In-Time Aviation Safety Management Systems (IASMS)

Briefing to the FAA UAM Strategic WG
Sept 1st, 2021

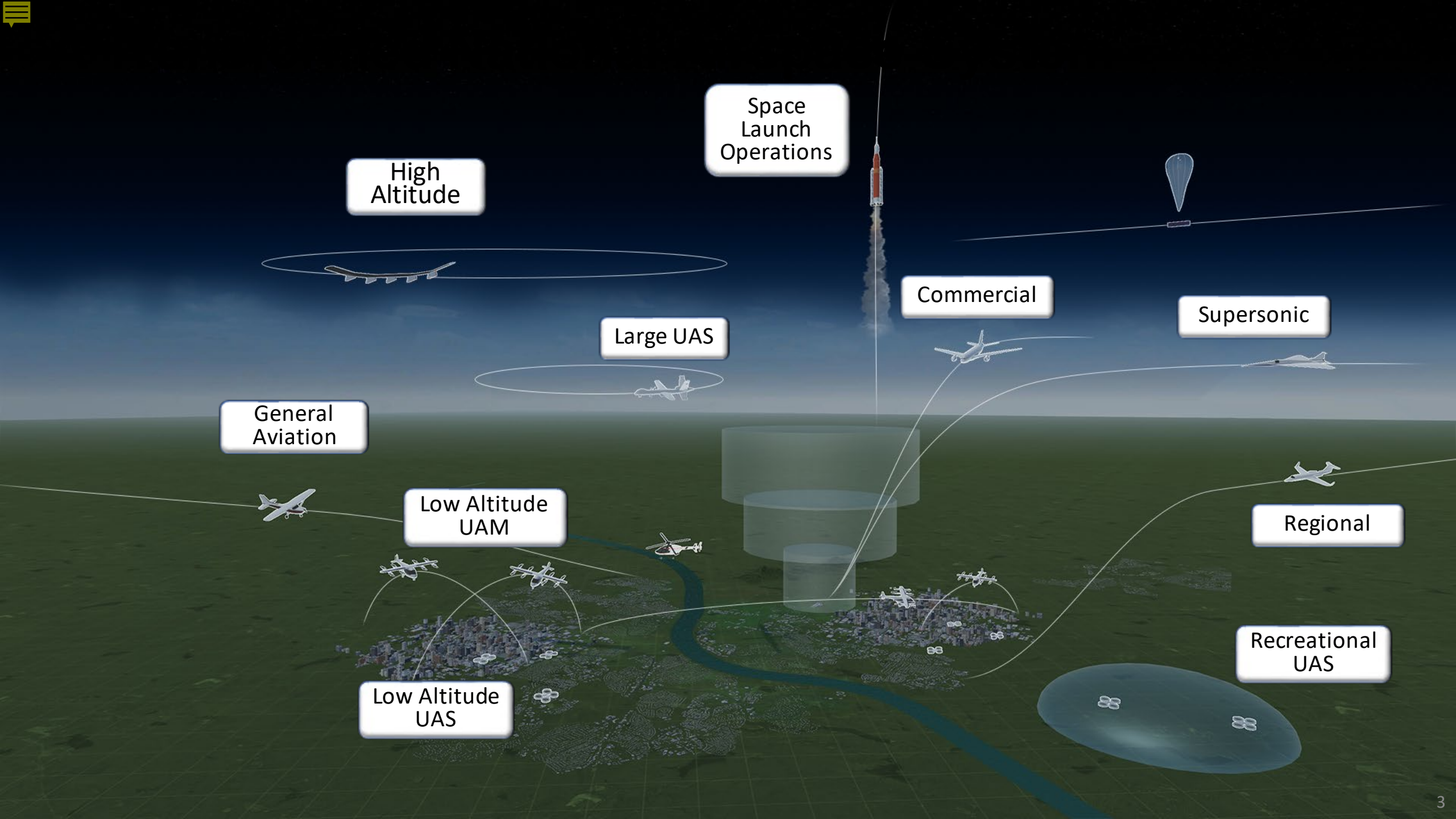
Dr. Kyle Ellis
System-Wide Safety Project
Airspace Operations and Safety Program
NASA Aeronautics Research Mission Directorate

A Safe Future National Airspace System

The Problem: Safety Assurance and Accessibility for integrating emerging domains into the NAS. The public has a low tolerance for risk in aviation and the current NAS is labor-intensive with limited ability to scale up for new entrants.

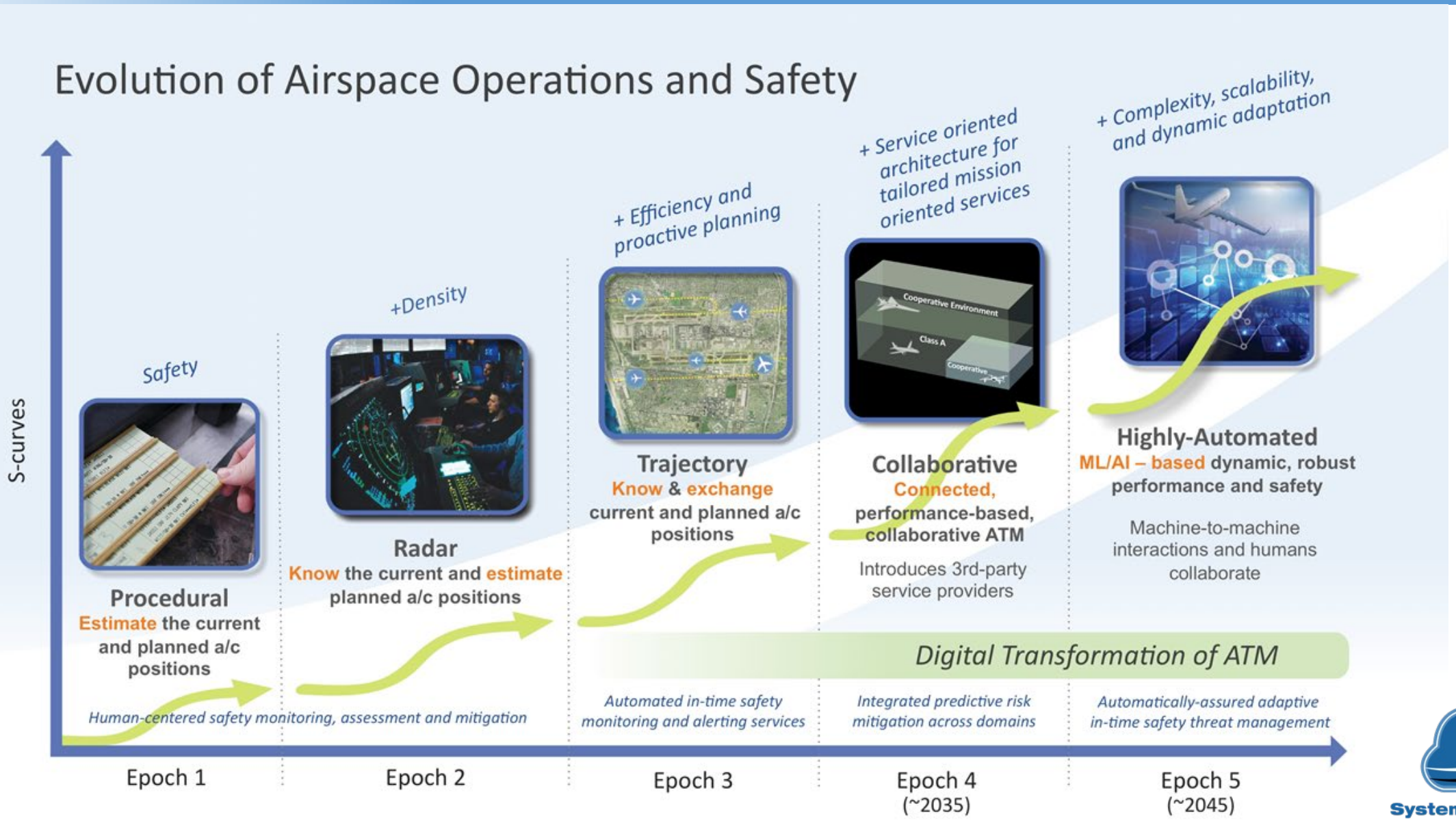
Possible Solution: Collaboratively define a Concept of Operations for scalable In-time Aviation Safety Management Systems (IASMS) with a service-oriented architecture to better focus safety investments in technological solutions that overcome barriers to future envisioned operations in the NAS (2045+).

Industry Collaboration: Consensus on desirable system traits based on relevant Use Cases to show integration of data and leveraging of automated/ autonomous systems that can identify anomalies, precursors, and trends to more proactively manage operational risks.


Space Launch Operations
High Altitude
Commercial
Supersonic
Large UAS
General Aviation
Low Altitude UAM
Regional
Recreational UAS
Low Altitude UAS


High Altitude
Long Endurance
Space
Launch
Large Commercial
Transportation
Airline
FAA
General
Aviation
Traditional Air Traffic Control
Collaborative Air Traffic Management
Communication
Control
Flight Path

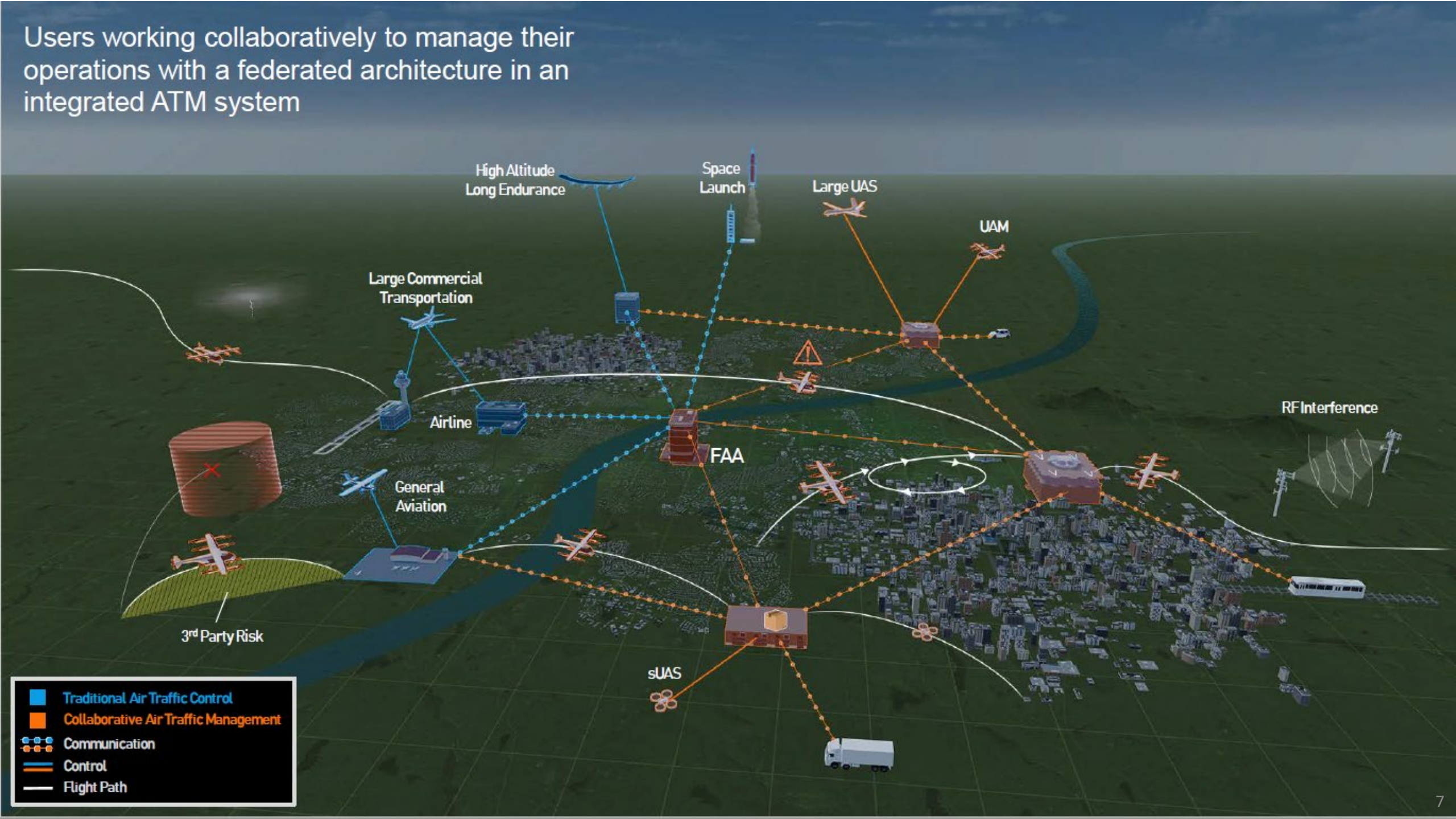
Evolution of Airspace Operations and Safety



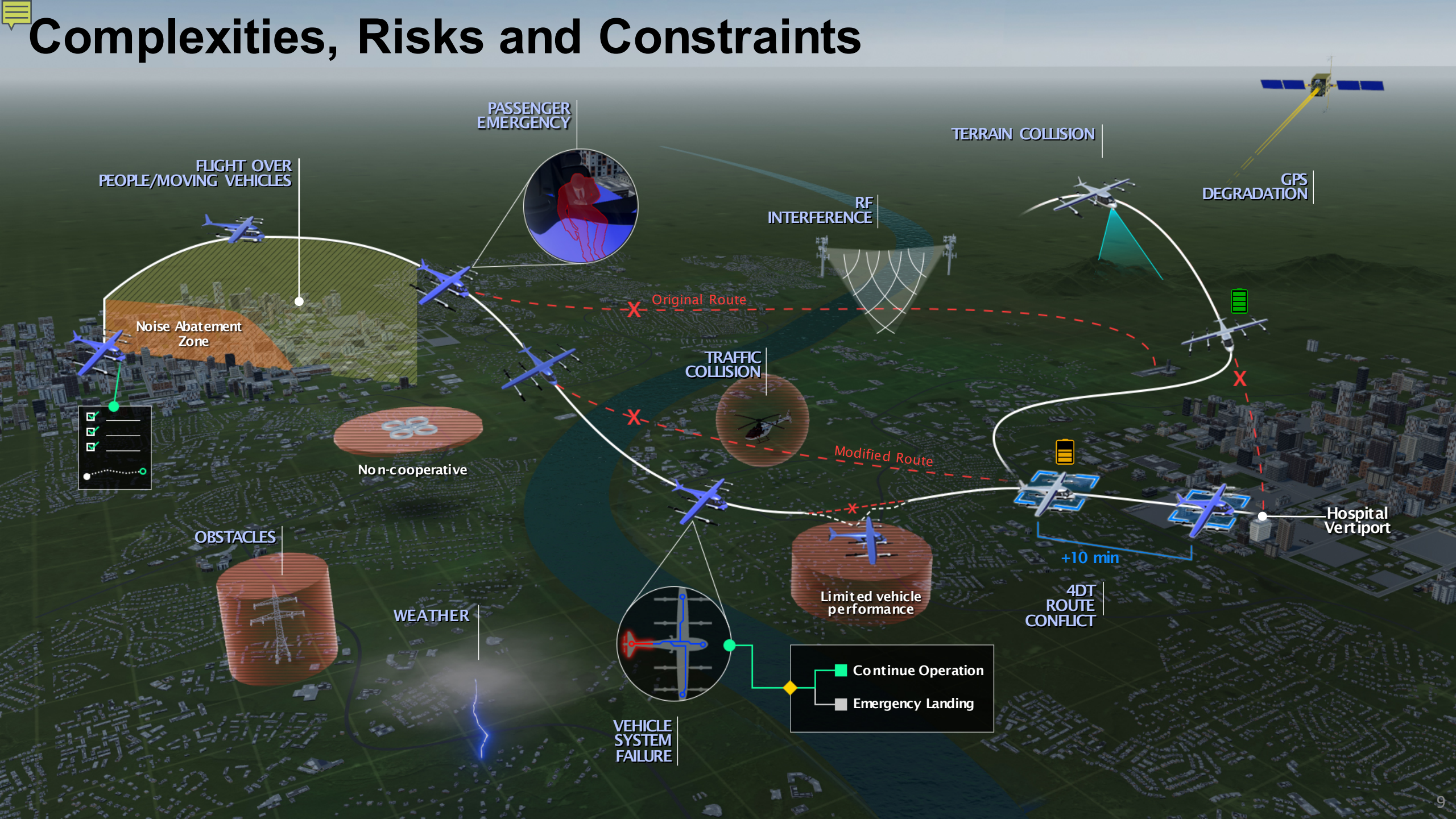
System-Wide Safety


High Altitude
Long Endurance
Space
Launch
Large UAS
UAM
Large Commercial
Transportation
Airline
FAA
General
Aviation
RF Interference
sUAS
Traditional Air Traffic Control
Collaborative Air Traffic Management
Communication
Control
Flight Path

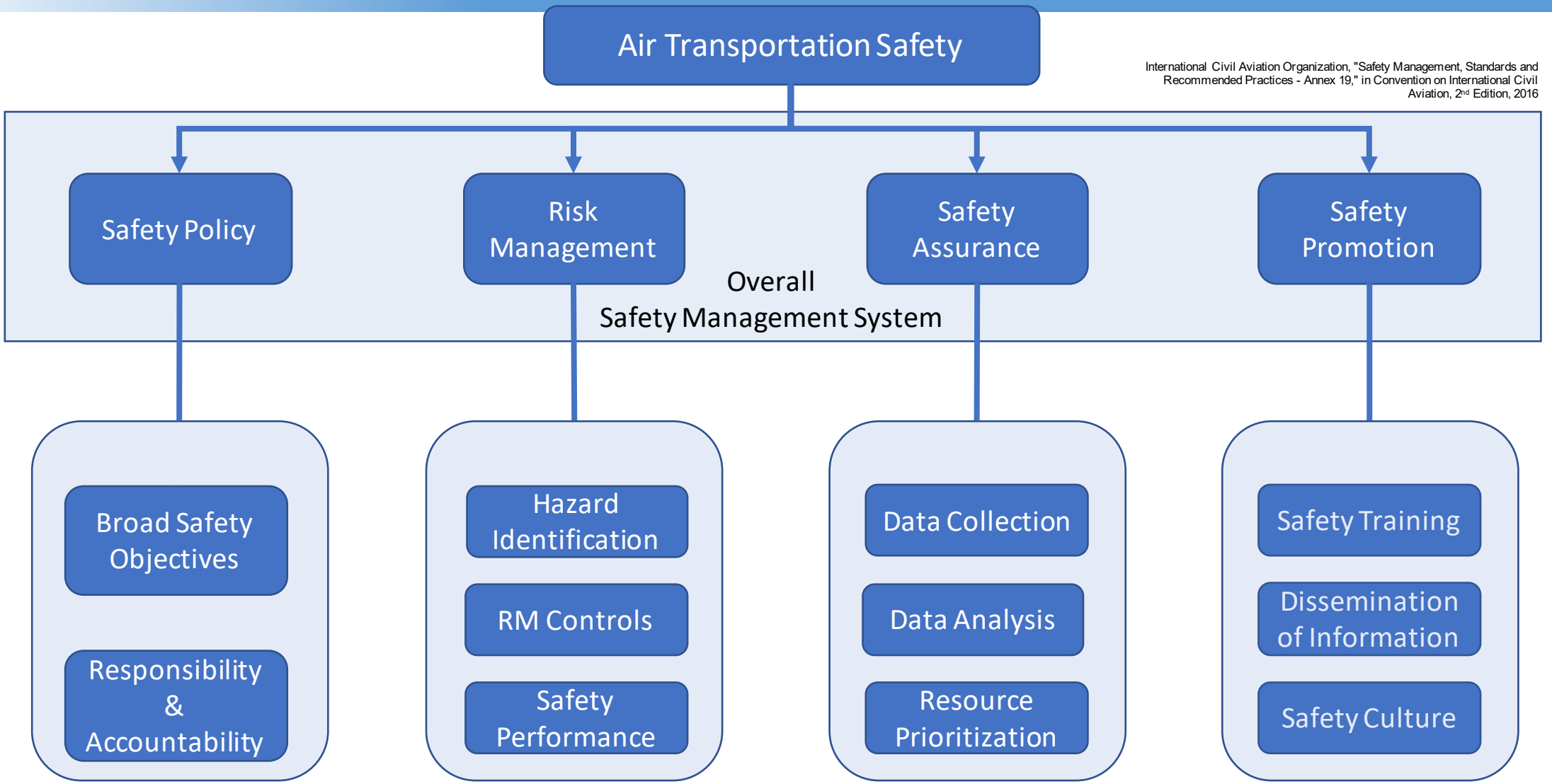
Users working collaboratively to manage their operations with a federated architecture in an integrated ATM system



Complexities, Risks and Constraints



Achieving Aviation Safety Today



International Civil Aviation Organization, "Safety Management, Standards and Recommended Practices - Annex 19," in Convention on International Civil Aviation, 2nd Edition, 2016

Labor intensive
Limited ability to scale
Not fast enough

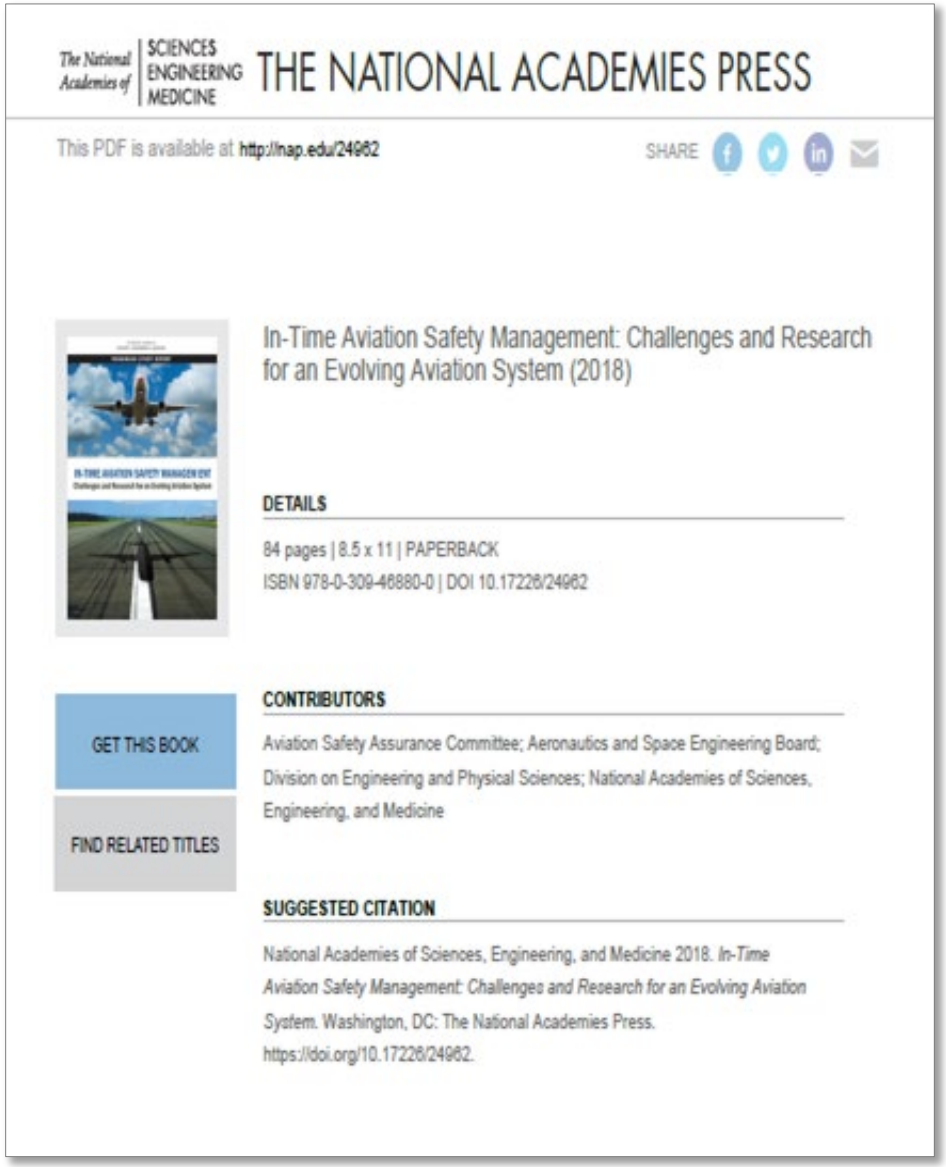
National Academies—IASMS

Outlines need for evolution of the existing Safety Management System

In-Time Aviation Safety Management System (IASMS)

Identifies 4 Fundamental System Element Development Areas:

1. Concept of Operations and Risk Prioritization
2. System Monitoring
3. System Analytics
4. Mitigation and Implementation



The National Academies of SCIENCES ENGINEERING MEDICINE THE NATIONAL ACADEMIES PRESS

This PDF is available at http://nap.edu/24962 SHARE

In-Time Aviation Safety Management: Challenges and Research for an Evolving Aviation System (2018)

DETAILS

84 pages | 8.5 x 11 | PAPERBACK
ISBN 978-0-309-46880-0 | DOI 10.17226/24962

GET THIS BOOK

FIND RELATED TITLES

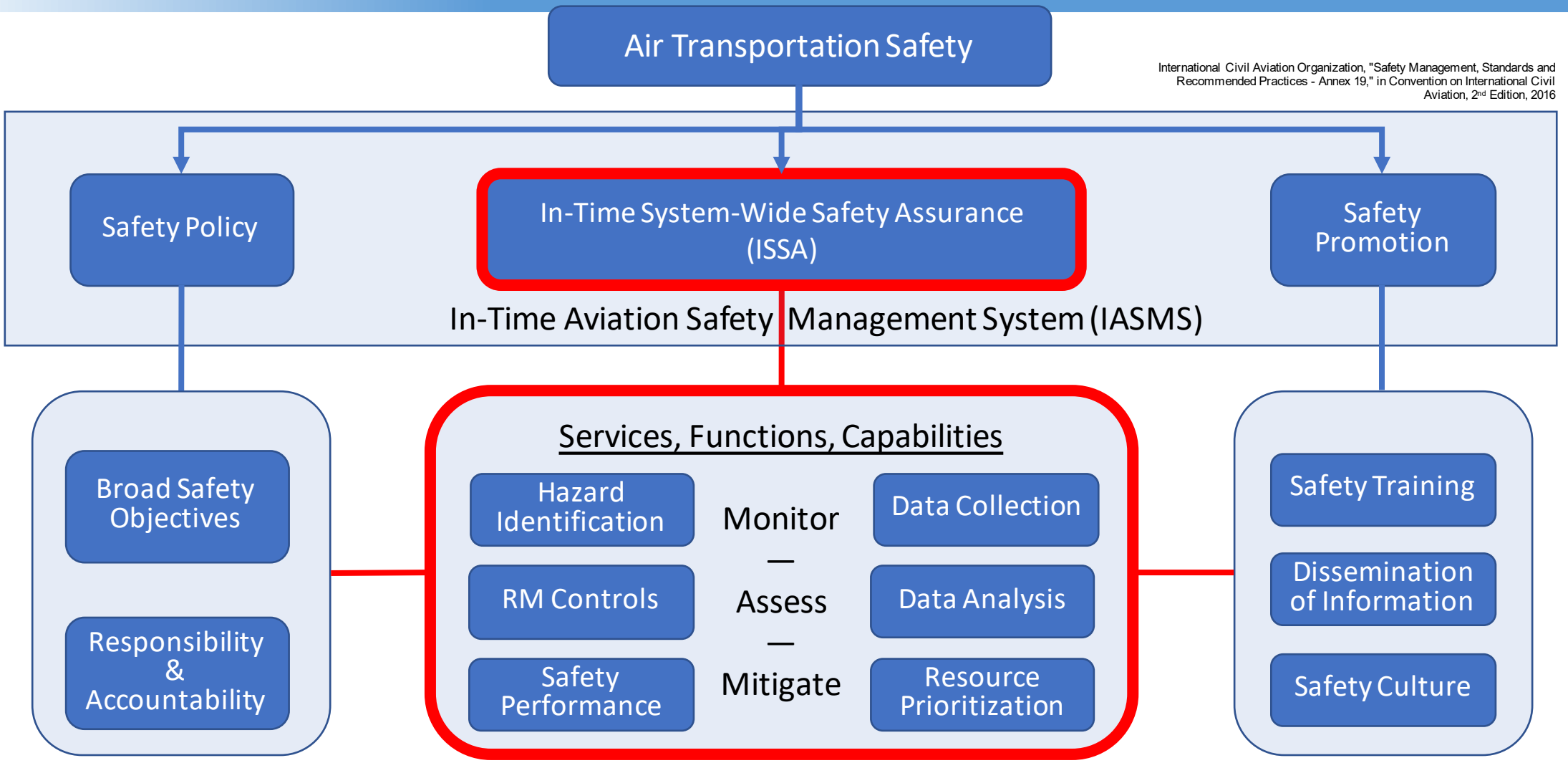
CONTRIBUTORS

Aviation Safety Assurance Committee; Aeronautics and Space Engineering Board; Division on Engineering and Physical Sciences; National Academies of Sciences, Engineering, and Medicine

SUGGESTED CITATION

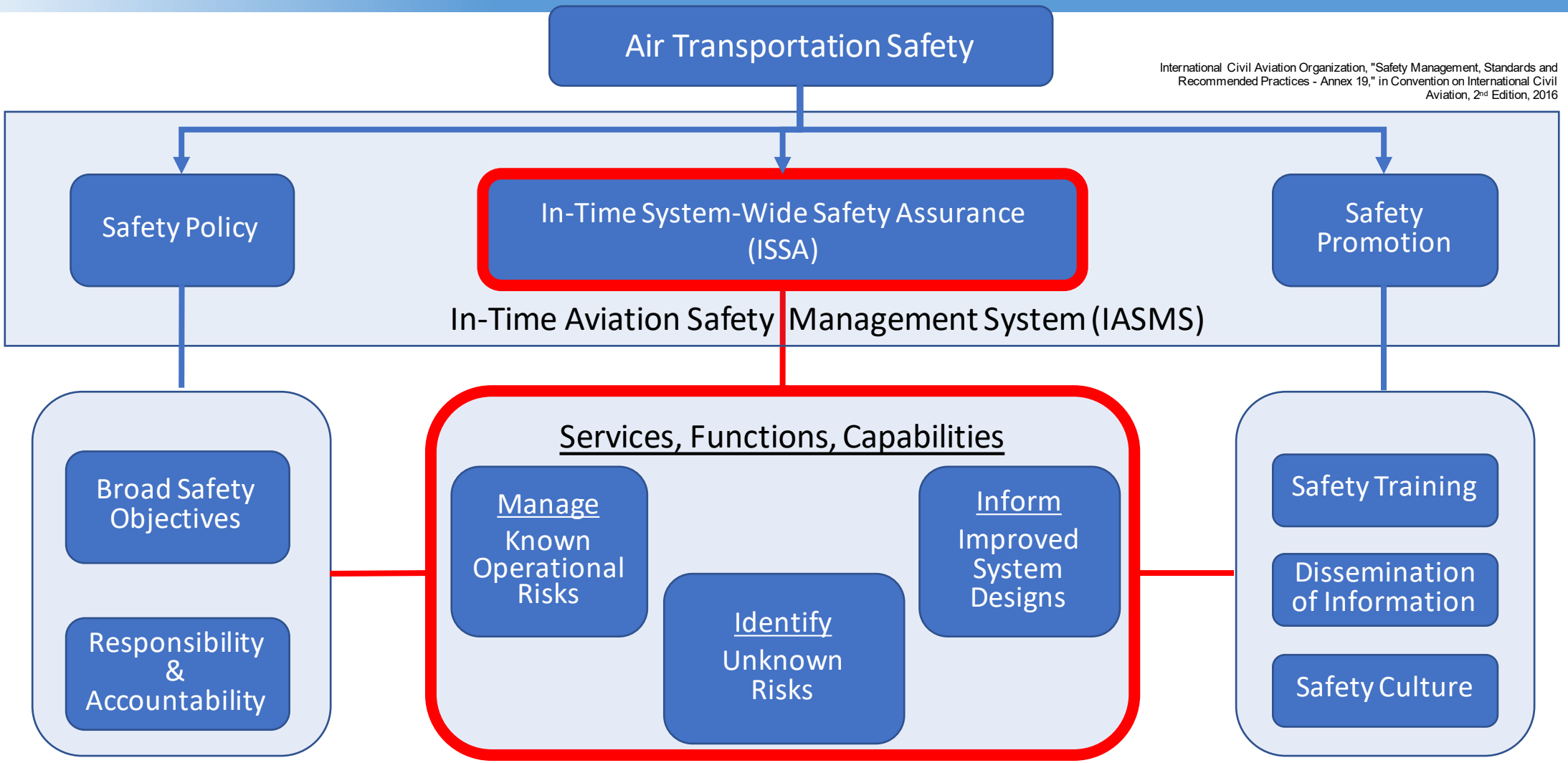
National Academies of Sciences, Engineering, and Medicine 2018. *In-Time Aviation Safety Management: Challenges and Research for an Evolving Aviation System*. Washington, DC: The National Academies Press. https://doi.org/10.17226/24962.

How We Achieve Aviation Safety Tomorrow



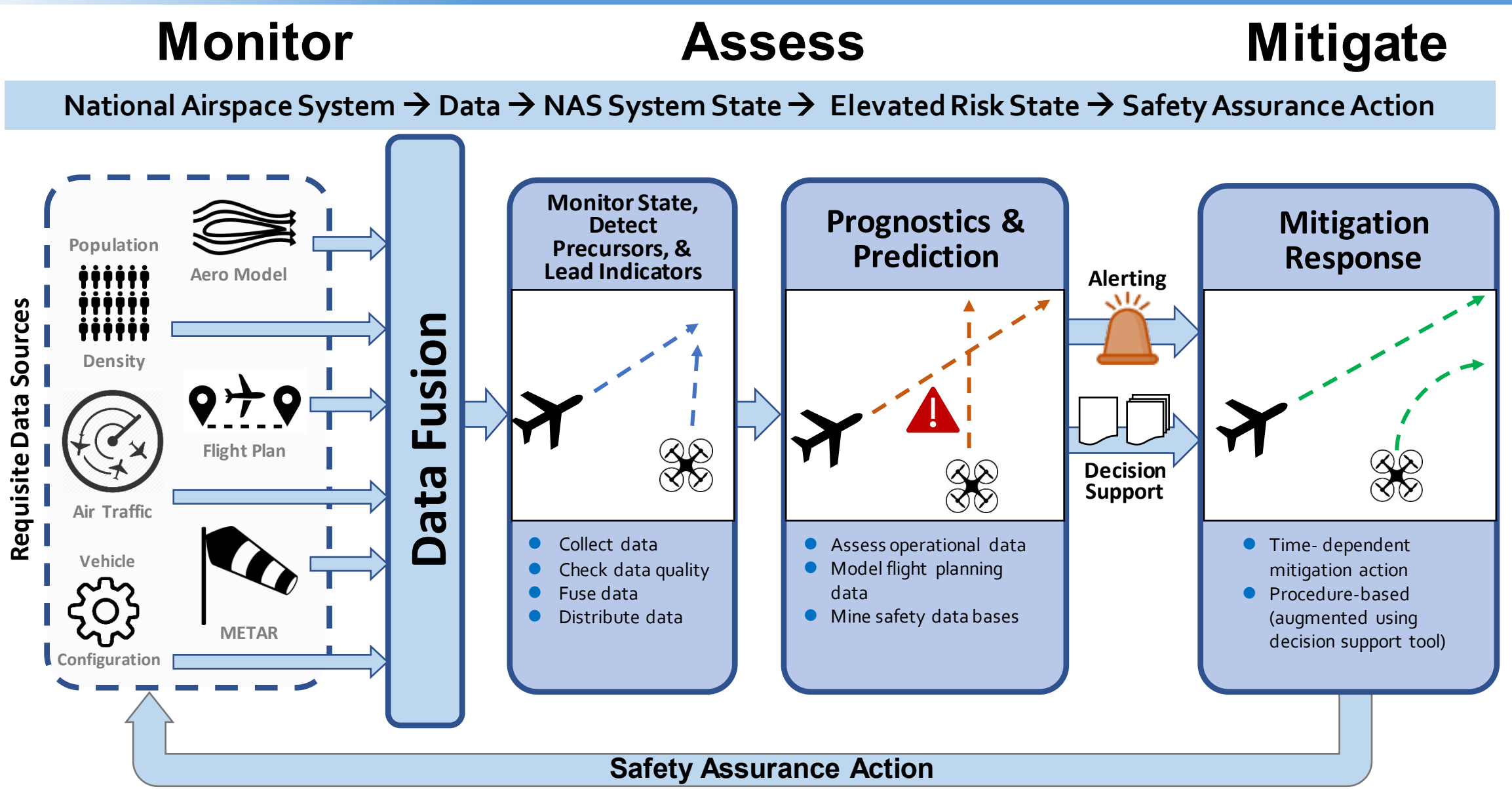
Services, Functions, and Capabilities Execute Risk Management and Safety Assurance Actions

How We Achieve Aviation Safety Tomorrow



Quickly manage known operational risks at scale
Quickly identify unknown risks
Quickly inform design

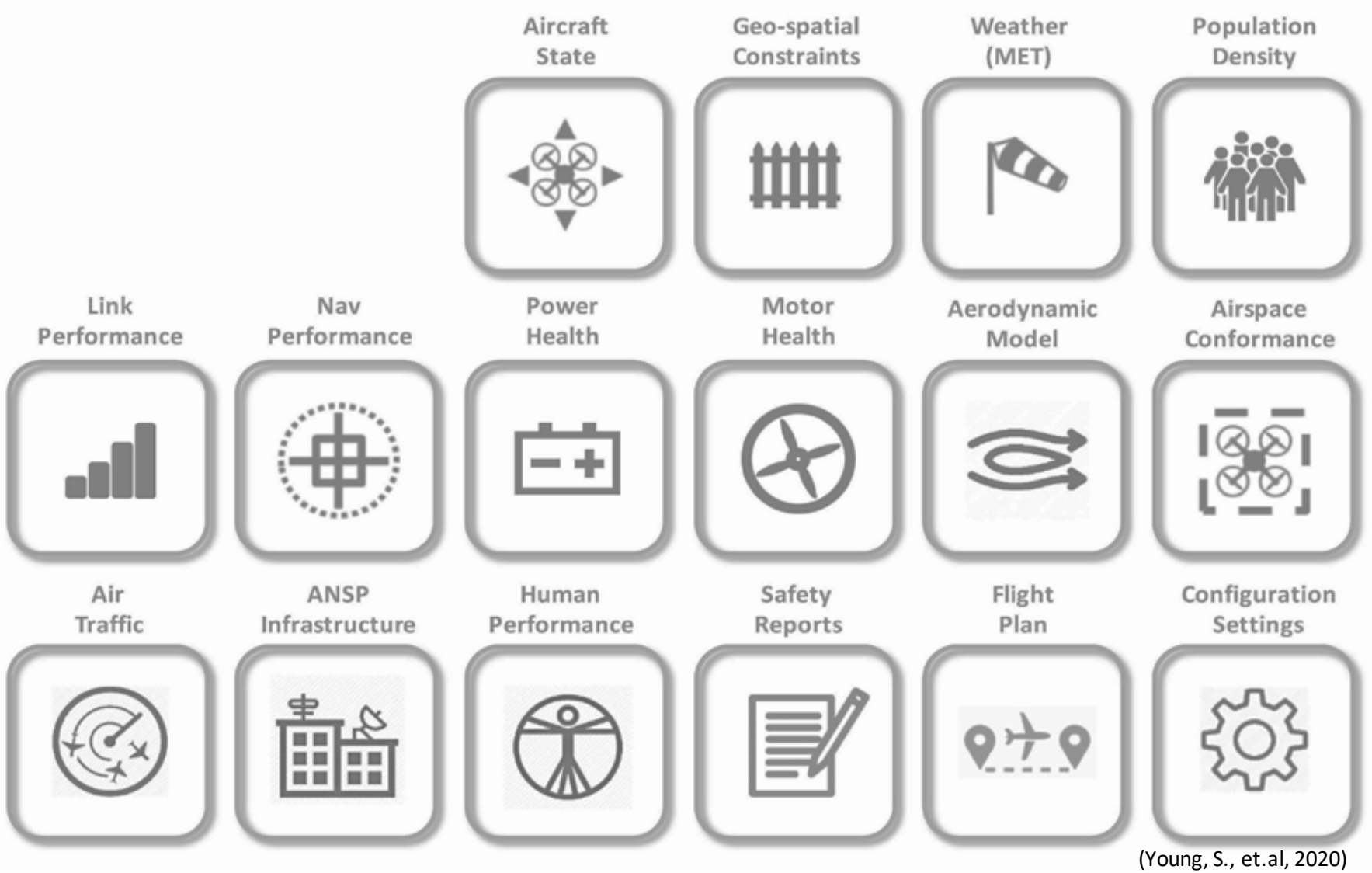
Services, Functions & Capabilities (SFCs)



It All Starts with Data…

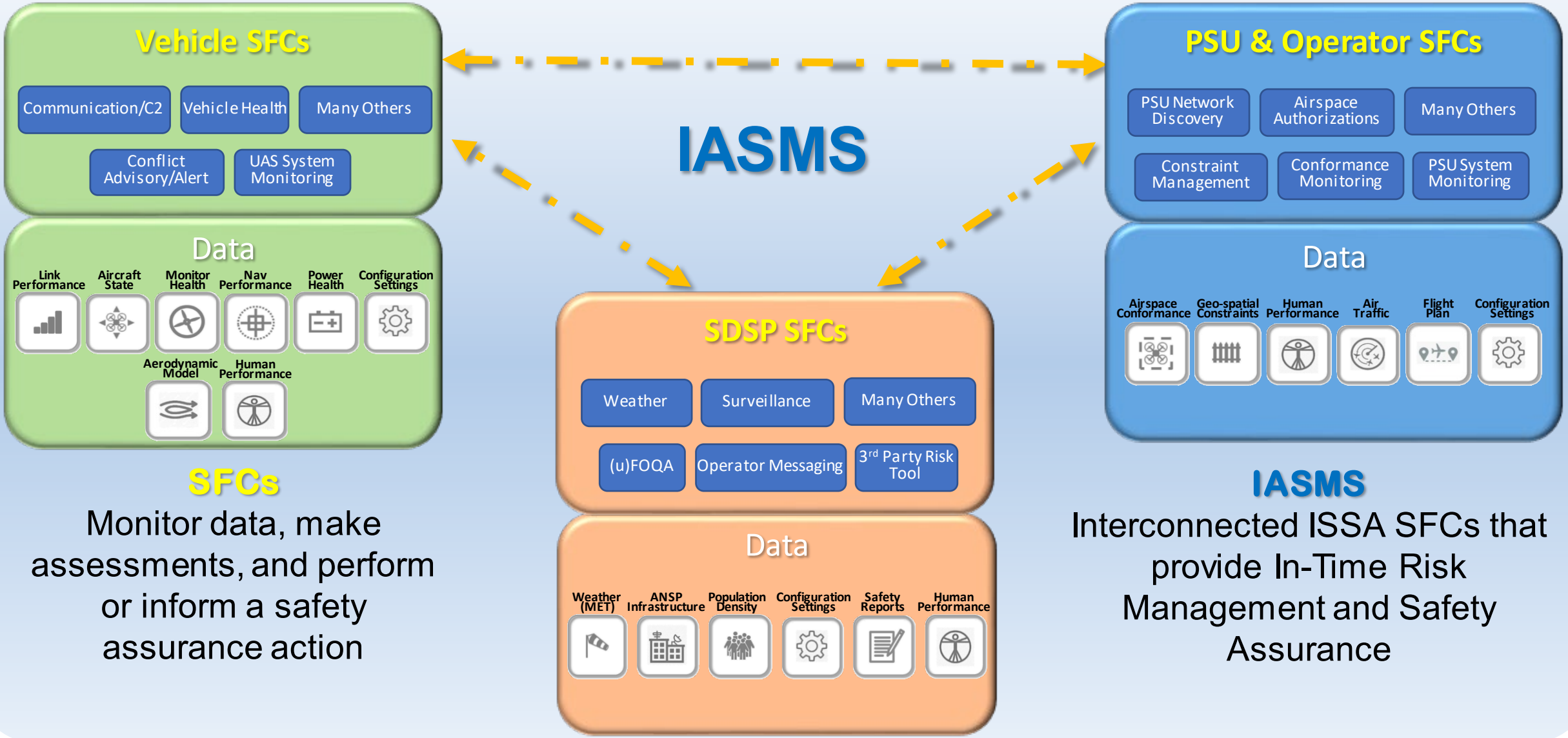
Information classes useful to enable IASMS SFCs

- ANSP Sourced
- Operator Sourced
- Vehicle Sourced
- Supplemental Data Service Provider (SDSP) Sourced
- System Wide Information Management (SWIM) / Flight Information Management System (FIMS) Sourced
- Other Sources…



(Young, S., et.al, 2020)

Service Oriented Architecture



SFCs

Monitor data, make assessments, and perform or inform a safety assurance action

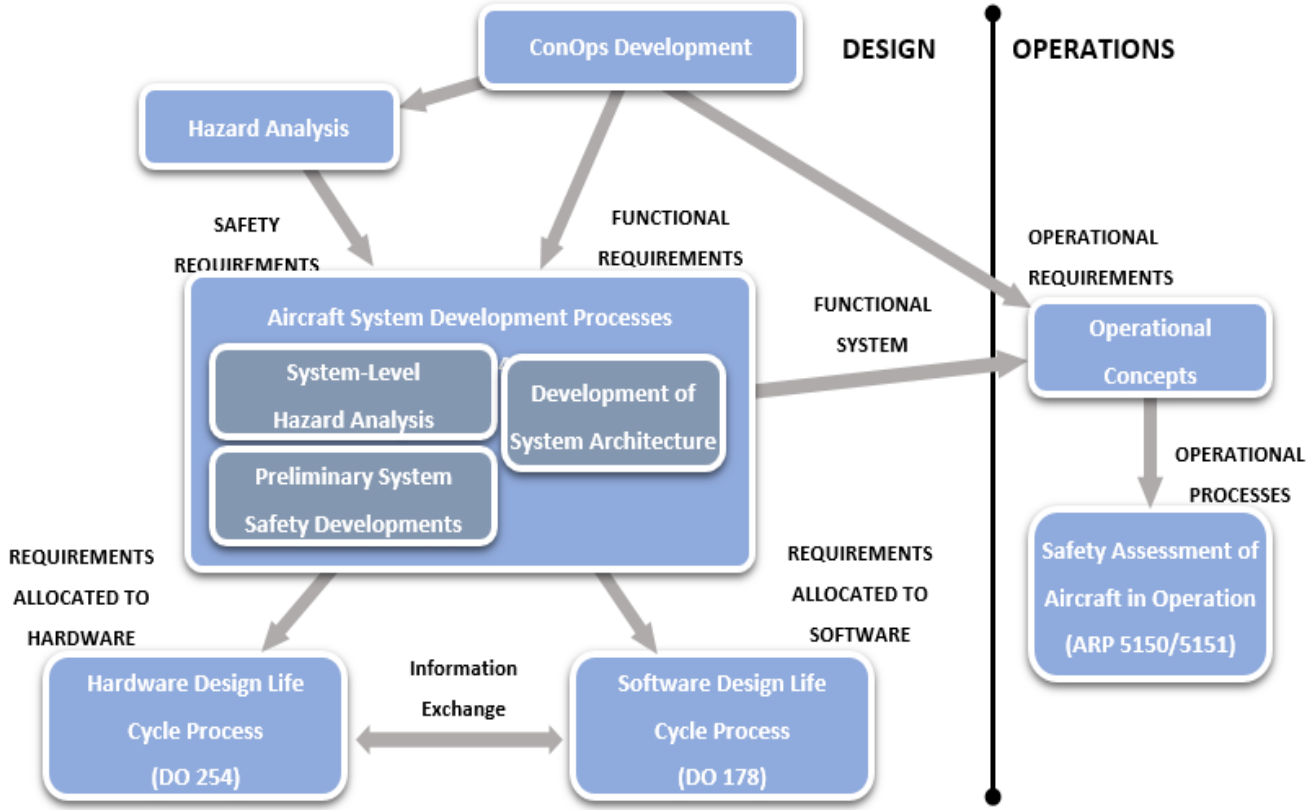
IASMS

Interconnected ISSA SFCs that provide In-Time Risk Management and Safety Assurance

SFC Assurance of Functionality

Assure Design

- Assurance requirements are specific to flight rules, operation complexity and risk criticality (SORA helps here)
- SFCs must be assured to an appropriate level via an acceptable process



Building Confidence

SFCs that

Manage Operational Risks:

Must mitigate risks with an acceptable level of certainty

SFCs that

Identify Unknown Risks:

Must correctly identify unknown anomalies and hazards in the system

SFCs that

Inform System Designs:

Must correctly assess performance and deficiencies of the existing design

SFC Assurance of Functionality

Assure Design

- **Assurance requirements are specific to flight rules, operation complexity and risk criticality (SORA helps here)**
- **SFCs must be assured to an appropriate level via an acceptable process**

Image credit: NASA

Building Confidence

SFCs that
Manage Operational Risks:
Must mitigate risks with an acceptable level of certainty

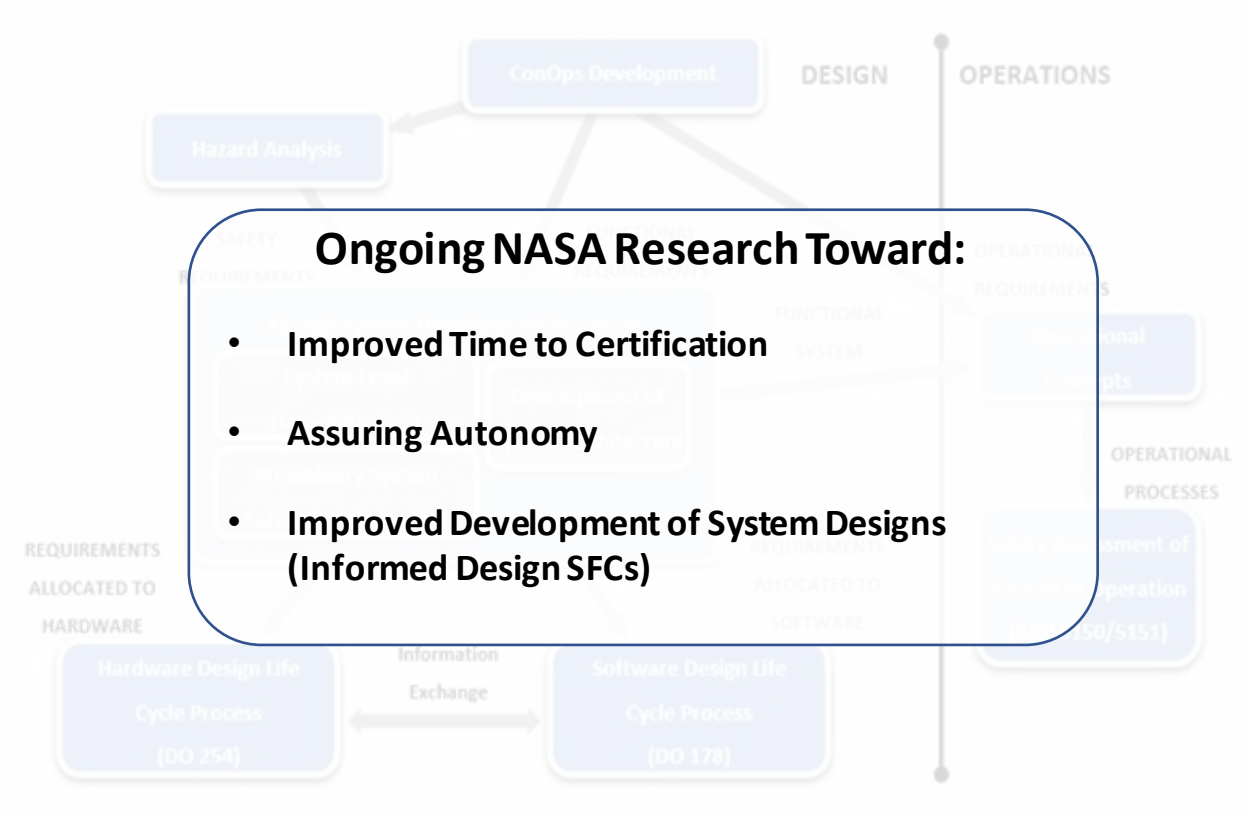
SFCs that
Identify Unknown Risks:
Must correctly identify unknown anomalies and hazards in the system

SFCs that
Inform System Designs:
Must correctly assess performance and deficiencies of the existing design

SFC Assurance of Functionality

Assure Design

- Assurance requirements are specific to flight rules, operation complexity and risk criticality (SORA helps here)
- SFCs must be assured to an appropriate level via an acceptable process



Ongoing NASA Research Toward:

- Improved Time to Certification
- Assuring Autonomy
- Improved Development of System Designs (Informed Design SFCs)

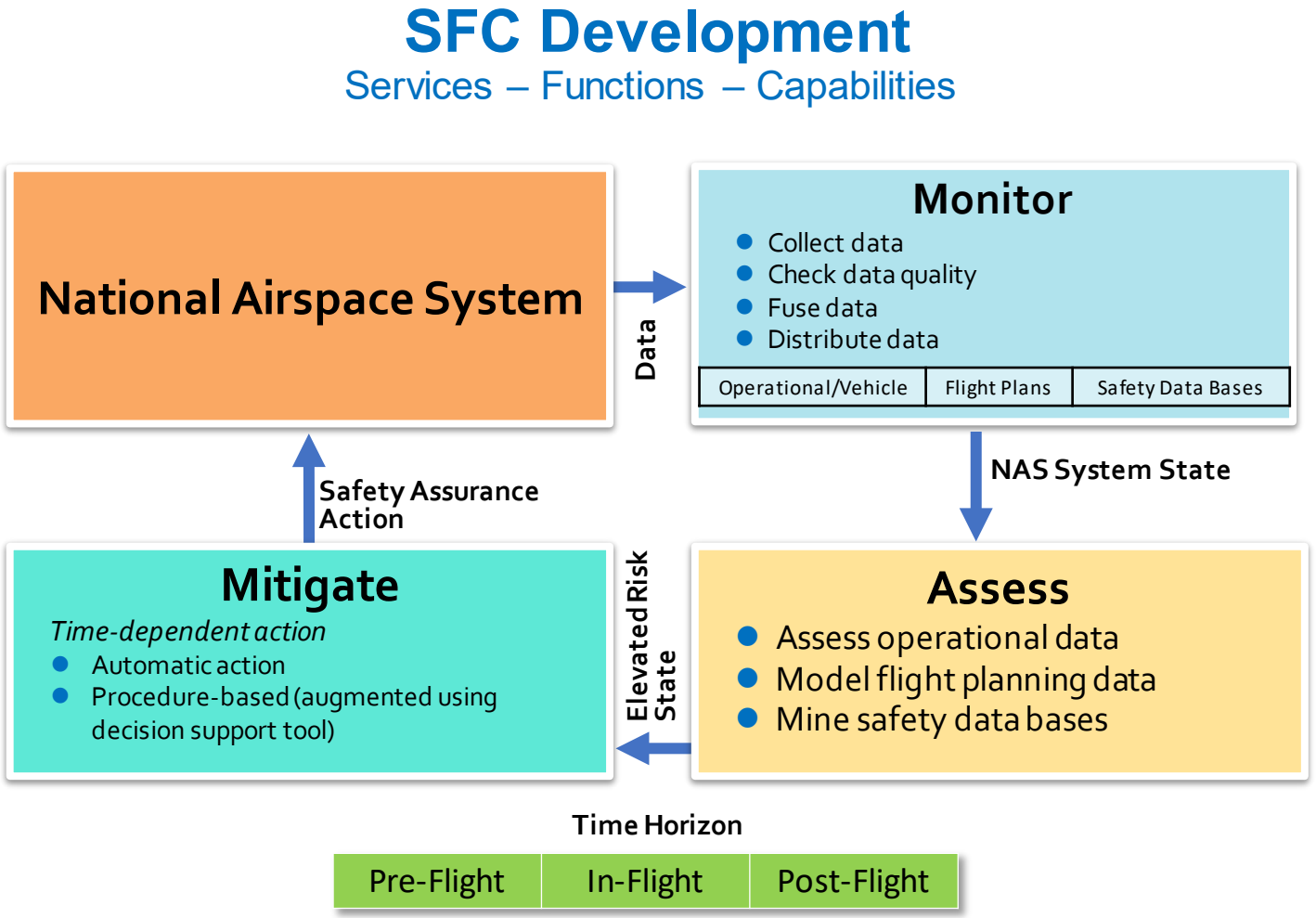
Building Confidence

SFCs that Manage Operational Risks:
Must mitigate risks with an acceptable level of certainty

SFCs that Identify Unknown Risks:
Must correctly identify unknown anomalies and hazards in the system

SFCs that Inform System Designs:
Must correctly assess performance and deficiencies of the existing design

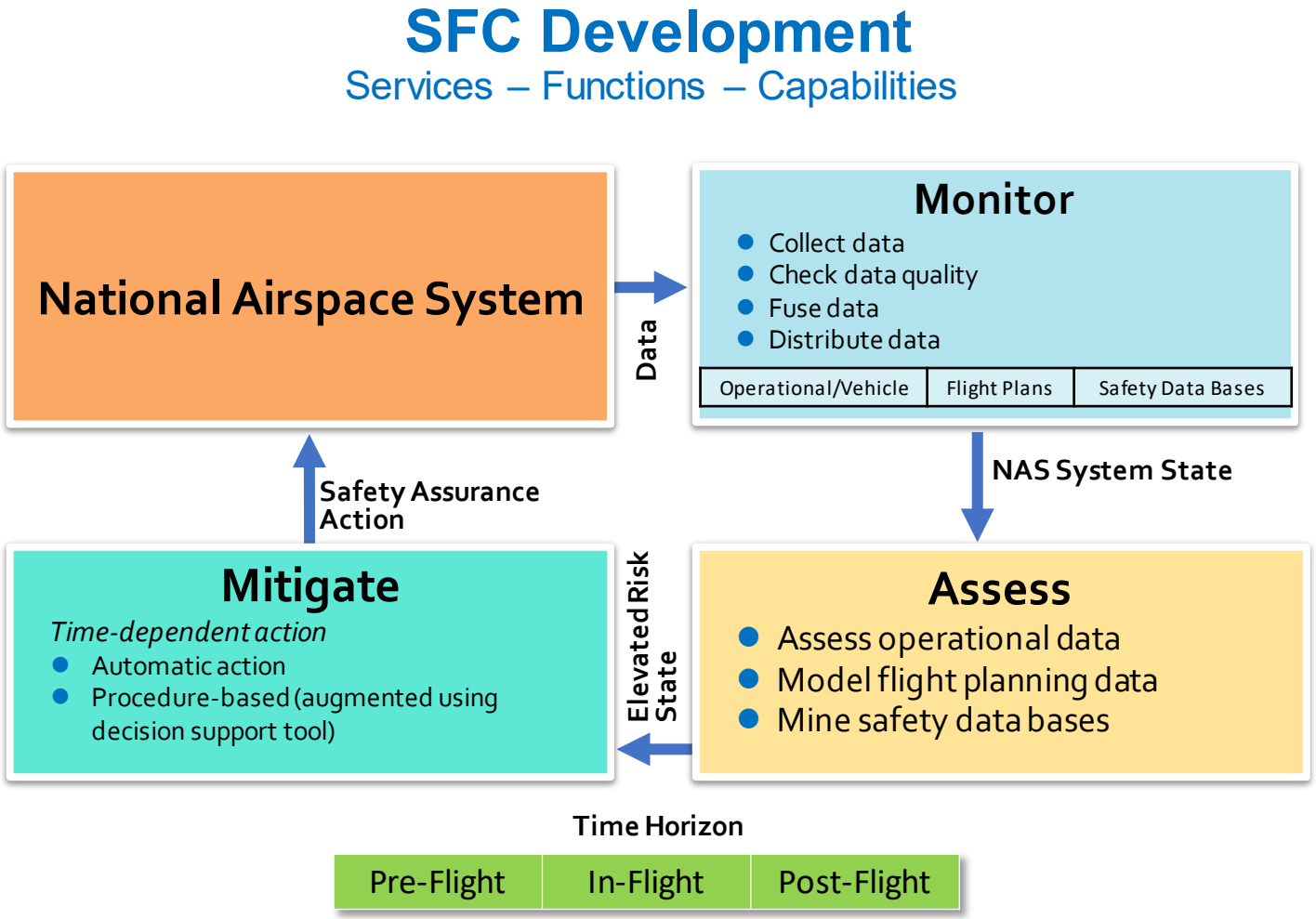
SFCs to Address Risks



Risks

- **Flight outside of approved airspace**
- **Unsafe proximity** to air traffic, people on the ground, terrain or property
- **Critical system failures** (including loss of link, loss or degraded positioning system performance, loss of power, flight control failure and engine failure
- **Loss-of-Control** (i.e., envelope excursions)
- **Physical/Environment Related Risks**
  - Weather encounters (including wind gusts)
  - Threat by person—malicious
- **Cyber-security** related risks
- Those our predictive and prognostic SFCs have **not identified yet…**

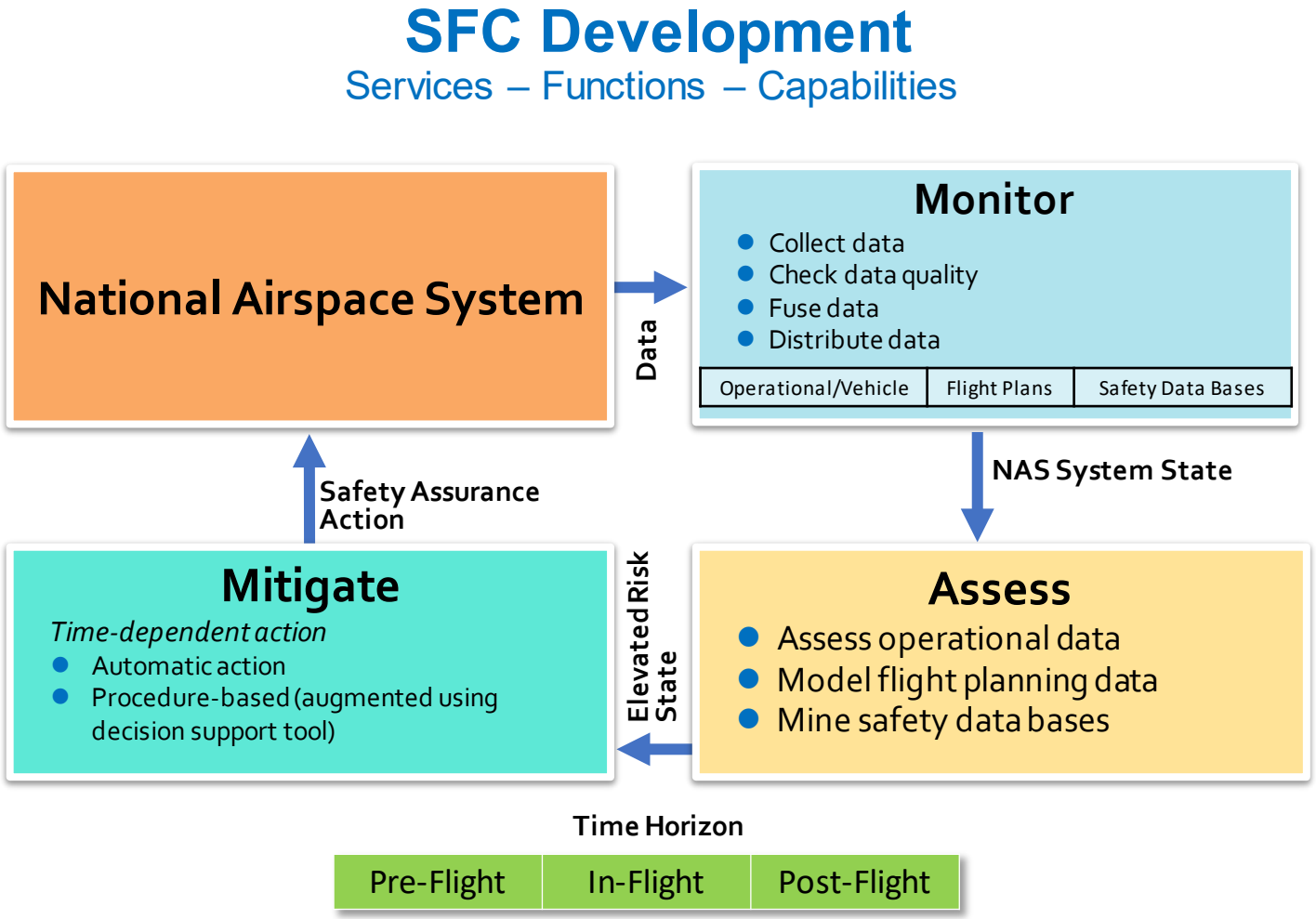
SFCs to Address Risks



Reference SFCs

- SAFEGUARD
- Proximity to Threat Service, Non-Participant Casualty Risk Assessment, ICAROUS, Safe2Ditch
- RF Interference Modeling
  GPS Degradation Modeling
  APNT Services (alternatives to GPS)
  Battery Health Prognostics
  Command and Control Link Monitor
- Hyper-local weather modeling → Climacell (SDSP example)
  Vehicle-as-a-sensor services
- Adaptive security procedure development
- Industry-developed Cyber-security solutions and protocols
- Multiple Kernel Anomaly Detection (MKAD)

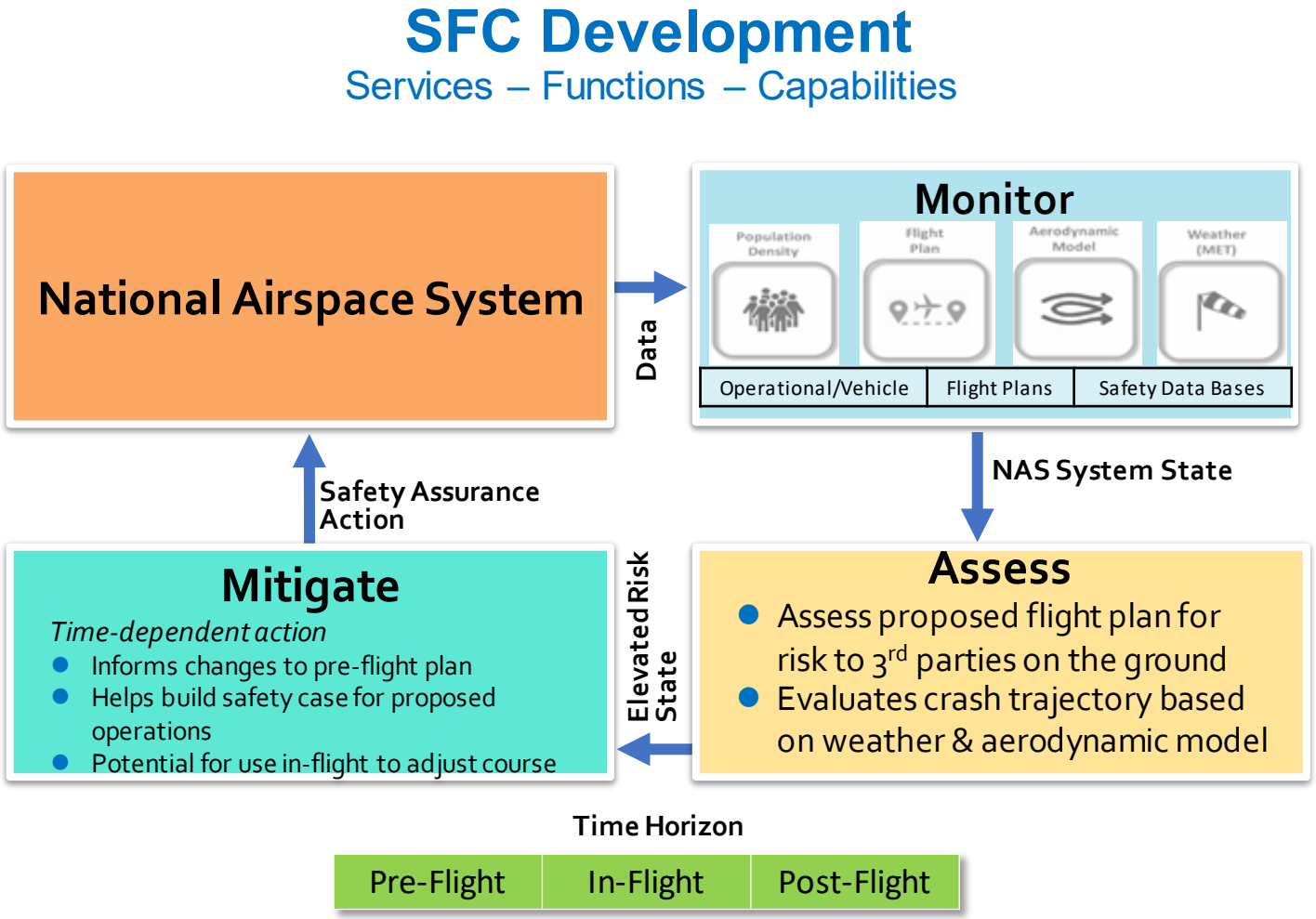
SFC Example – NPCRA Tool



Reference SFCs

- SAFEGUARD
- Proximity to Threat Service, **Non-participant Casualty Risk Assessment**, ICAROUS, Safe2Ditch
- RF Interference Modeling
  GPS Degradation Modeling
  APNT Services (alternatives to GPS)
  Battery Health Prognostics
  Command and Control Link Monitor
- Hyper-local weather modeling → Climacell (SDSP example)
  Vehicle-as-a-sensor services
- Adaptive security procedure development
- Industry-developed Cyber-security solutions and protocols
- Multiple Kernel Anomaly Detection (MKAD)

SFC Example – NPCRA Tool



Reference SFCs

- SAFEGUARD
- Proximity to Threat Service, **Non-participant Casualty Risk Assessment**, ICAROUS, Safe2Ditch
- RF Interference Modeling
  GPS Degradation Modeling
  APNT Services (alternatives to GPS)
  Battery Health Prognostics
  Command and Control Link Monitor
- Hyper-local weather modeling → Climacell (SDSP example)
  Vehicle-as-a-sensor services
- Adaptive security procedure development
- Industry-developed Cyber-security solutions and protocols
- Multiple Kernel Anomaly Detection (MKAD)

SFC Maturity for IASMS Evolution

In-Time

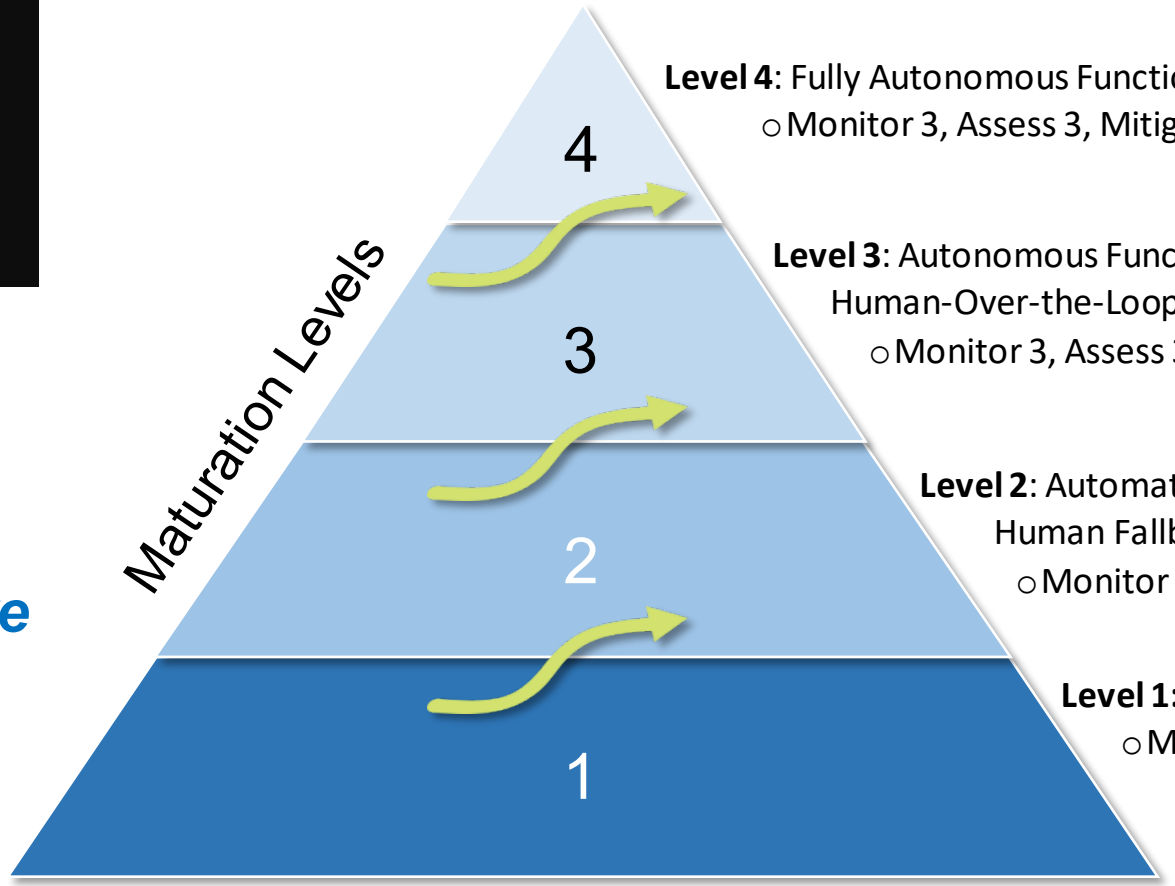
Adaptive

Increasingly Scalable

Decreasingly Labor-Intensive

SFC Maturity

Services – Functions – Capabilities



Level 4: Fully Autonomous Functionality
- Monitor 3, Assess 3, Mitigate 3

Level 3: Autonomous Functionality with Human-Over-the-Loop
- Monitor 3, Assess 3, Mitigate 2

Level 2: Automated Function with Human Fallback
- Monitor 2, Assess 2, Mitigate 1

Level 1: Alerting Function for Human
- Monitor 1*; Assess 1, Mitigate 0

*The Monitor-Assess-Mitigate numbers signify increases in capability

IASMS Capability Development Goal

Through a series of operationally challenging demonstrations, develop and demonstrate an assured system-wide safety framework that enables increasingly complex airspace operations.

- ***Safety framework*** is the set of requirements and their substantiations needed to enable safe, repeatable and efficient access to the NAS

- Such a safety framework may be highly valuable in supporting the FAA's rule-making process for UAS operations across many domains

Establishing the IASMS Safety Framework

Concept of Operations

Hazard Analysis: Identify Safety Critical Risks

Determine Acceptable Safety Assurance Requirements

IASMS Services and Capabilities Framework of SFCs to Assure Safety

Data and Architecture Requirements for IASMS SFCs

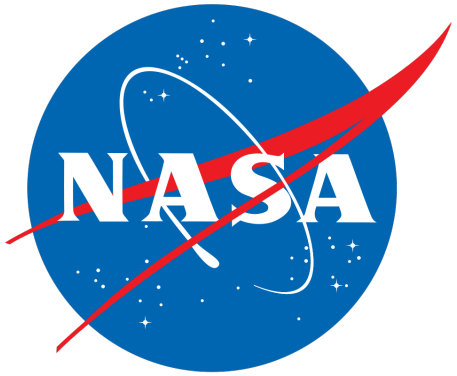
Development of Assured Functional IASMS

Flight Demonstration with Functional & Assured IASMS

Operational IASMS Data Generation to Inform Recommendations for Safety Framework Standards

Recommendations Document published by Standards Committees to Inform Safety Framework Requirements

New Safety Framework Requirements Established by Regulators (FAA)



SAE INTERNATIONAL

UL

ASTM INTERNATIONAL
Standards Worldwide

RTCA

IASMS in Operational Context

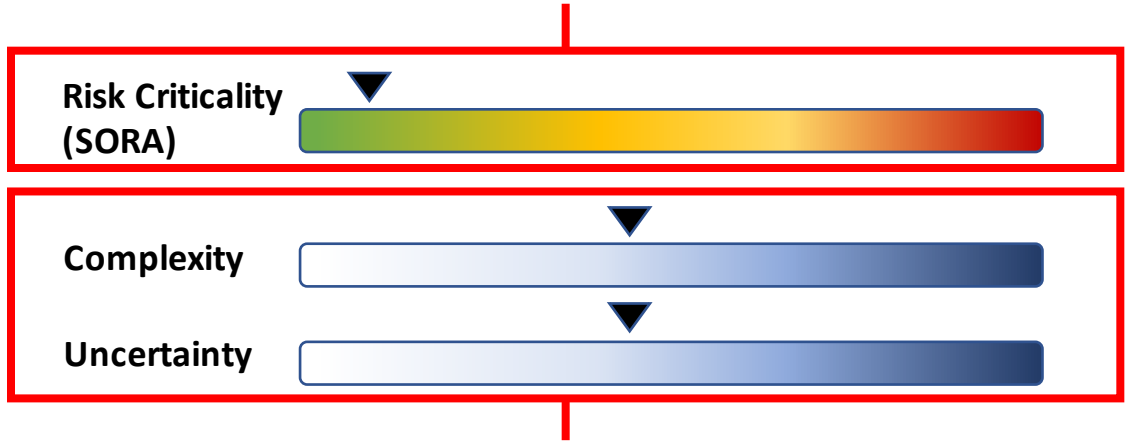
Increasingly Complex and Risk Critical Operational Use Cases:

1. Wildfire Fighting
2. Post-Hurricane Disaster Relief and Survey
3. Medical Courier Delivery (Urban Environment)
4. Un-evacuated Urban Area Disaster Response

….

10+. UML-4 Urban Air Taxi Ops

Risk criticality primarily affects the maturity and required assurance levels of the IASMS and its SFCs

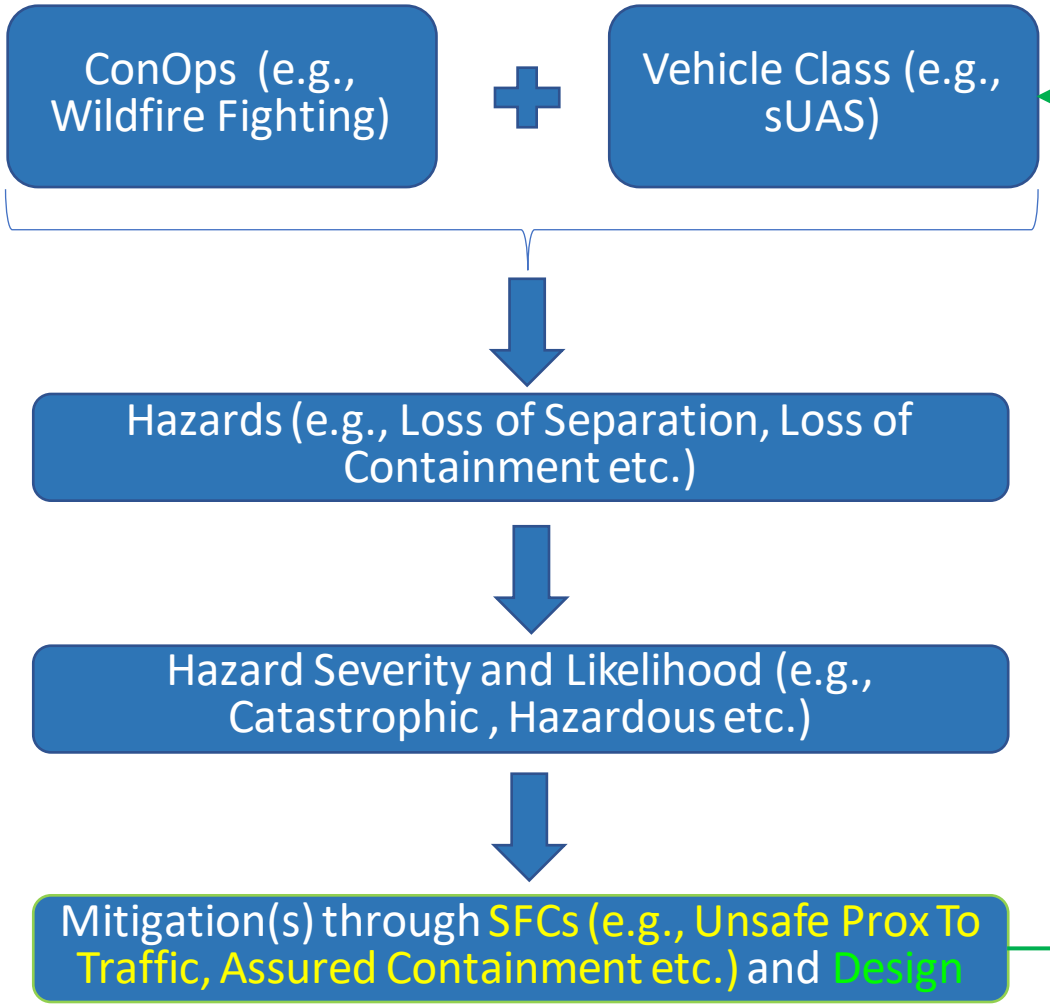


Complexity and uncertainty primarily affect the number of required SFCs

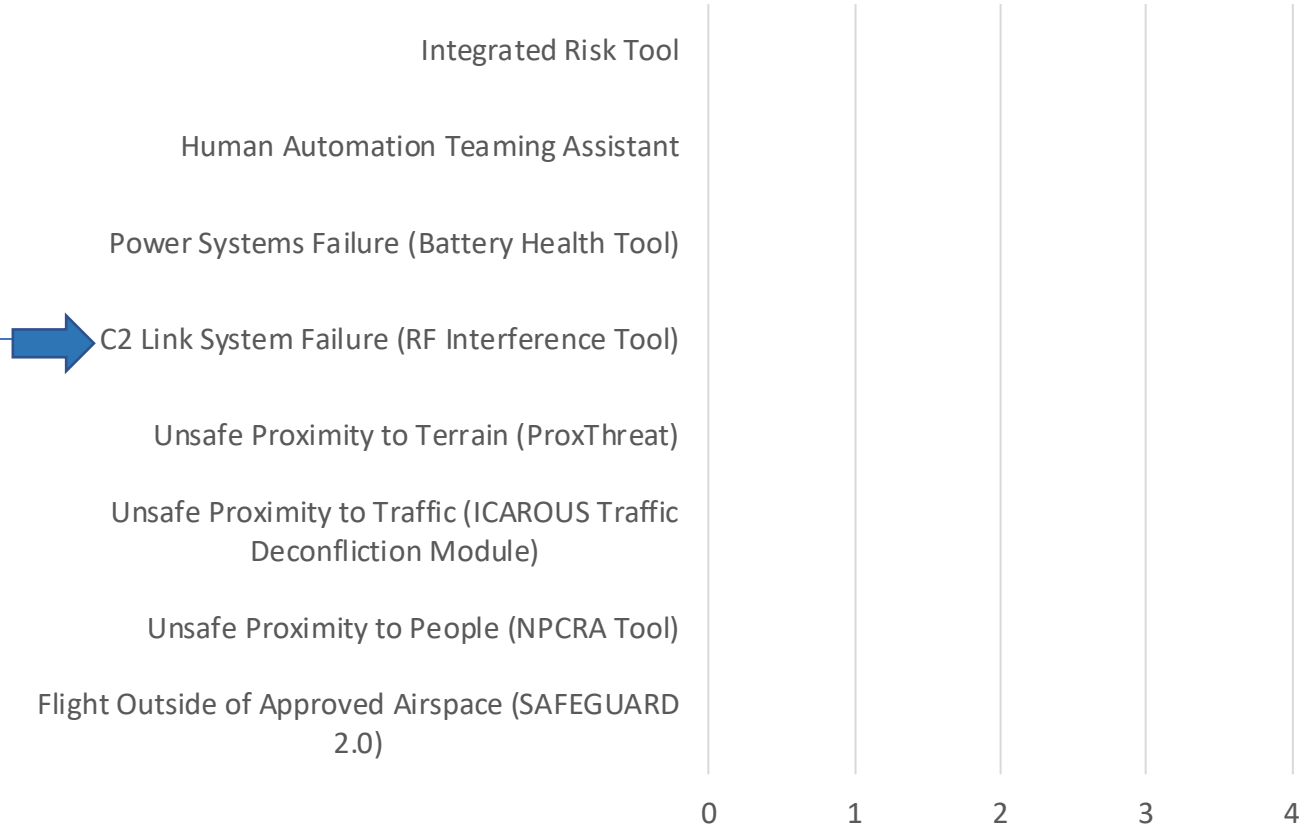
Seek to address industry needs by:

- Increasing the maturity of the individual SFCs that measure and ensure safety
- Placing those SFCs in the framework of an IASMS that enables rapid approval of operations
- Moving to operational use cases in which the IASMS must be able to handle increased complexity and uncertainty, and a reduced tolerance for risk in a manner that generates data to validate operational safety frameworks (Increasing IASMS Capability Level)

IASMS Capability Levels Explained (I)

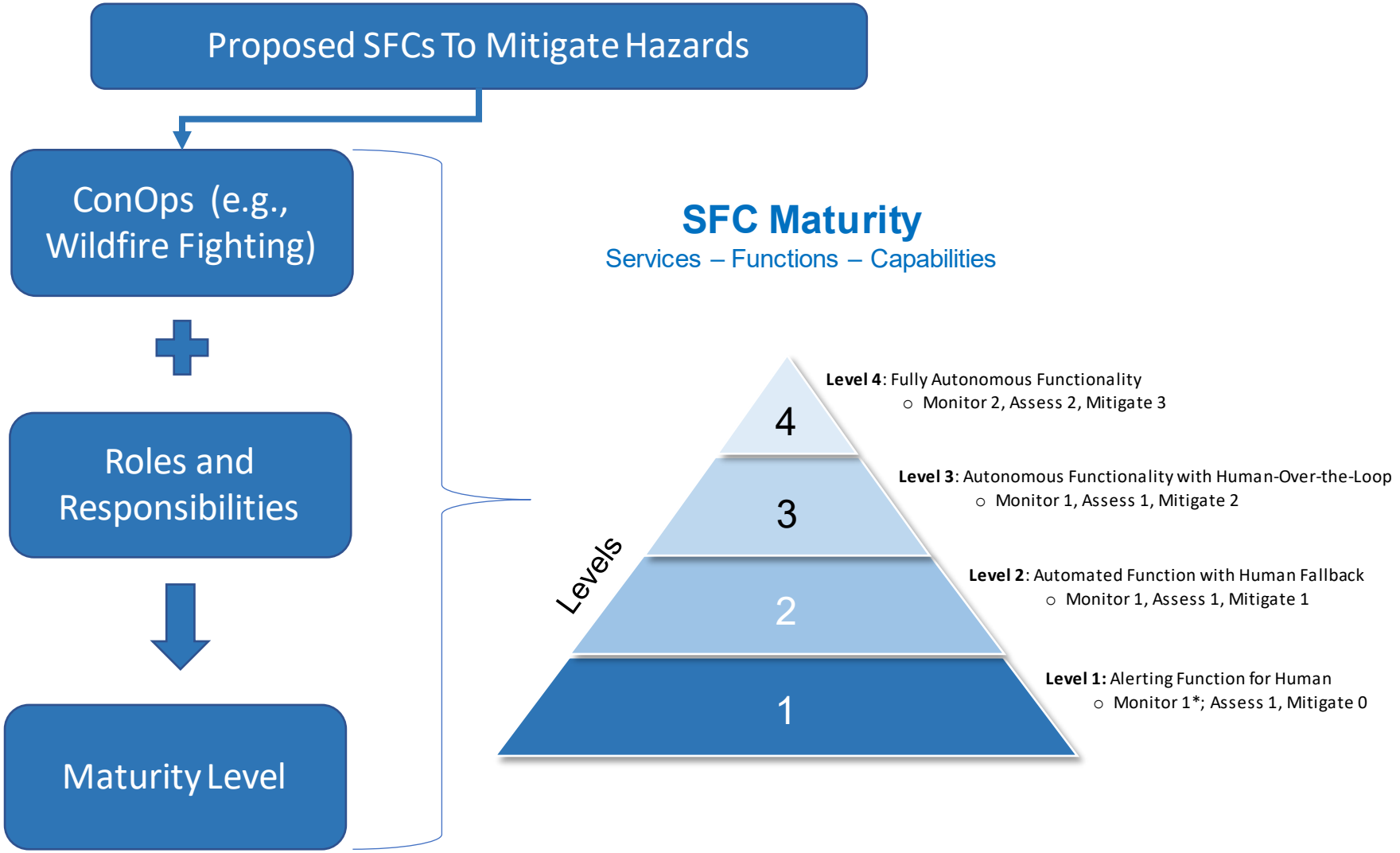


SD-1 Proposed Key SFCs For SD-1 (Wildfire Fighting)



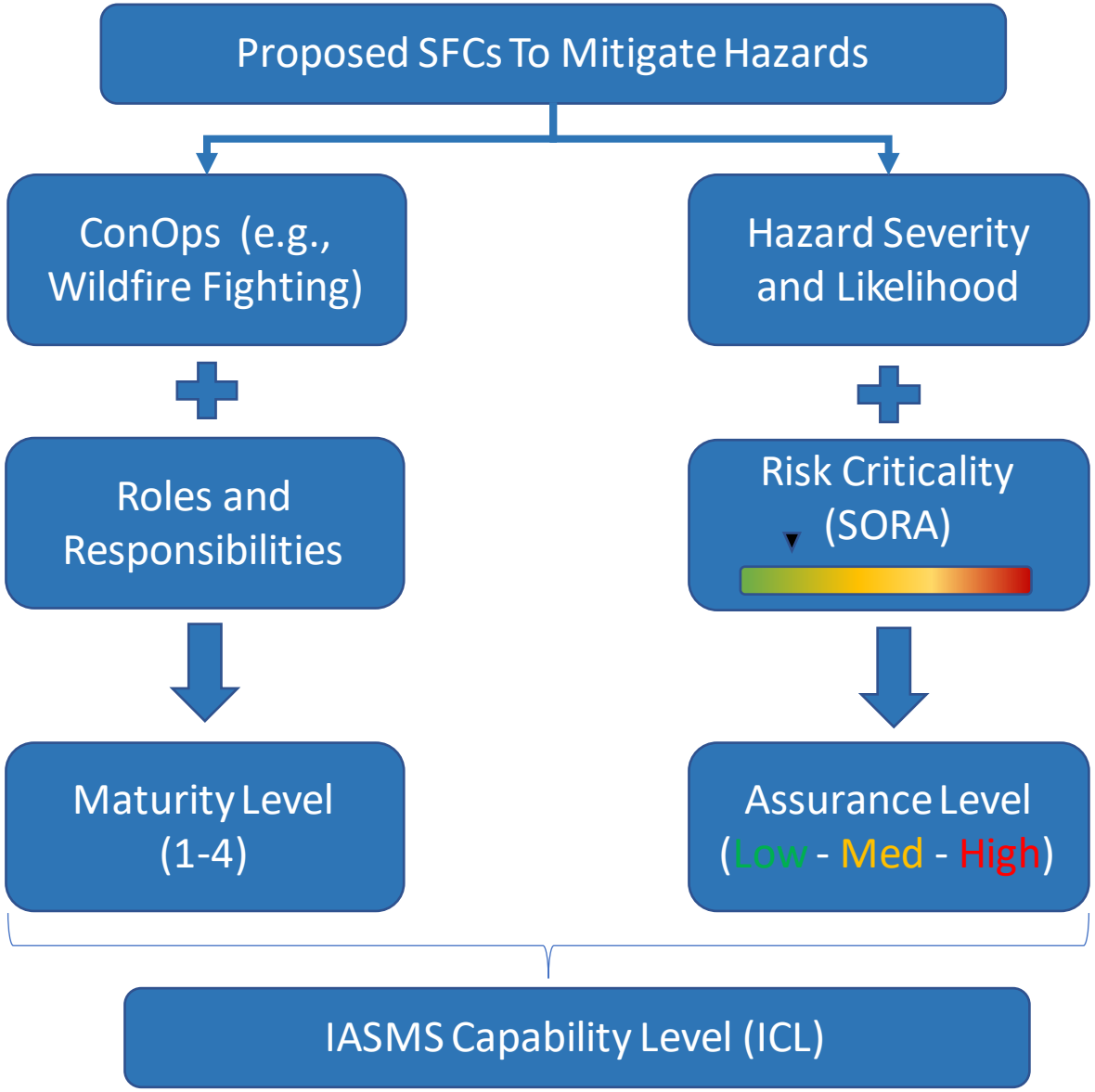
Note: Proposed SFCs and ICLs to enable safe operations are still being analyzed with our operational and regulatory partners.

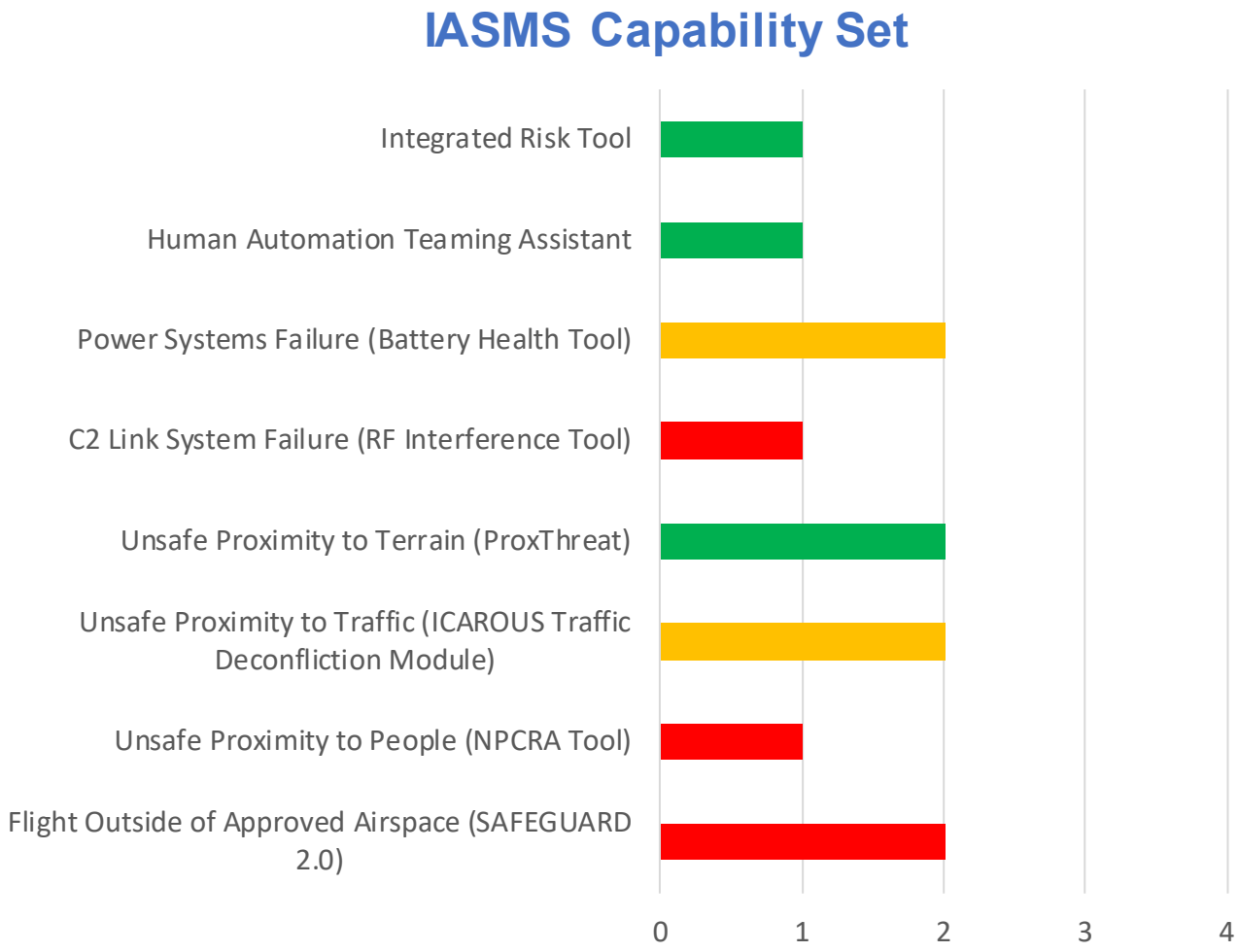
IASMS Capability Levels Explained (II)



Note: Proposed SFCs and ICLs to enable safe operations are still being analyzed with our operational and regulatory partners.

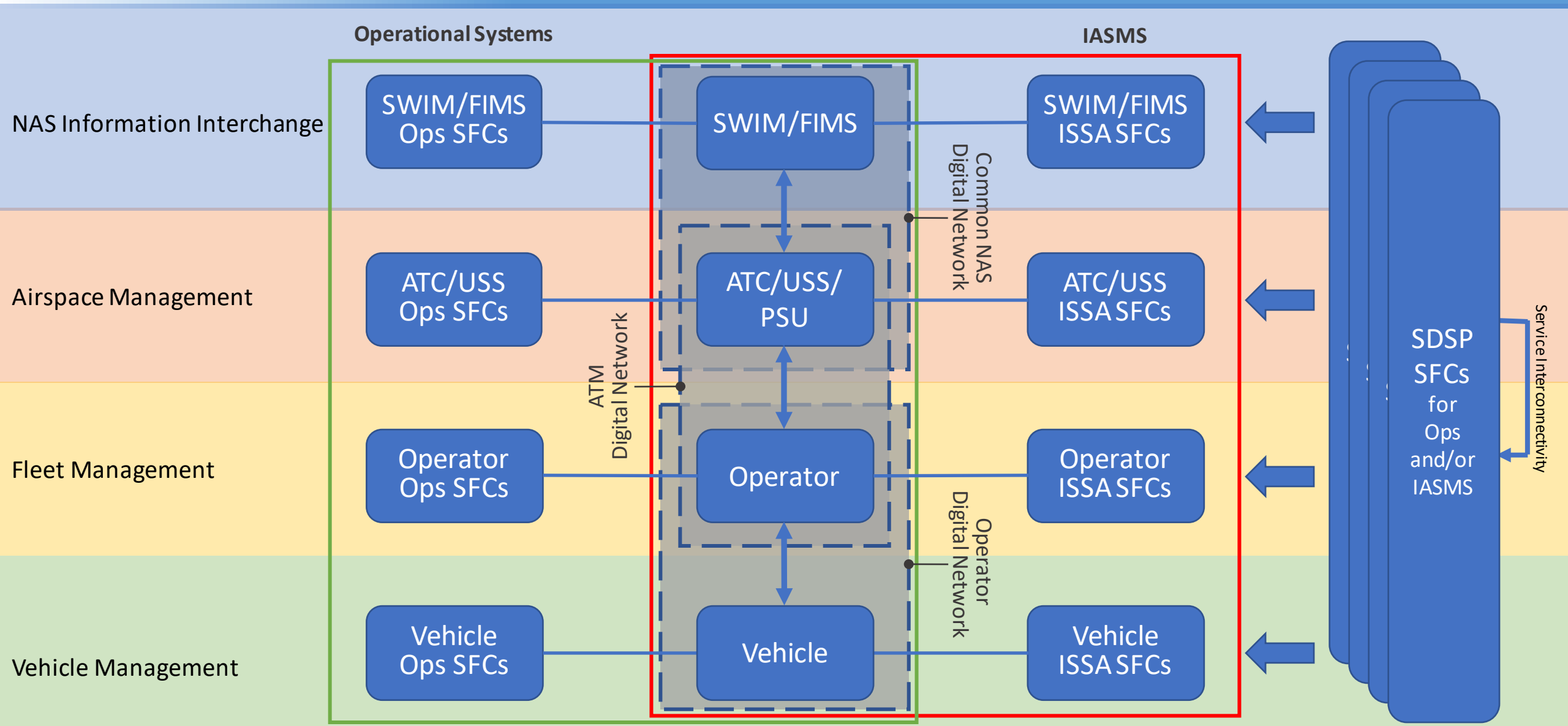
IASMS Capability Levels Explained (III)



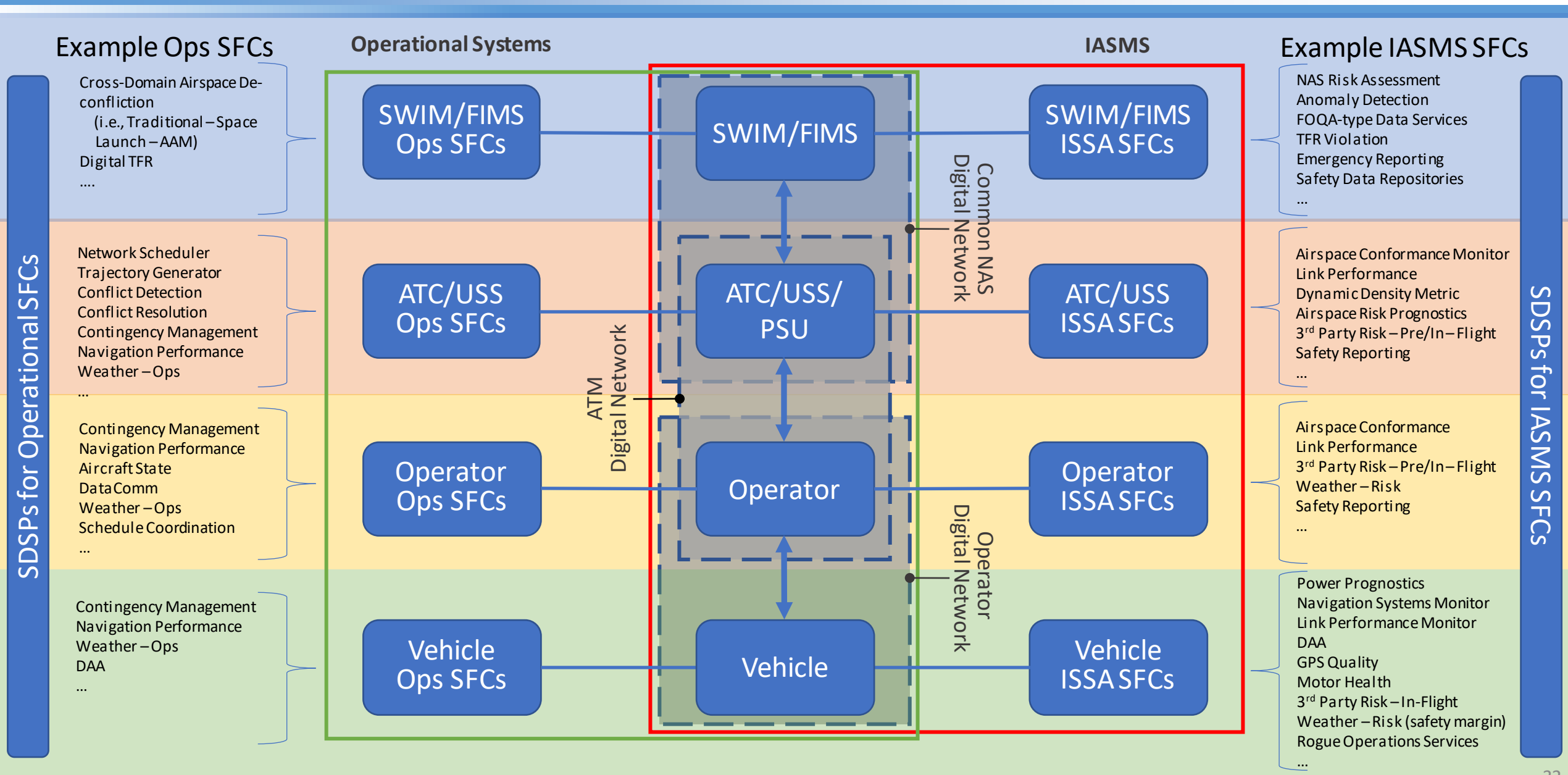


Note: Proposed SFCs and ICLs to enable safe operations are still being analyzed with our operational and regulatory partners.

IASMS Integration and Architecture



Service-Oriented Architecture



Test System Architecture

OS&N: Observation Stations and Network – Exemplars of urban infrastructure

Based on NASA-TM/2020-220440 (Jan 2020) (Revised)

NavQ OS&N | Wx OS&N | RFE/RFI OS&N

ARC SDSP (@ARC)

DD service | BP service | PtT service

BP+Eng

APPDAT Provider (@JSC)

NPCRA service | NavQ (CAP) service

TBD Provider

NavQ (GAP) service

LaRC SDSP (@LaRC)

RFE/RFI service | Wind service | OS&N service

USS (w ATM-X)

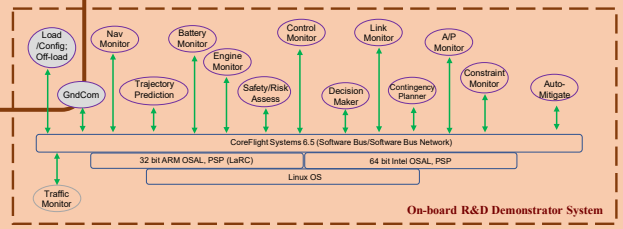
Other service(s)

Optional direct connect to services

Designers/ Analytics | Telemetry and Event "logs" | UAS Ground Station | USS/PSU | FIMS

Data and Event "logs"

UAS Vehicle System



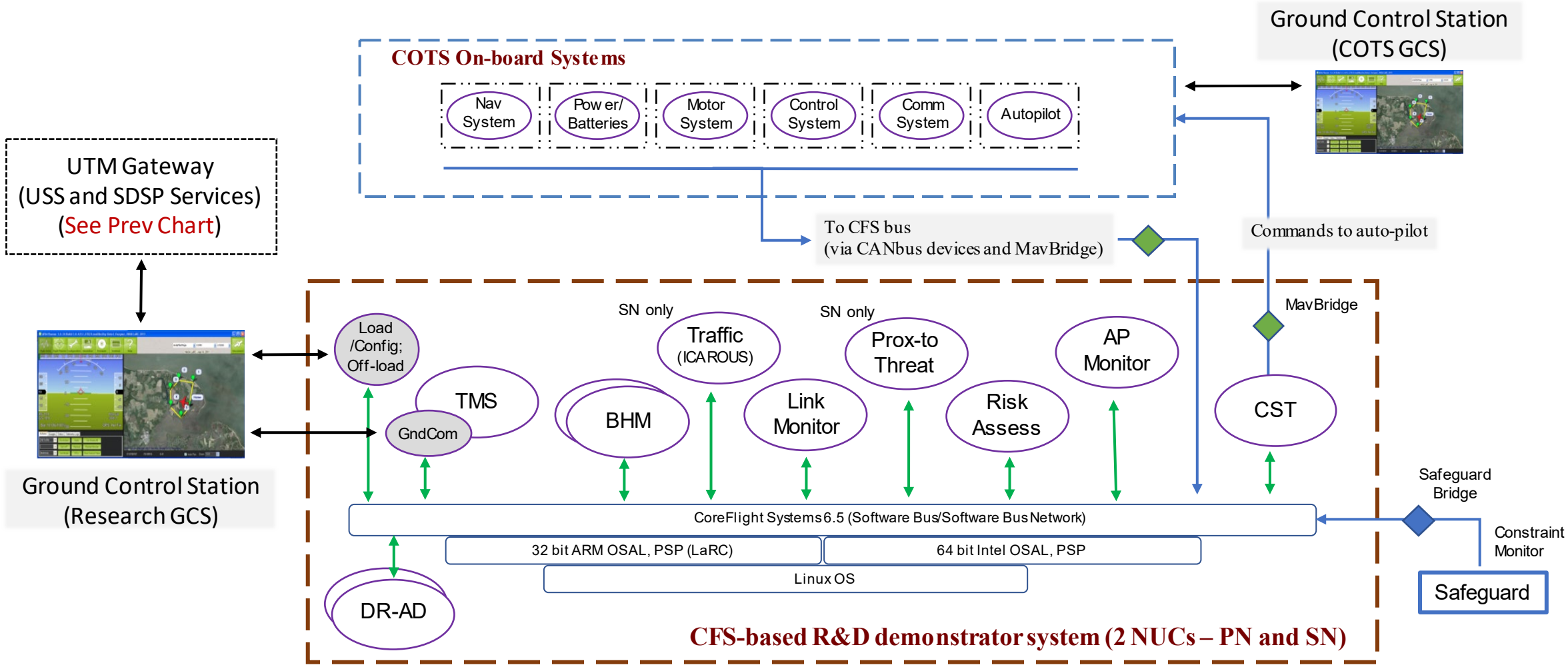
See next chart

Elements of 2019 test system (SWS-RED)

Added for 2021 test system (SWS-21)

Vehicle System Architecture

Based on NASA-TM/2020-220440 (January 2020) – Research support platform;
Revised to support evaluation of 2021 SFC set



CFS = Core Flight System (NASA GSFC platform for developing modular flight software; Certifiable to NASA Class B)

TMS = Telemetry Service; BHM = Battery Health Management; AP = Auto-pilot; CST = Contingency Select and Trigger; DR-AD = Diagnostic Reasoner and Anomaly Detector

Establishing the IASMS Safety Framework

Safety Demonstrator Series Concept of Operations

Hazards Analysis: Identify Safety Critical Risks

Determine Acceptable Safety Assurance Requirements

IASMS Services and Capabilities Framework of SFCs to Assure Safety

Data and Architecture Requirements for IASMS SFCs

Development of Assured Functional IASMS for SD Use Cases

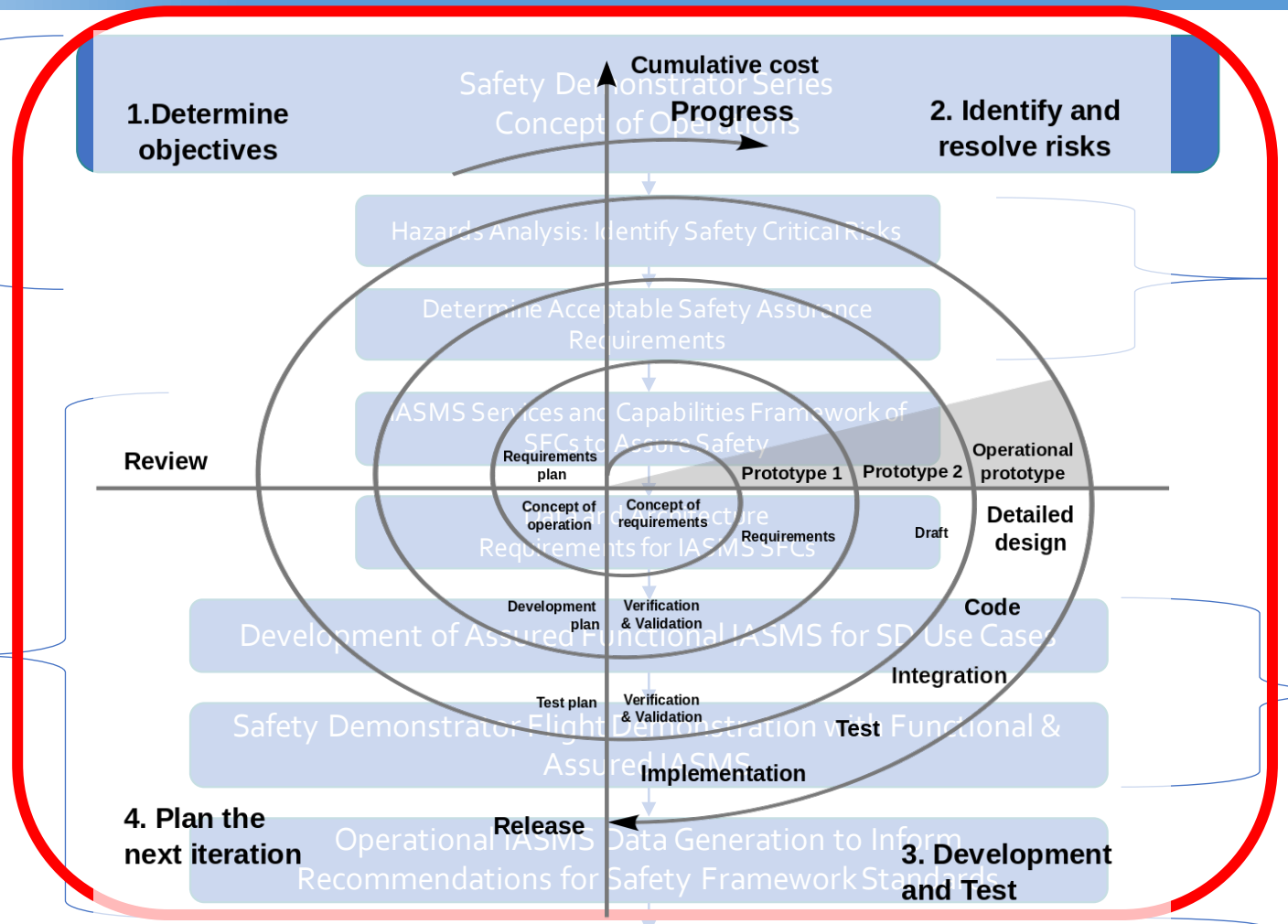
Safety Demonstrator Flight Demonstration with Functional & Assured IASMS

Operational IASMS Data Generation to Inform Recommendations for Safety Framework Standards

Recommendations Document published by Standards Committees to Inform Safety Framework Requirements

New Safety Framework Requirements Established by Regulators (FAA)

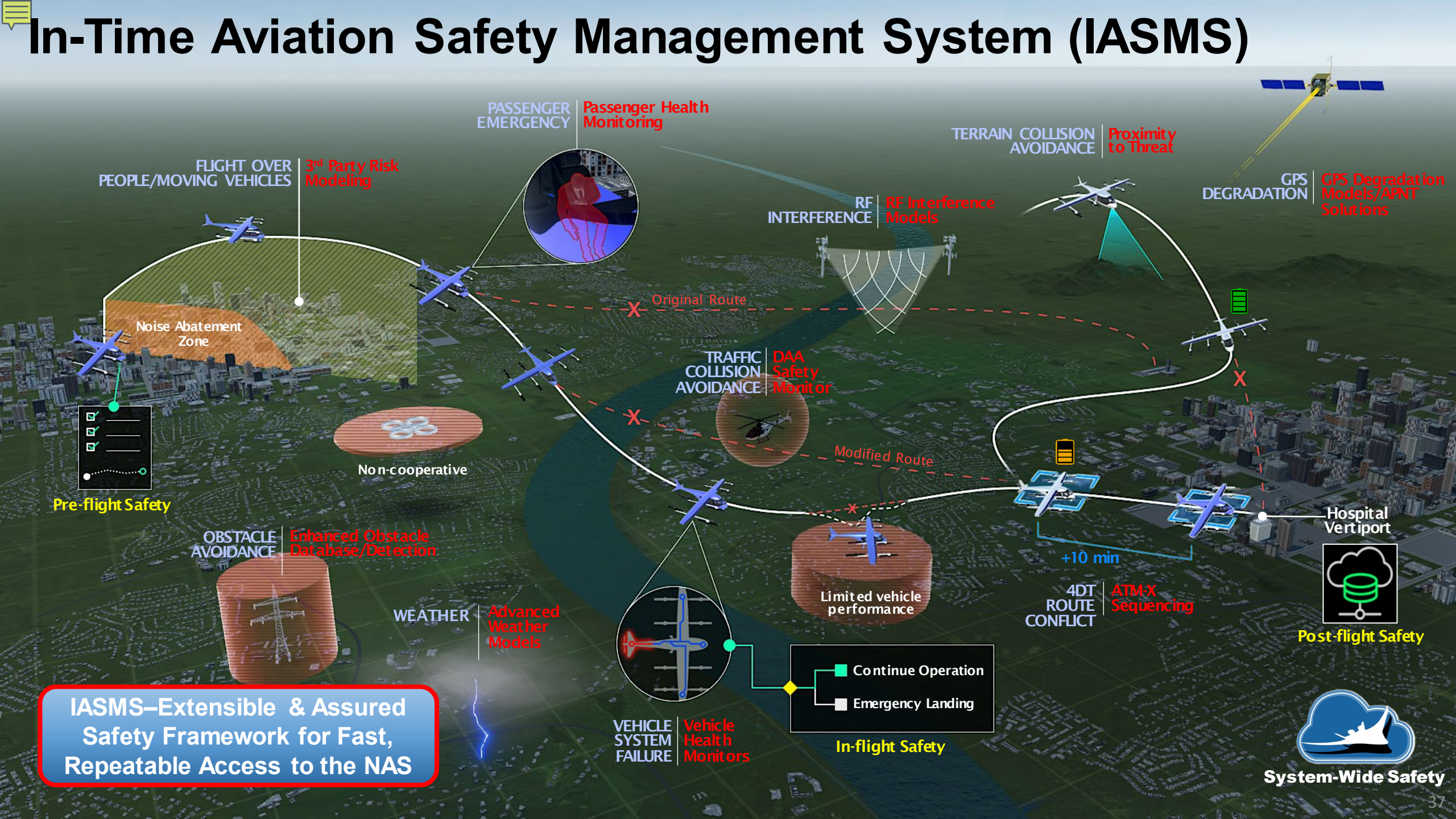
Spiral Development of IASMS



Recommendations Document published by Standards Committees to Inform Safety Framework Requirements

New Safety Framework Requirements Established by Regulators (FAA)

In-Time Aviation Safety Management System (IASMS)



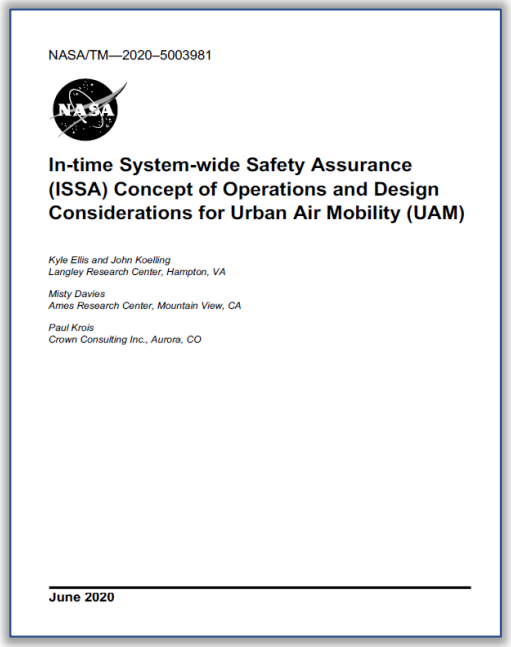
Progress Toward IASMS

National Academies Report

Identifies 4 Fundamental System Element Development Areas:

1. Concept of Operations and Risk Prioritization
2. System Monitoring
3. System Analytics
4. Mitigation and Implementation

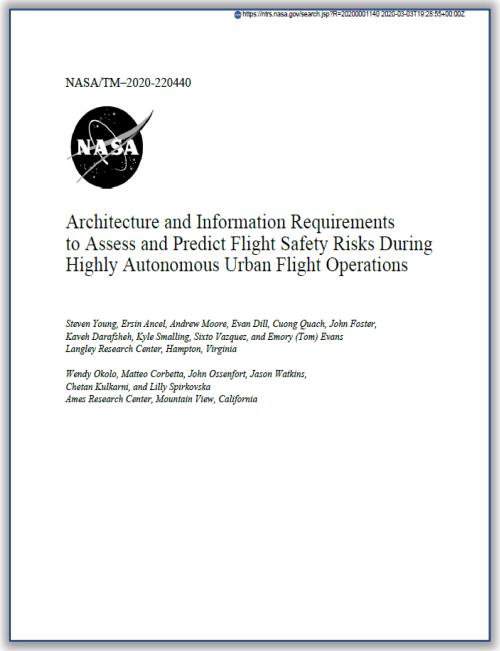
IASMS ConOps



Outlines Scope, Functionality and Risk Priorities for IASMS

1. Drafted with Industry Input
2. V.1 of ConOps focused on UAM domain with relevant use cases. V.2 expanding across domains (in dev)
3. FAA-NASA RTT Near-Term ConOps (in dev)
4. Built upon service-oriented architecture of UTM

Architecture and Information Requirements TM



Describes NASA approach to development of IASMS

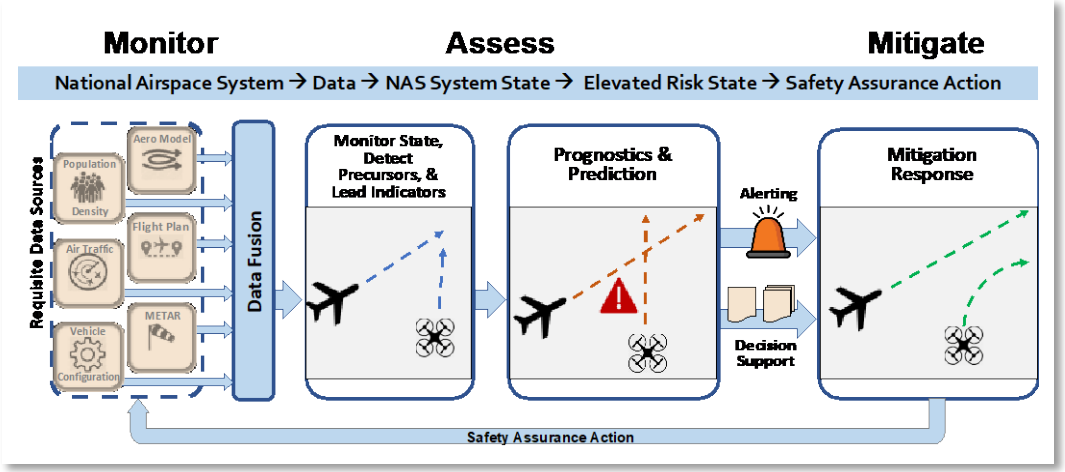
1. Identifies Information Classes
2. Discussion of Initial IASMS SFC Developments
3. Design Considerations for IASMS
4. Reference architecture for autonomous urban flight operation


NASA
EXPLORE FLIGHT
WE'RE WITH YOU WHEN YOU FLY

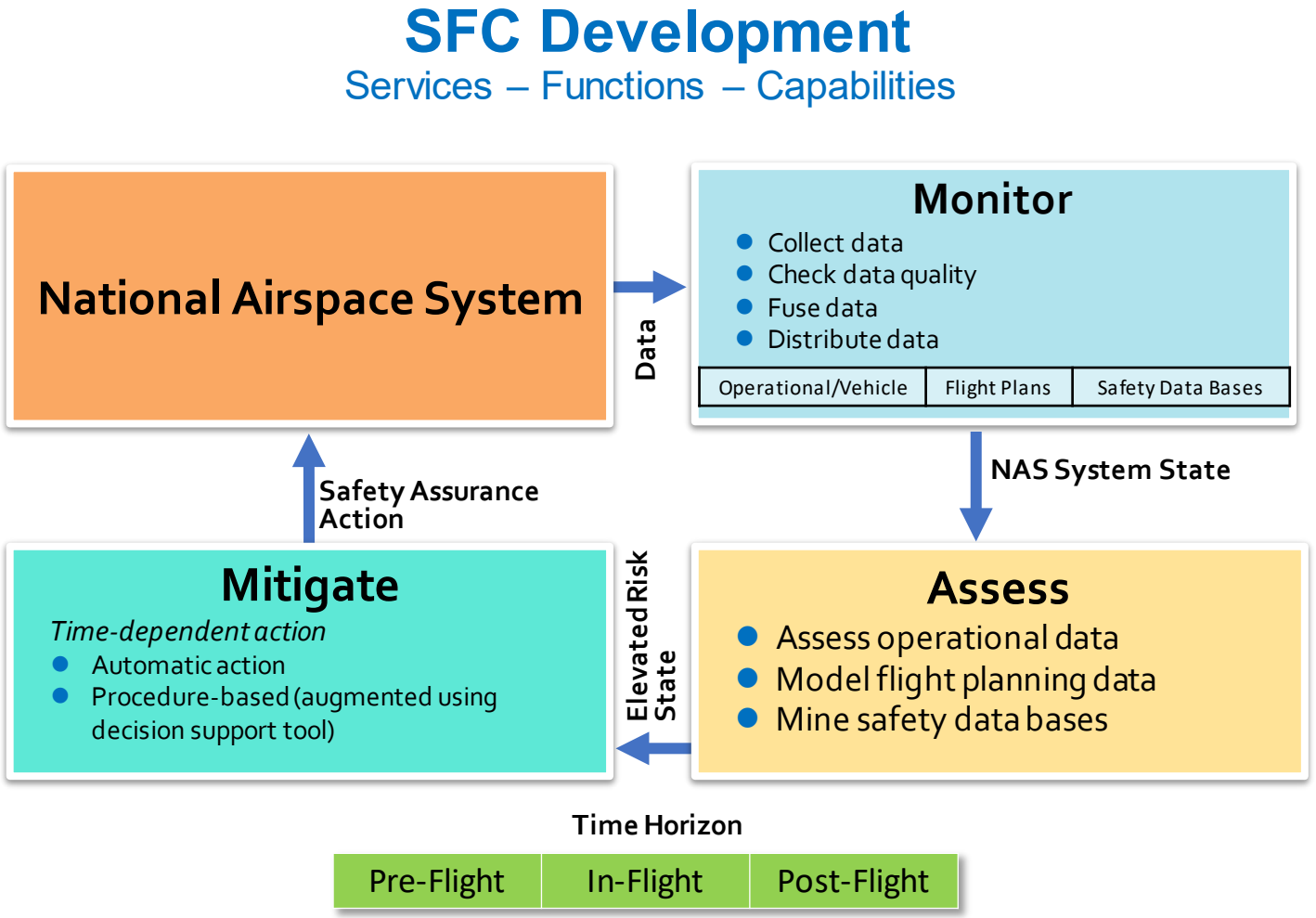
SWS Project Objectives

- To explore, discover, and understand the impact on safety of growing complexity introduced by modernization aimed at improving the efficiency of flight, the access to airspace, and/or the expansion of services provided by air vehicles.

- To develop and demonstrate innovative solutions that enable this modernization and the aviation transformation envisioned by ARMD through proactive mitigation of risks in accordance with target levels of safety.



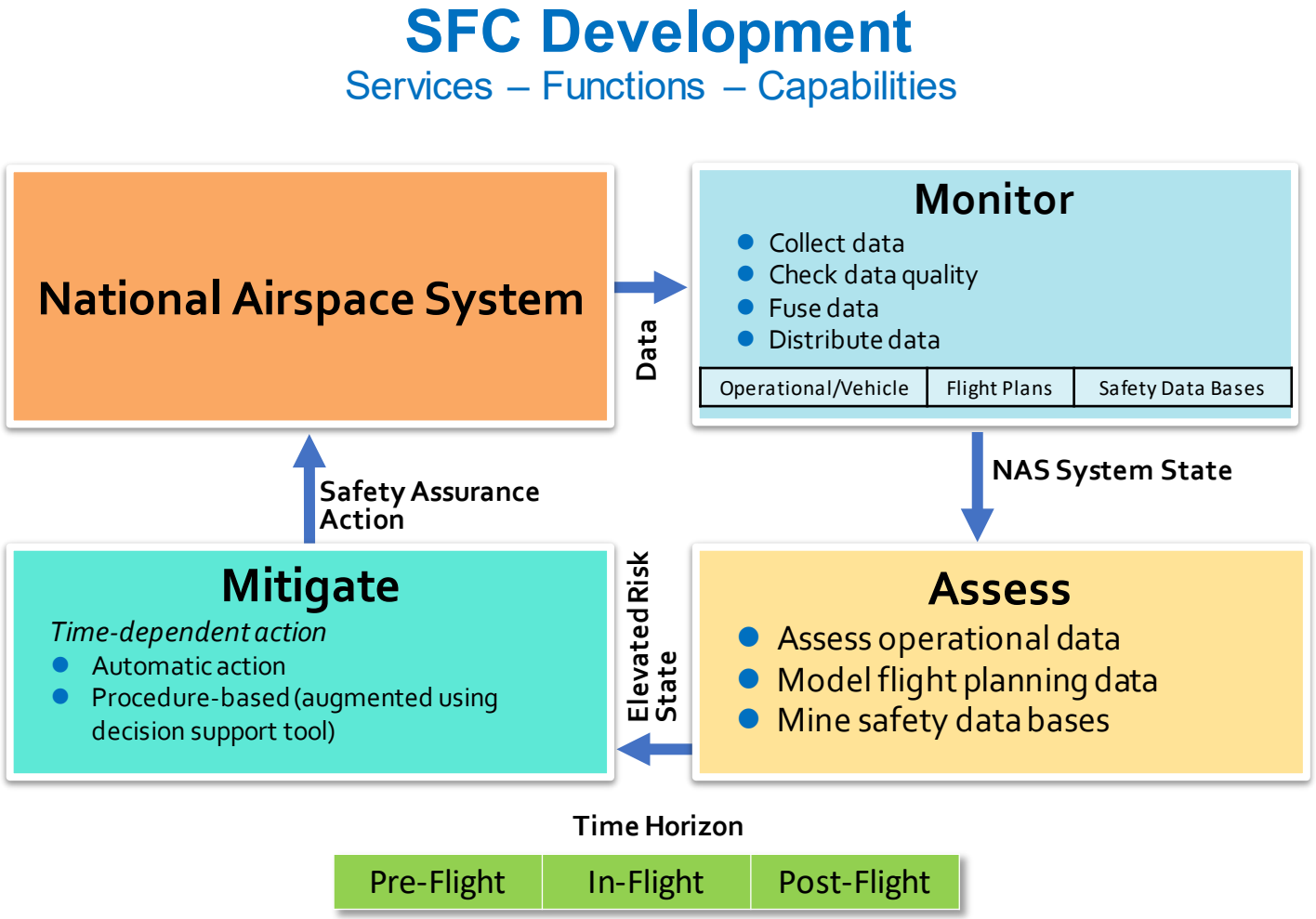
SFCs to Address Risks



Risks

- **Flight outside of approved airspace**
- **Unsafe proximity** to air traffic, people on the ground, terrain or property
- **Critical system failures** (including loss of link, loss or degraded positioning system performance, loss of power, flight control failure and engine failure
- **Loss-of-Control** (i.e., envelope excursions)
- **Physical/Environment Related Risks**
  - Weather encounters (including wind gusts)
  - Threat by person—malicious
- **Cyber-security** related risks
- Those our predictive and prognostic SFCs have **not identified yet…**

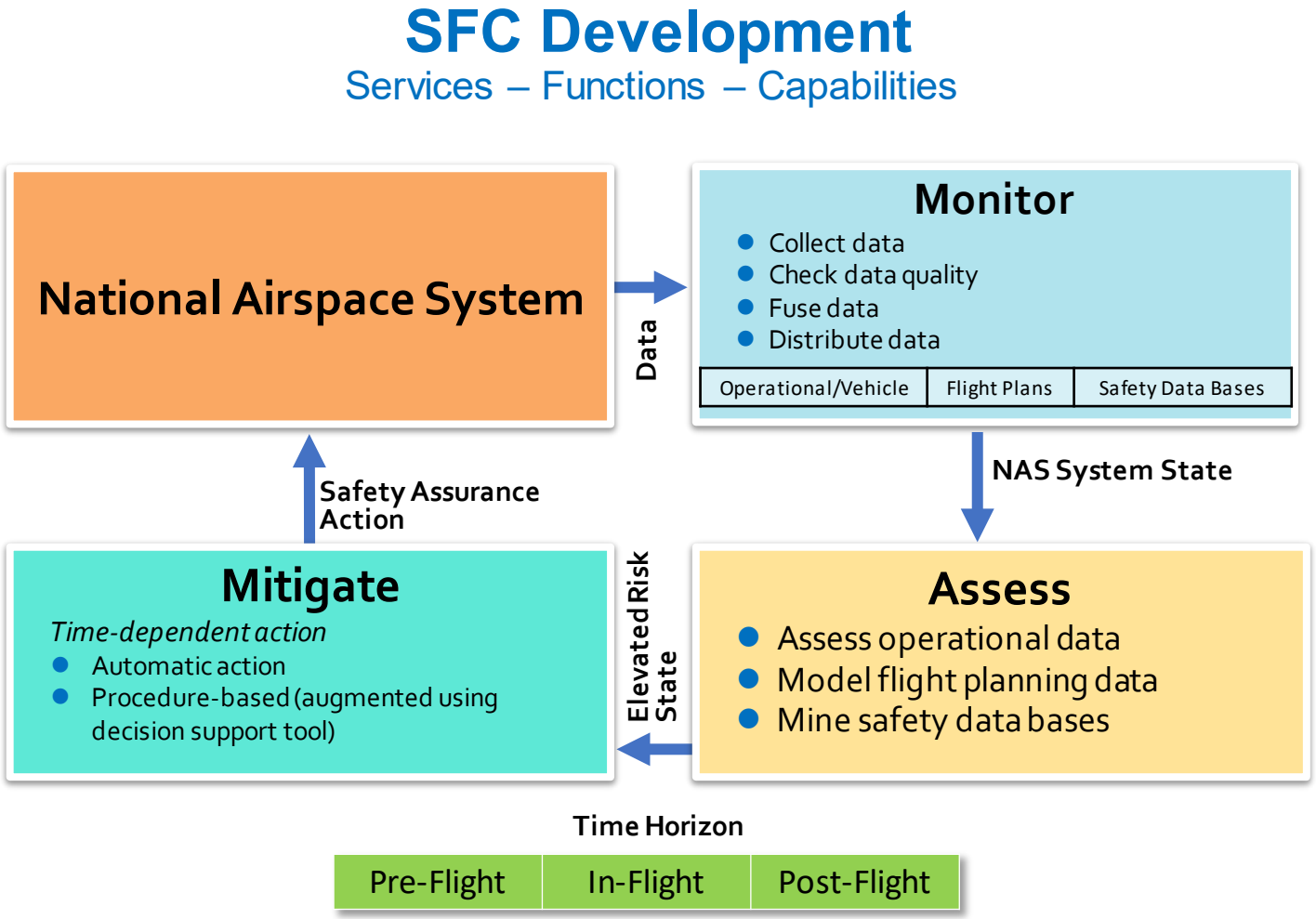
SFCs to Address Risks



Reference SFCs

- SAFEGUARD
- Proximity to Threat Service, Non-Participant Casualty Risk Assessment, ICAROUS, Safe2Ditch
- RF Interference Modeling
  GPS Degradation Modeling
  APNT Services (alternatives to GPS)
  Battery Health Prognostics
  Command and Control Link Monitor
- Hyper-local weather modeling → Climacell (SDSP example)
  Vehicle-as-a-sensor services
- Adaptive security procedure development
- Industry-developed Cyber-security solutions and protocols
- Multiple Kernel Anomaly Detection (MKAD)

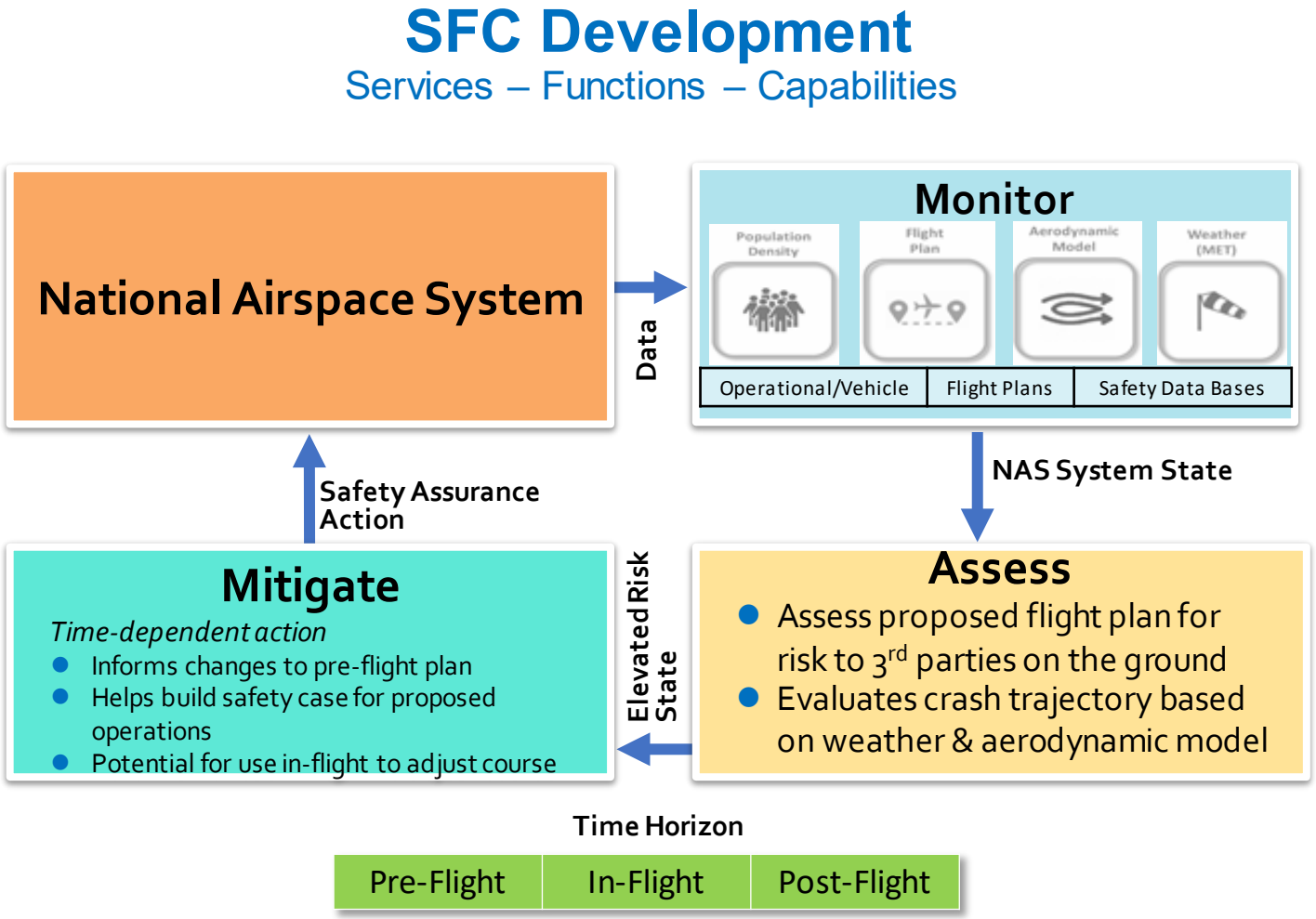
SFC Example – NPCRA Tool



Reference SFCs

- SAFEGUARD
- Proximity to Threat Service, **Non-participant Casualty Risk Assessment**, ICAROUS, Safe2Ditch
- RF Interference Modeling
  GPS Degradation Modeling
  APNT Services (alternatives to GPS)
  Battery Health Prognostics
  Command and Control Link Monitor
- Hyper-local weather modeling → Climacell (SDSP example)
  Vehicle-as-a-sensor services
- Adaptive security procedure development
- Industry-developed Cyber-security solutions and protocols
- Multiple Kernel Anomaly Detection (MKAD)

SFC Example – NPCRA Tool



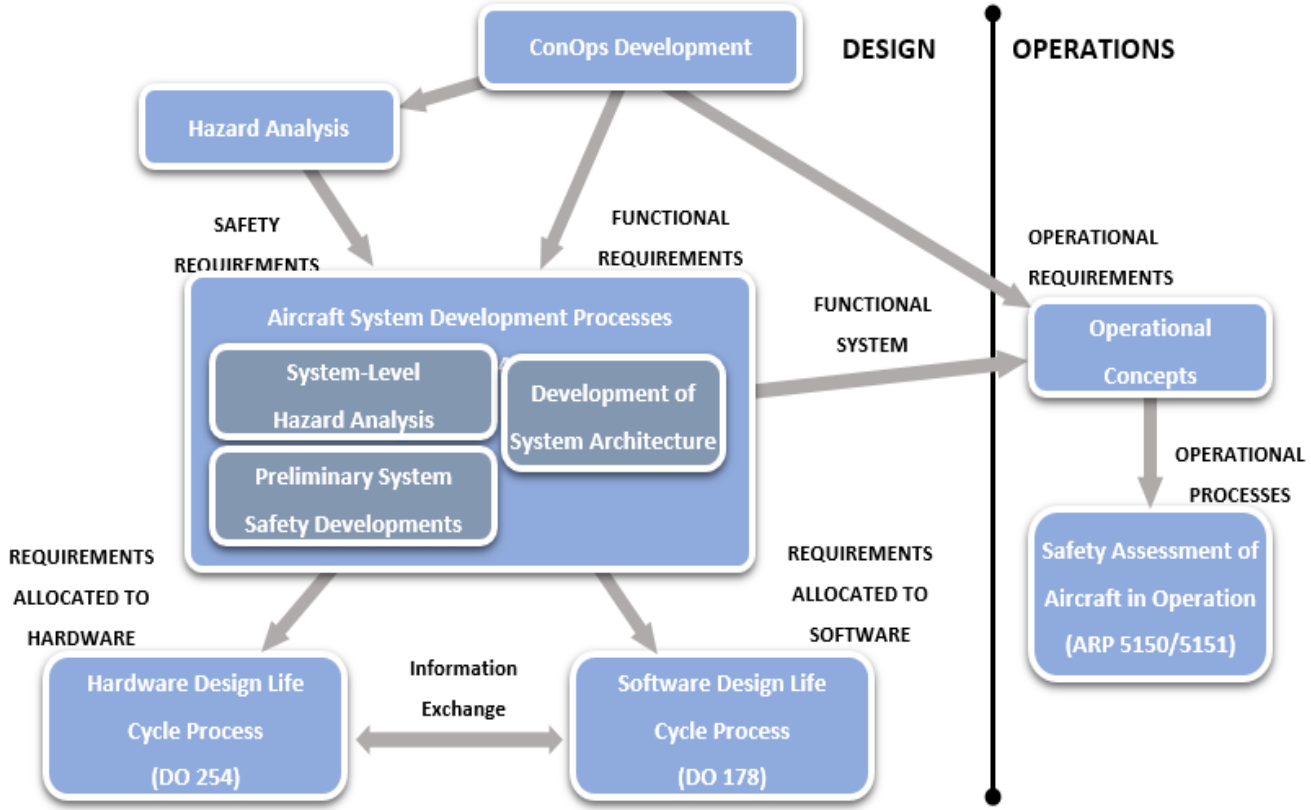
Reference SFCs

- SAFEGUARD
- Proximity to Threat Service, **Non-participant Casualty Risk Assessment**, ICAROUS, Safe2Ditch
- RF Interference Modeling
  GPS Degradation Modeling
  APNT Services (alternatives to GPS)
  Battery Health Prognostics
  Command and Control Link Monitor
- Hyper-local weather modeling → Climacell (SDSP example)
  Vehicle-as-a-sensor services
- Adaptive security procedure development
- Industry-developed Cyber-security solutions and protocols
- Multiple Kernel Anomaly Detection (MKAD)

SFC Assurance of Functionality

Assure Design

- Assurance requirements are specific to flight rules, operation complexity and risk criticality (SORA helps here)
- SFCs must be assured to an appropriate level via an acceptable process



Building Confidence

SFCs that

Manage Operational Risks:

Must mitigate risks with an acceptable level of certainty

SFCs that

Identify Unknown Risks:

Must correctly identify unknown anomalies and hazards in the system

SFCs that

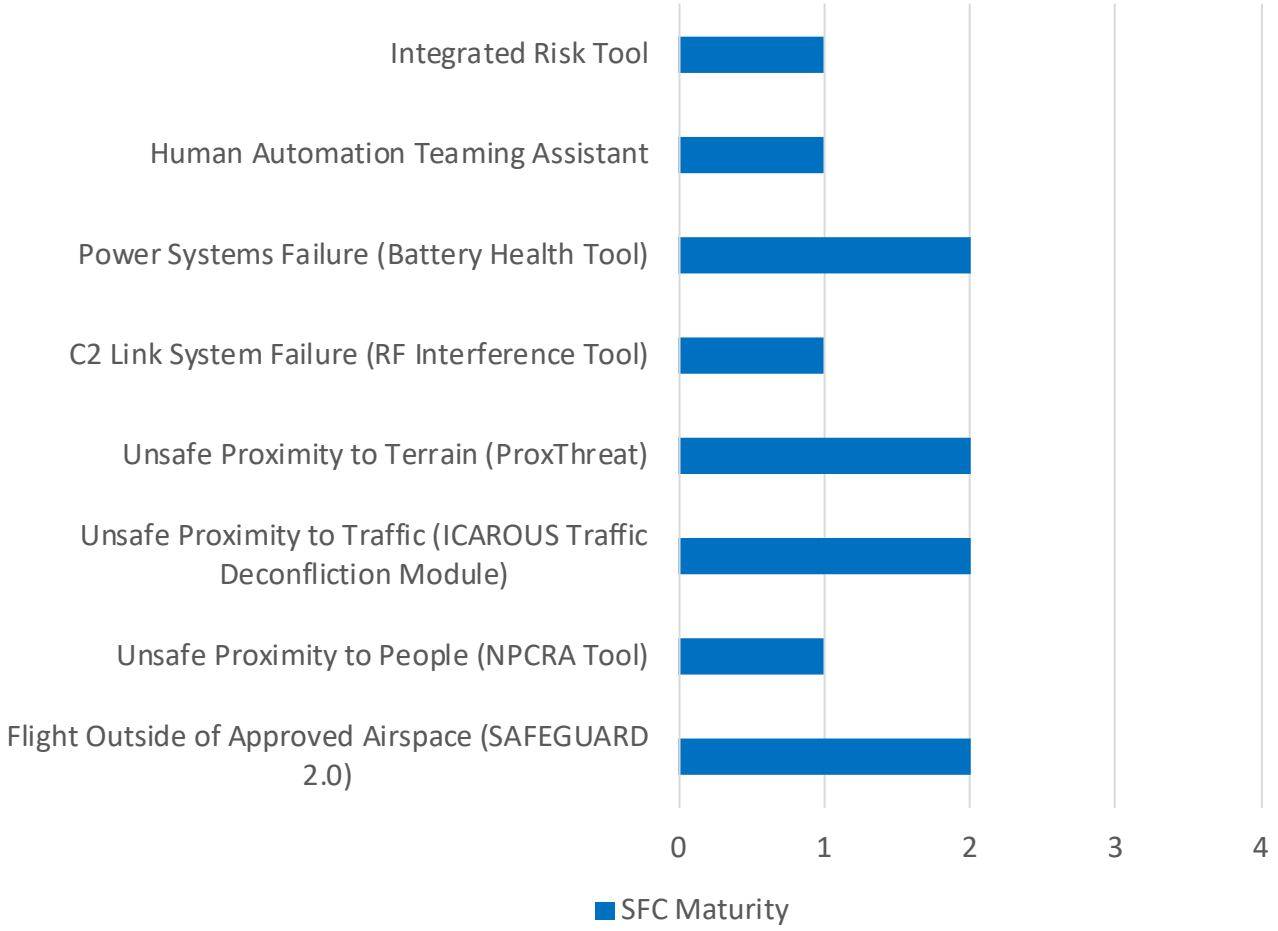
Inform System Designs:

Must correctly assess performance and deficiencies of the existing design

SD-1 Assured IASMS Components (SFCs)

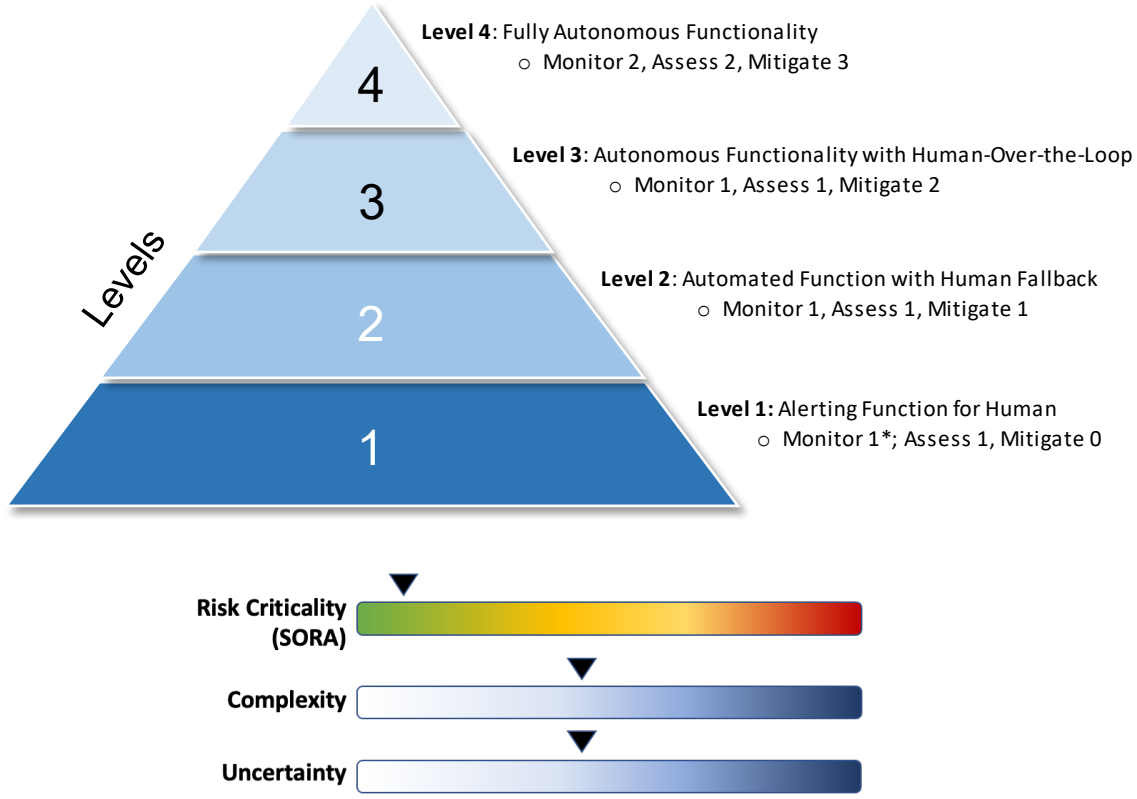
Wildfire Fighting - Key risks have been identified through significant stakeholder interaction. **The required maturity levels to enable safe operations are still being analyzed with our operational and regulatory partners.**

SFC Maturity Levels for Key Risks



SFC Maturity

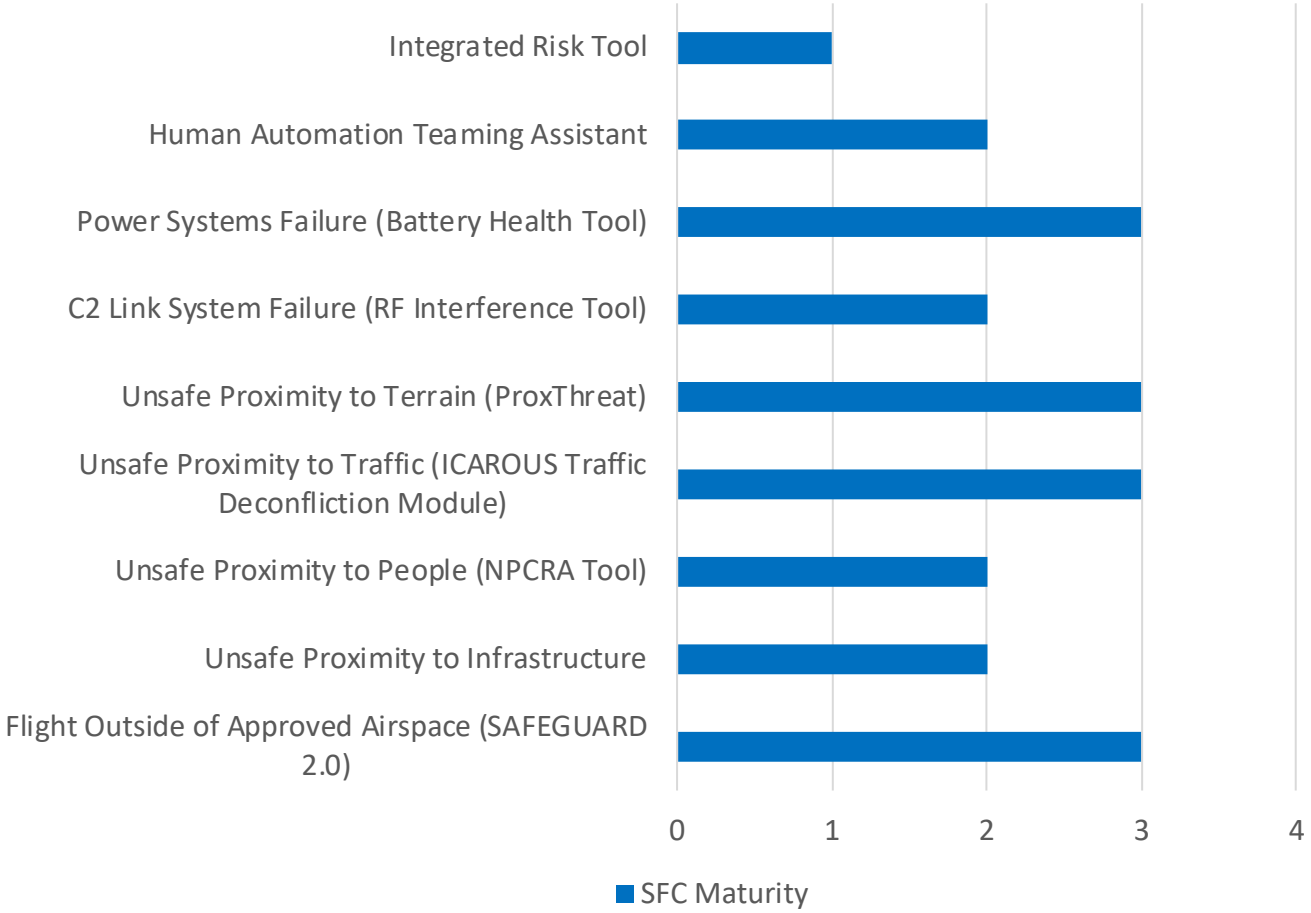
Services – Functions – Capabilities



SD-2 Assured IASMS Components (SFCs)

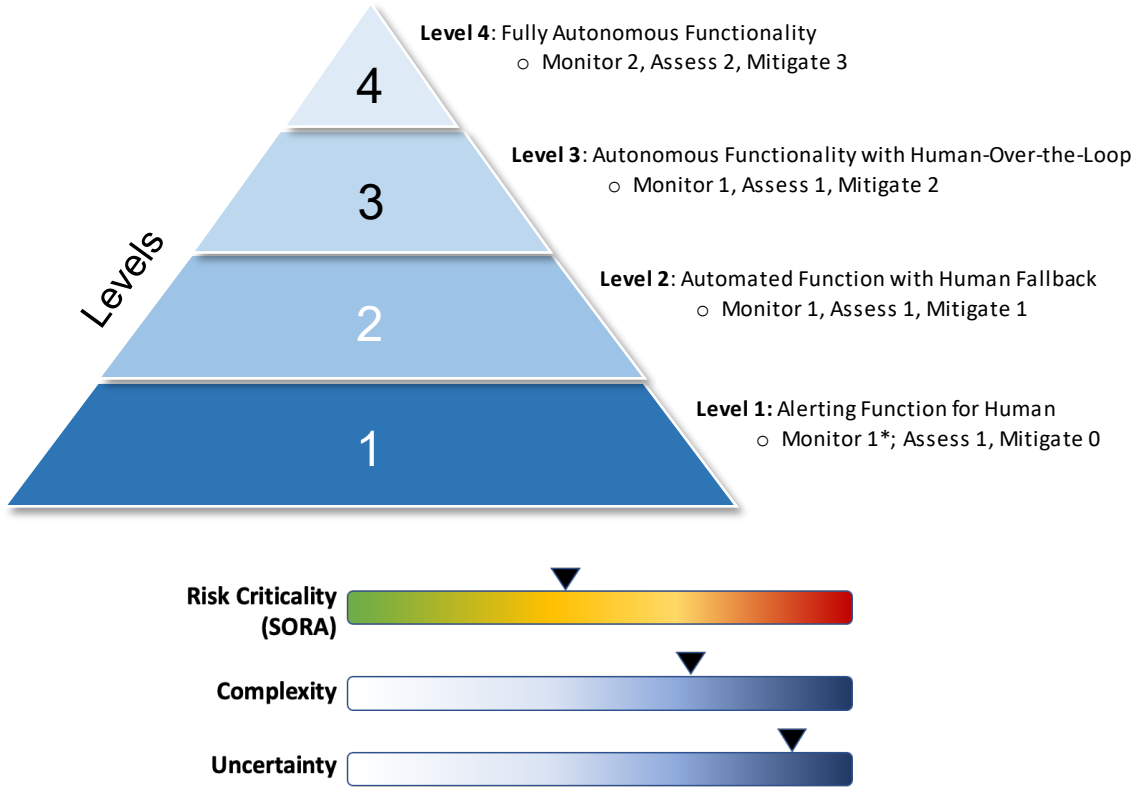
Post Hurricane Disaster Relief - Key risks have been identified through significant stakeholder interaction. **The required maturity levels to enable safe operations are still being analyzed with our operational and regulatory partners.**

SFC Maturity Levels for Key Risks



SFC Maturity

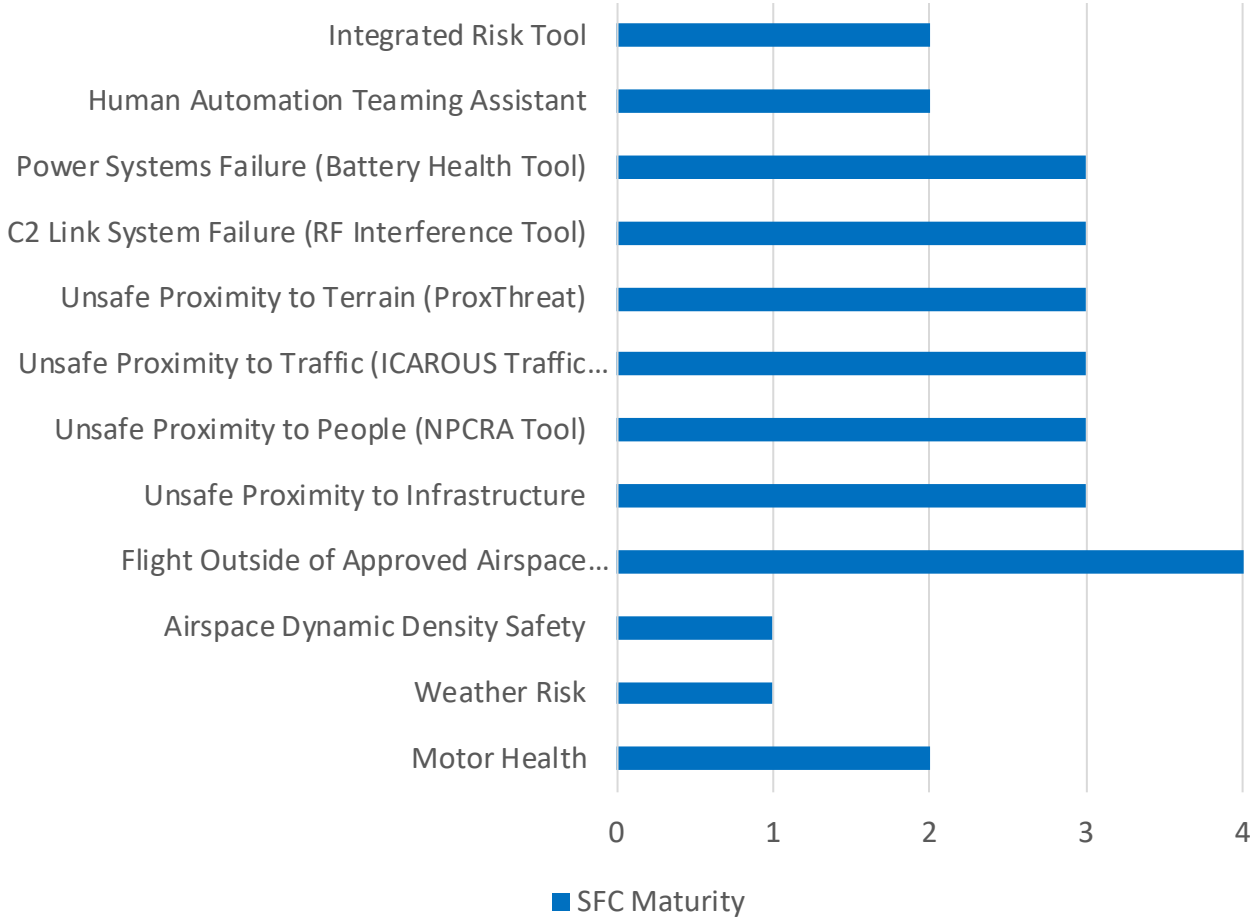
Services – Functions – Capabilities



SD-3 Assured IASMS Components (SFCs)

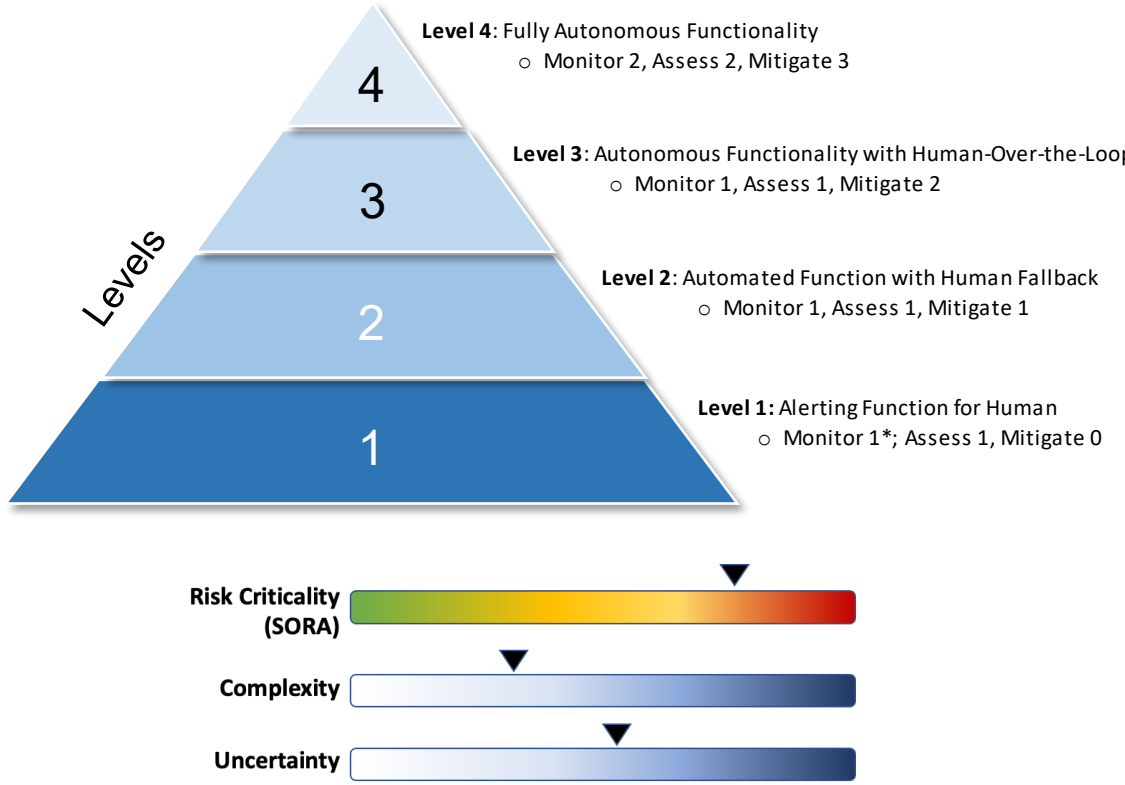
Medical Courier Delivery (URBAN) - Key risks have been identified through significant stakeholder interaction. **The required maturity levels to enable safe operations are still being analyzed with our operational and regulatory partners.**

SFC Maturity Levels for Key Risks



SFC Maturity

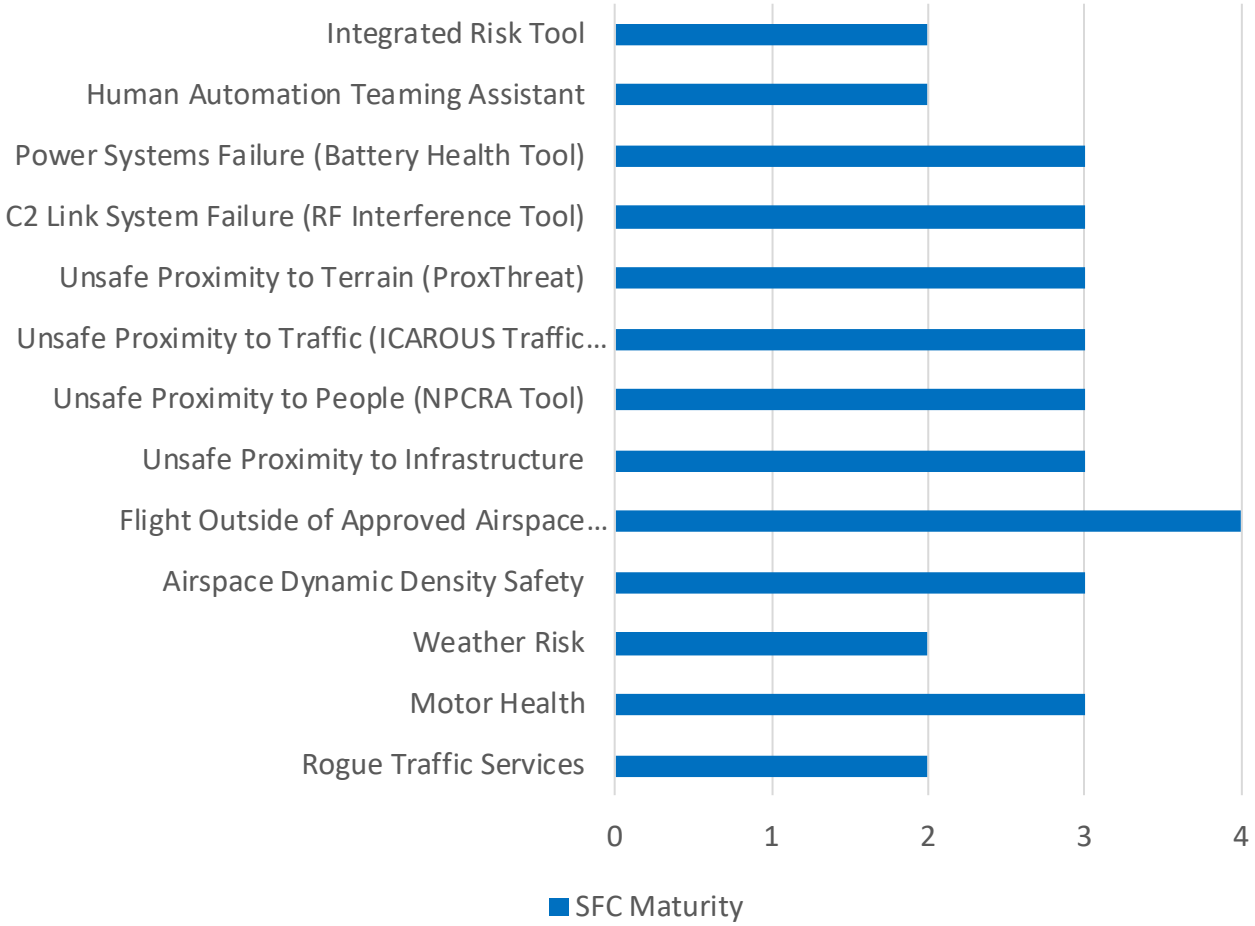
Services – Functions – Capabilities



SD-4 Assured IASMS Components (SFCs)

Un-evacuated Urban Area Disaster Response - Key risks have been identified through significant stakeholder interaction. **The required maturity levels to enable safe operations are still being analyzed with our operational and regulatory partners.**

SFC Maturity Levels for Key Risks



SFC Maturity

Services – Functions – Capabilities