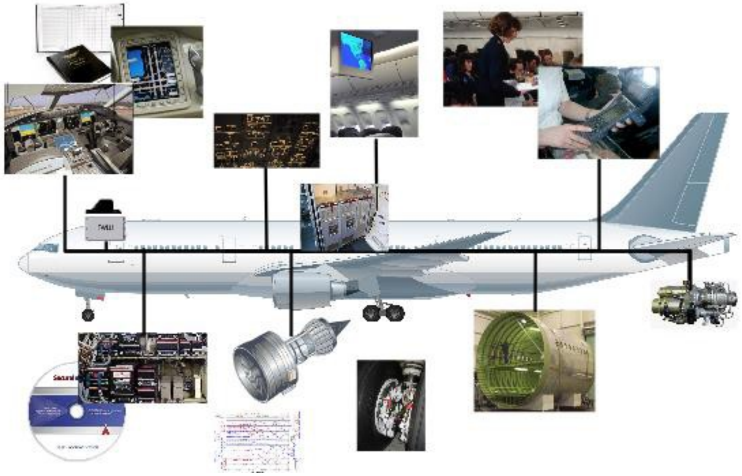
Risk ID	Mitigation ID	Selected Controls	Residual Safety Impact	Residual Individual Adversary Level	Total Mitigation Cost	Total Mitigation Time	System Impact Expense
…	…	…	…	…	…	…	…

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

		Safety Impact			
	NOTIONAL	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)

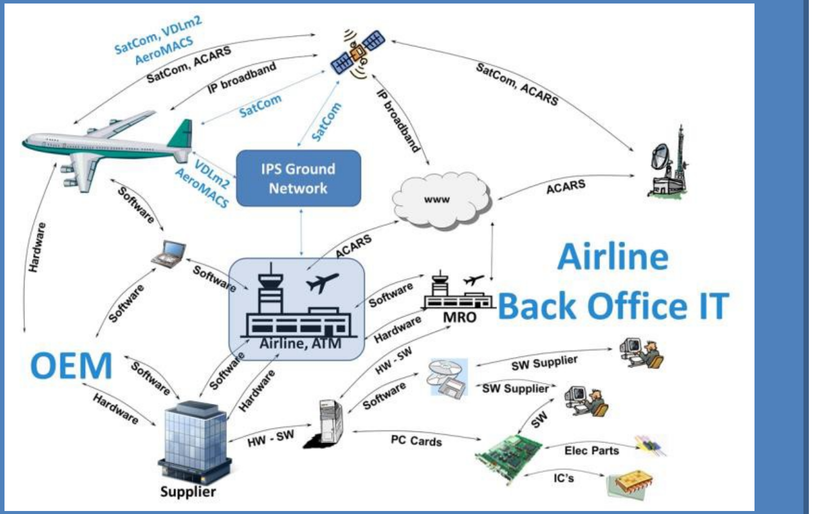
Field-Loadable Software (FLS)

Flight Management Systems

Cyber SRA End-to-End System Analysis

Aircraft Communications Addressing and Reporting System (ACARS)

Field-Loadable Software (FLS)

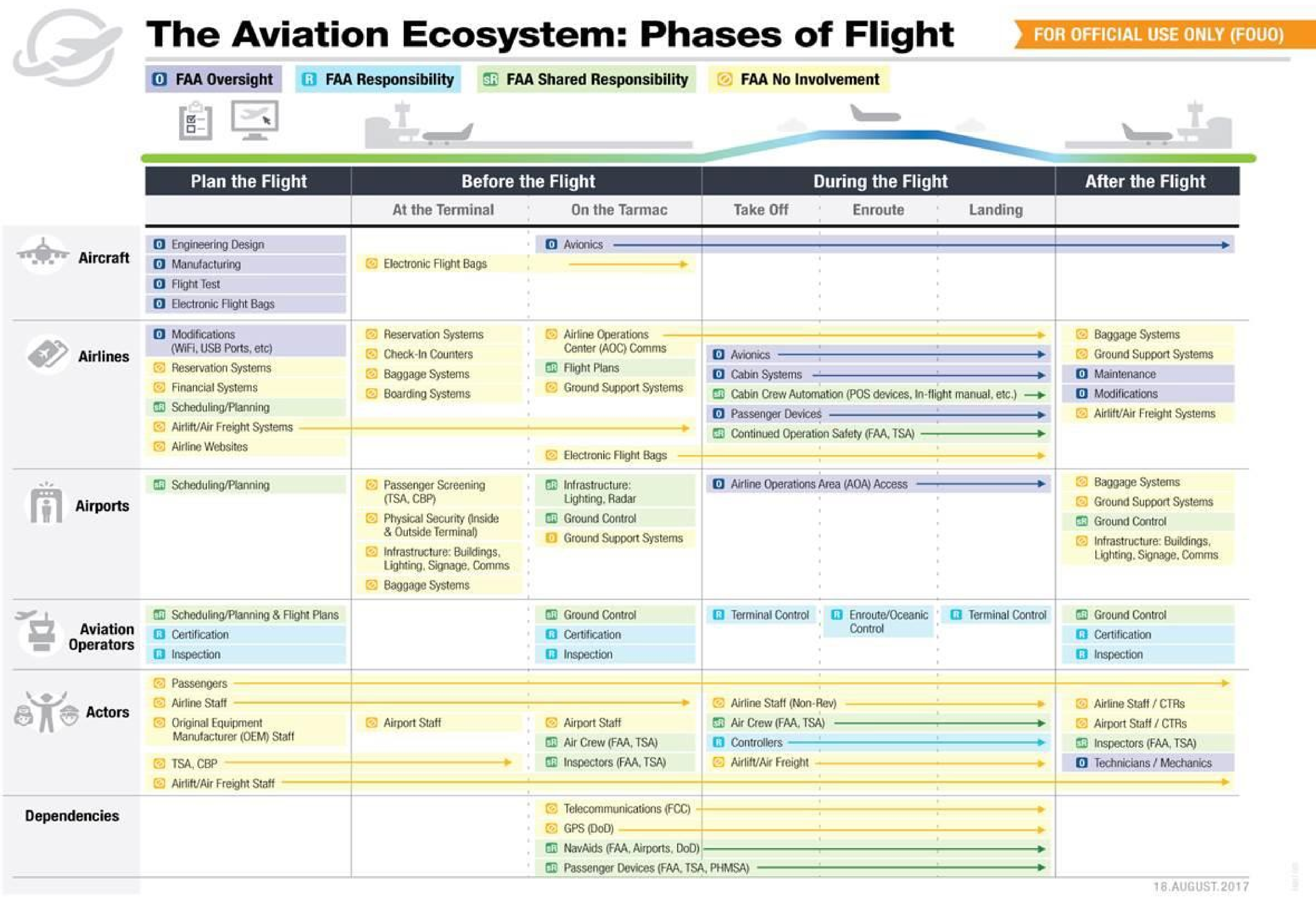


Air Traffic Services (ATS)
Internet Protocol Suite (IPS)

November 2020 completion

Electronic Interface Device (EID)

Flight Management Systems



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 ⊘ 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 methodolgy 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)

PART II

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

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

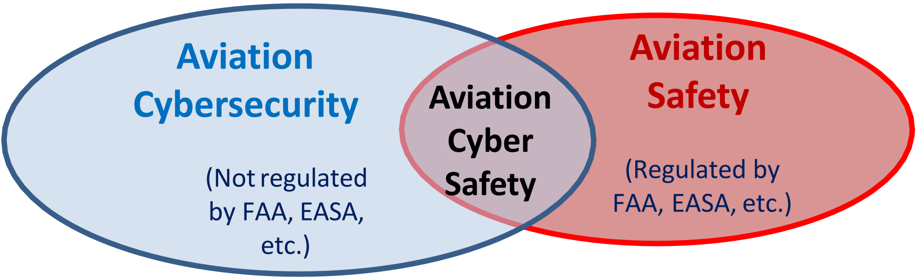
- Reduce U.S. commercial aviation cyber safety risk
- Work with international partners to reduce cyber safety risk world-wide

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:

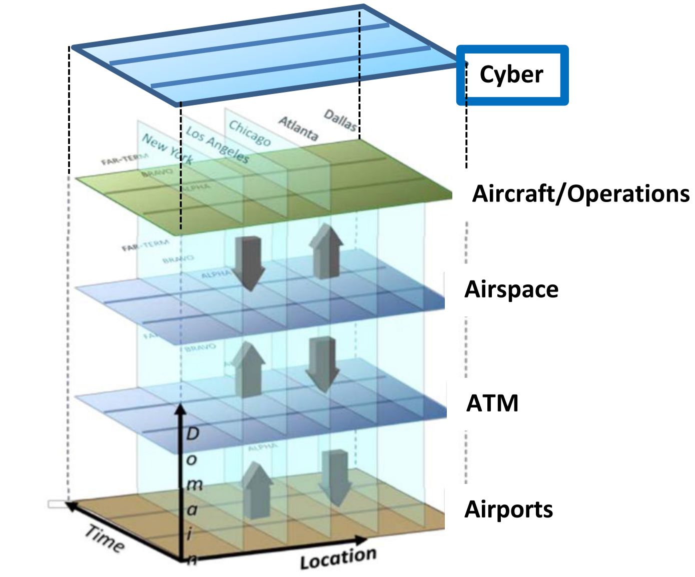

Aviation Cybersecurity
(Not regulated by FAA, EASA, etc.)
Aviation Cyber Safety
Aviation Safety
(Regulated by FAA, EASA, etc.)

- 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


Cyber

Aircraft/Operations

Airspace

ATM

Airports

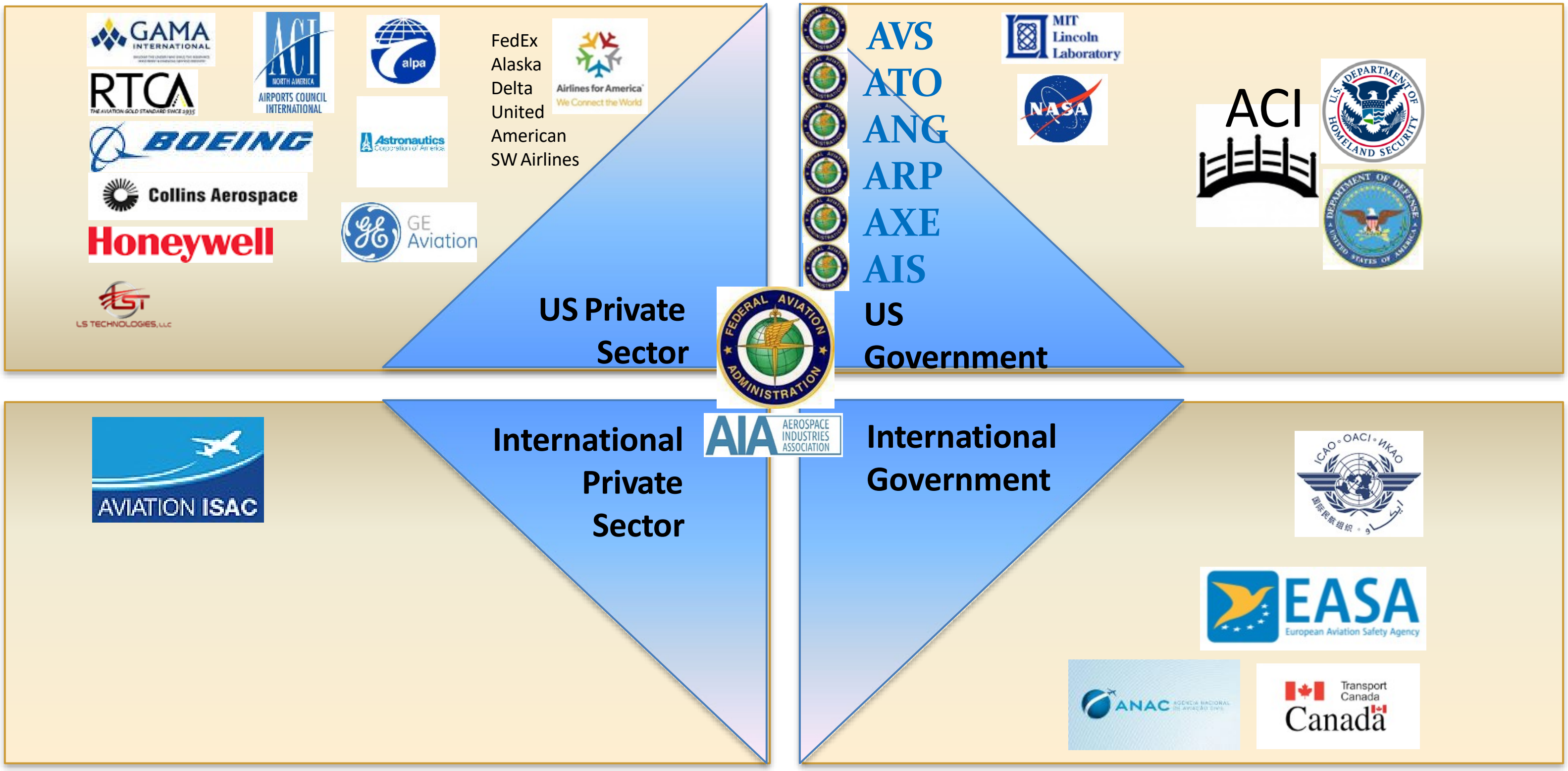
The Complex Integration Aspects of a Capability

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



US Private Sector

FedEx
Alaska
Delta
United
American
SW Airlines

AVS
ATO
ANG
ARP
AXE
AIS

US Government

ACI

International Private Sector

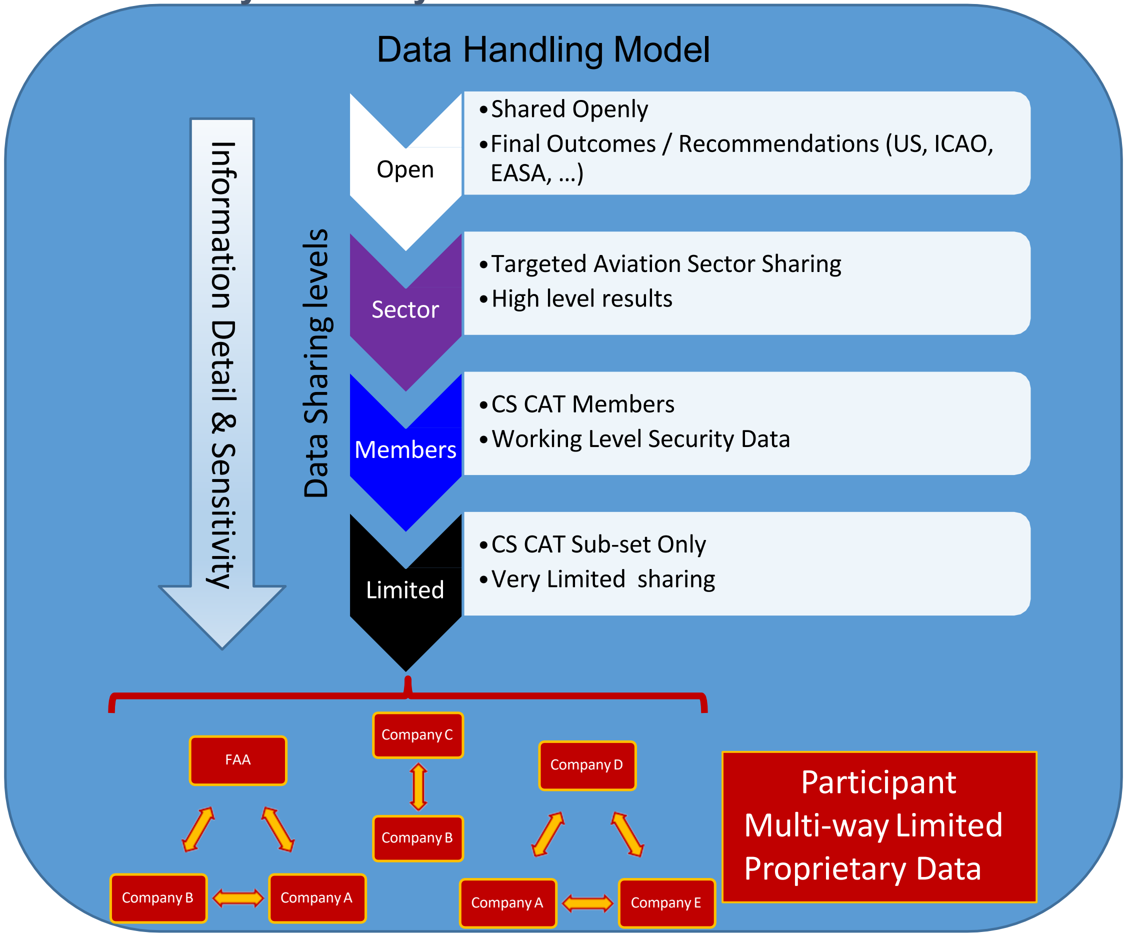
International Government

GAMA INTERNATIONAL
RTCA
ACI NORTH AMERICA AIRPORTS COUNCIL INTERNATIONAL
alpa
Airlines for America We Connect the World
BOEING
Astronautics Corporation of America
Collins Aerospace
Honeywell
GE Aviation
LS TECHNOLOGIES, LLC
MIT Lincoln Laboratory
NASA
U.S. DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA
FEDERAL AVIATION ADMINISTRATION
AIA AEROSPACE INDUSTRIES ASSOCIATION
AVIATION ISAC
ICAO • OACI • ИКАО
EASA European Aviation Safety Agency
ANAC
Transport Canada
Canada

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

- Shared Openly
- Final Outcomes / Recommendations (US, ICAO, EASA, …)

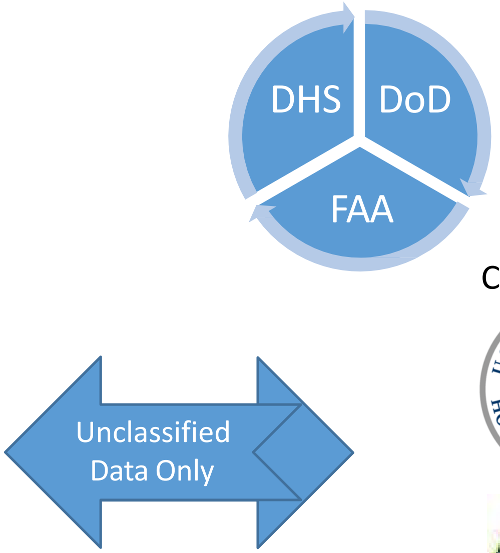
- Targeted Aviation Sector Sharing
- High level results

- CS CAT Members
- Working Level Security Data

- CS CAT Sub-set Only
- Very Limited sharing

Participant Multi-way Limited Proprietary Data

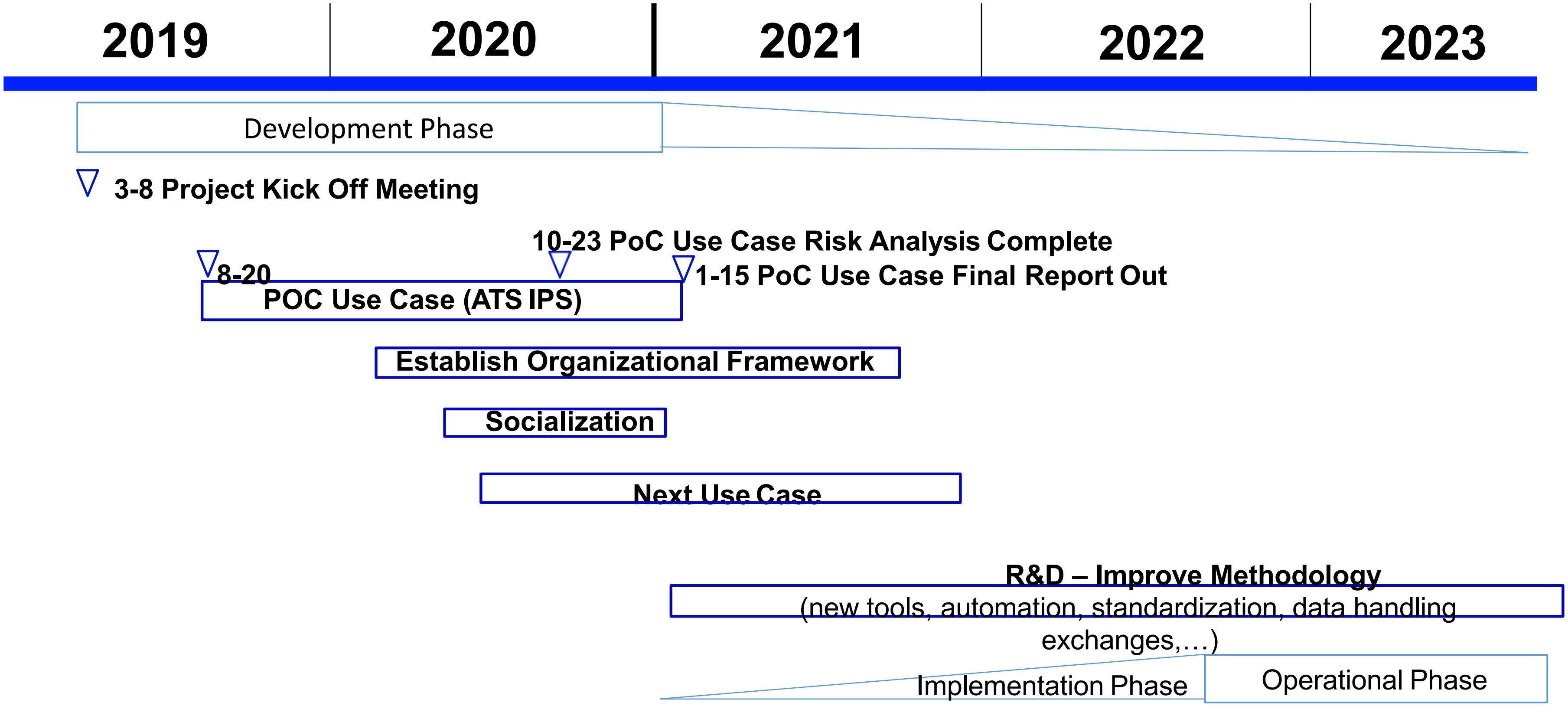
Partners / Data Sharing



ACI Tri-Chair

CISA Central

Cyber Safety CAT Proposed Timeline



2019 2020 2021 2022 2023

Development Phase

3-8 Project Kick Off Meeting

10-23 PoC Use Case Risk Analysis Complete

8-20

1-15 PoC Use Case Final Report Out

POC Use Case (ATS IPS)

Establish Organizational Framework

Socialization

Next Use Case

R&D – Improve Methodology
(new tools, automation, standardization, data handling exchanges,…)

Implementation Phase

Operational Phase

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

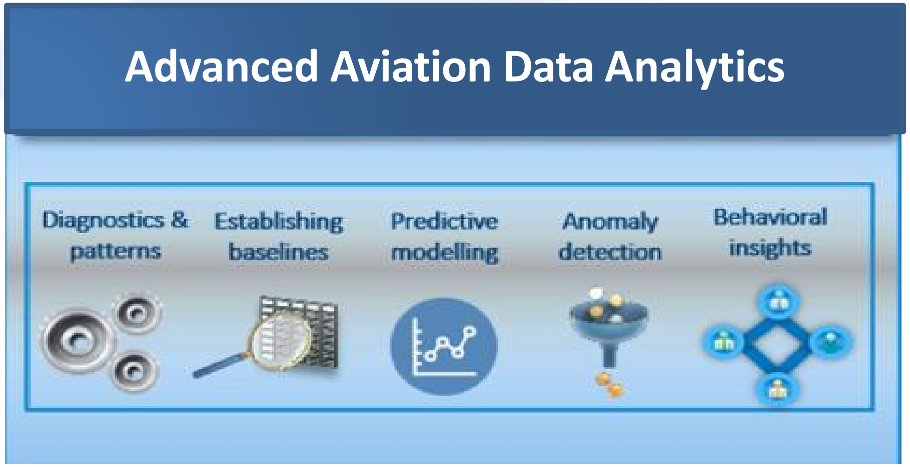
Susan Cabler

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



Advanced Aviation Data Analytics

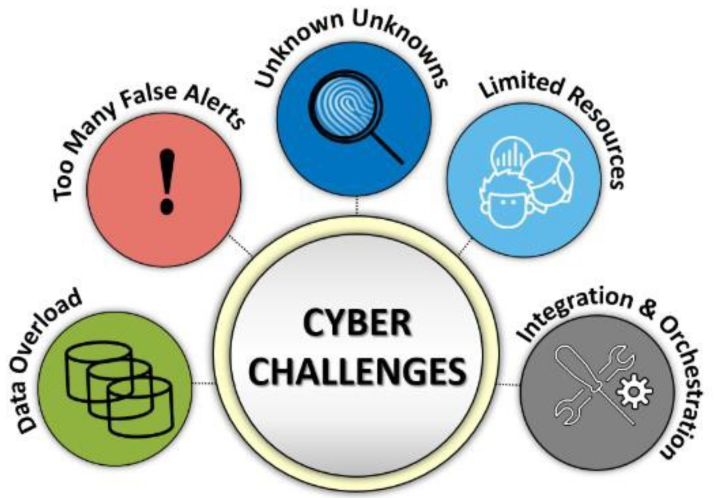
Diagnostics & patterns

Establishing baselines

Predictive modelling

Anomaly detection

Behavioral insights



CYBER CHALLENGES

Too Many False Alerts

Unknown Unknowns

Limited Resources

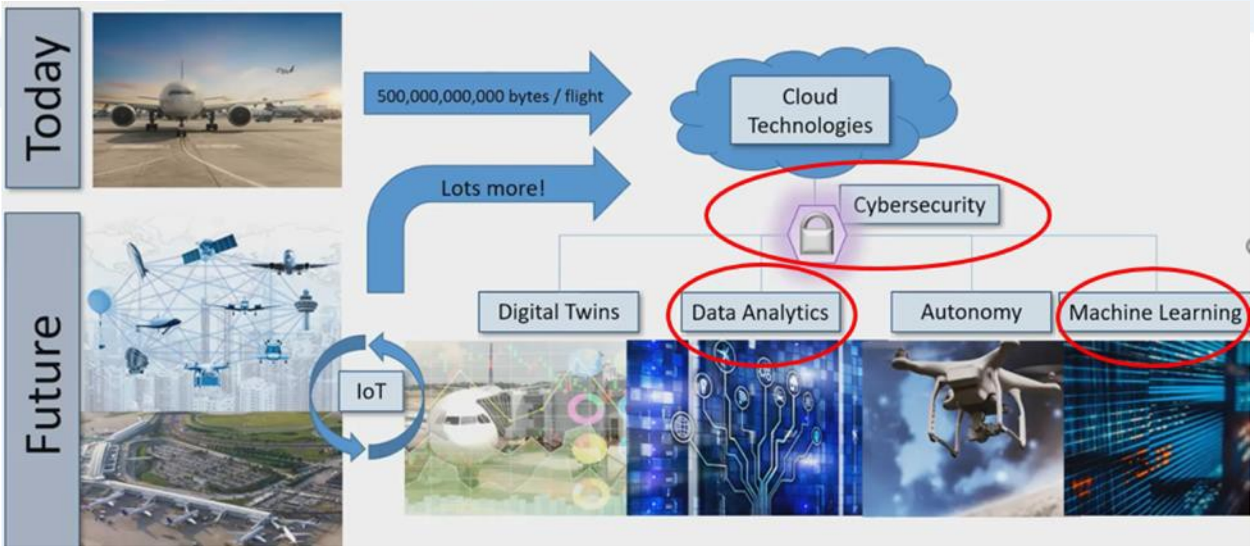
Data Overload

Integration & Orchestration

- Extend research for CS CAT to also utilize Cybersecurity Data Science (CSDS) principles
- CSDS offers a path forward to utilize data rich environments besieged by unknown-unknowns

CSDS CONCEPT IN PLANNING PHASE

Future Research: Cyber Security Data Science



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

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