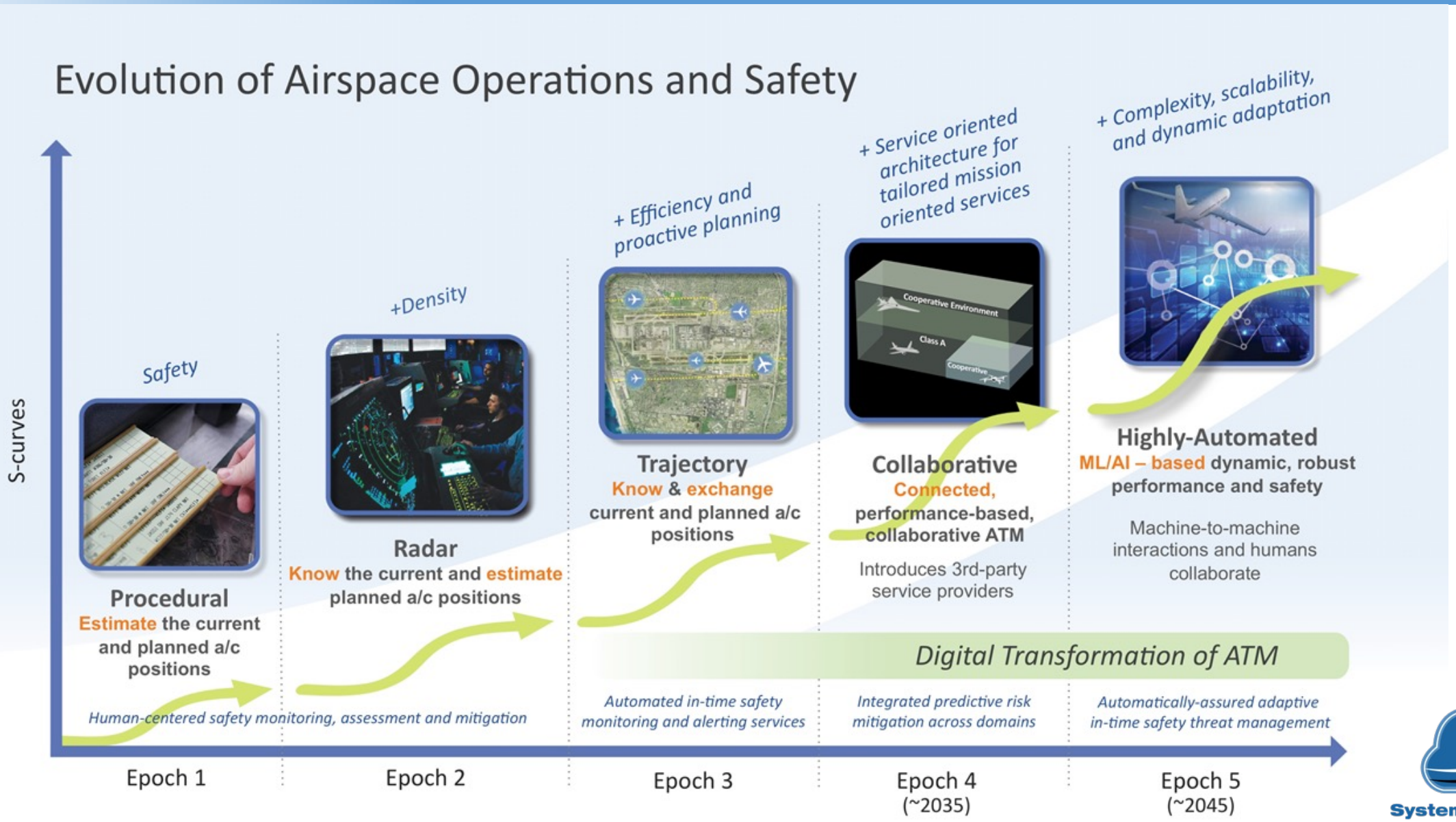
National Airspace Security Event Identification using the In-Time Aviation Safety Management System Technologies

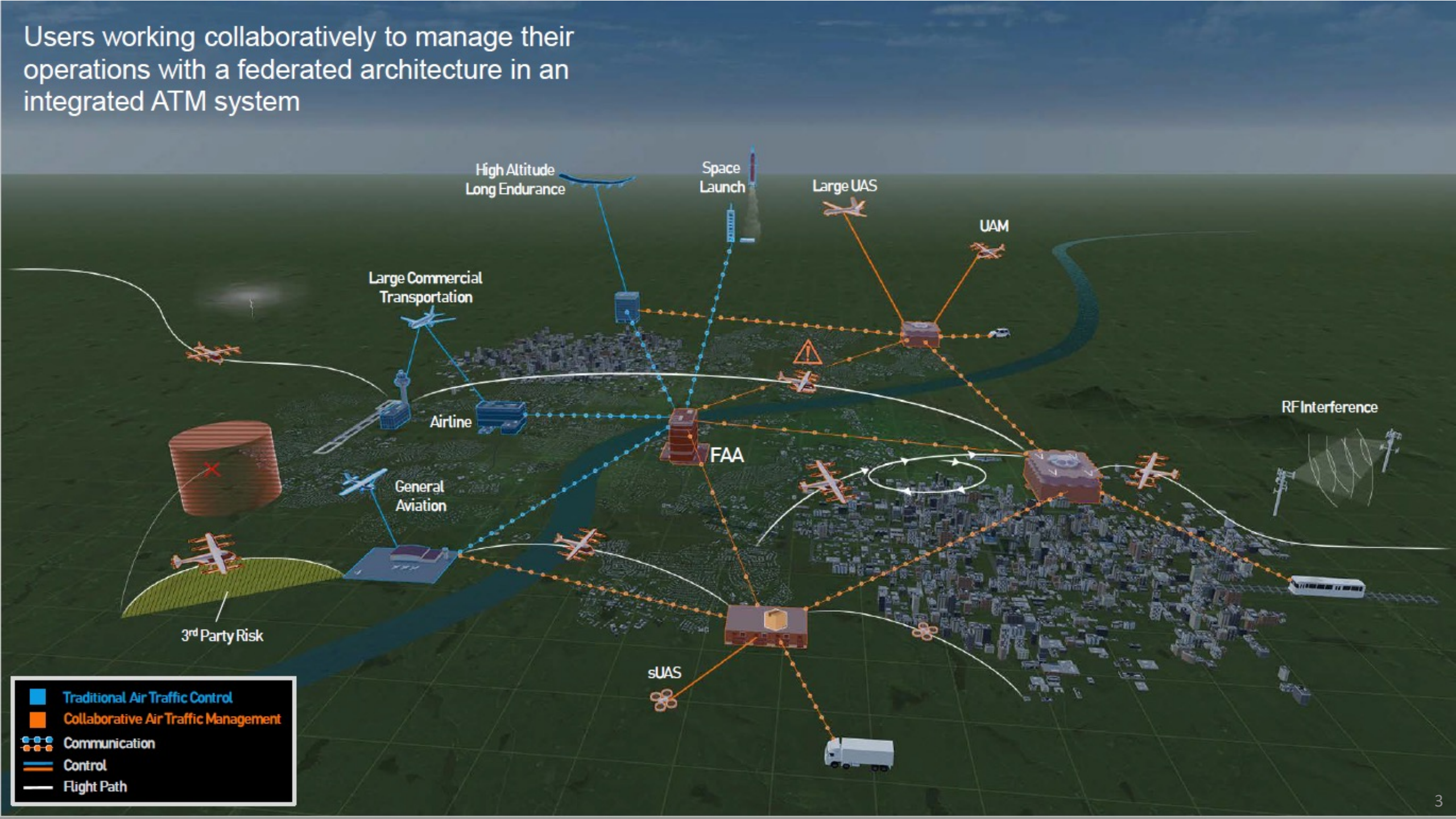
Paul Hoyt Nelson
Senior Cybersecurity Advisor
NASA Aeronautics Research

Evolution of Airspace Operations and Safety

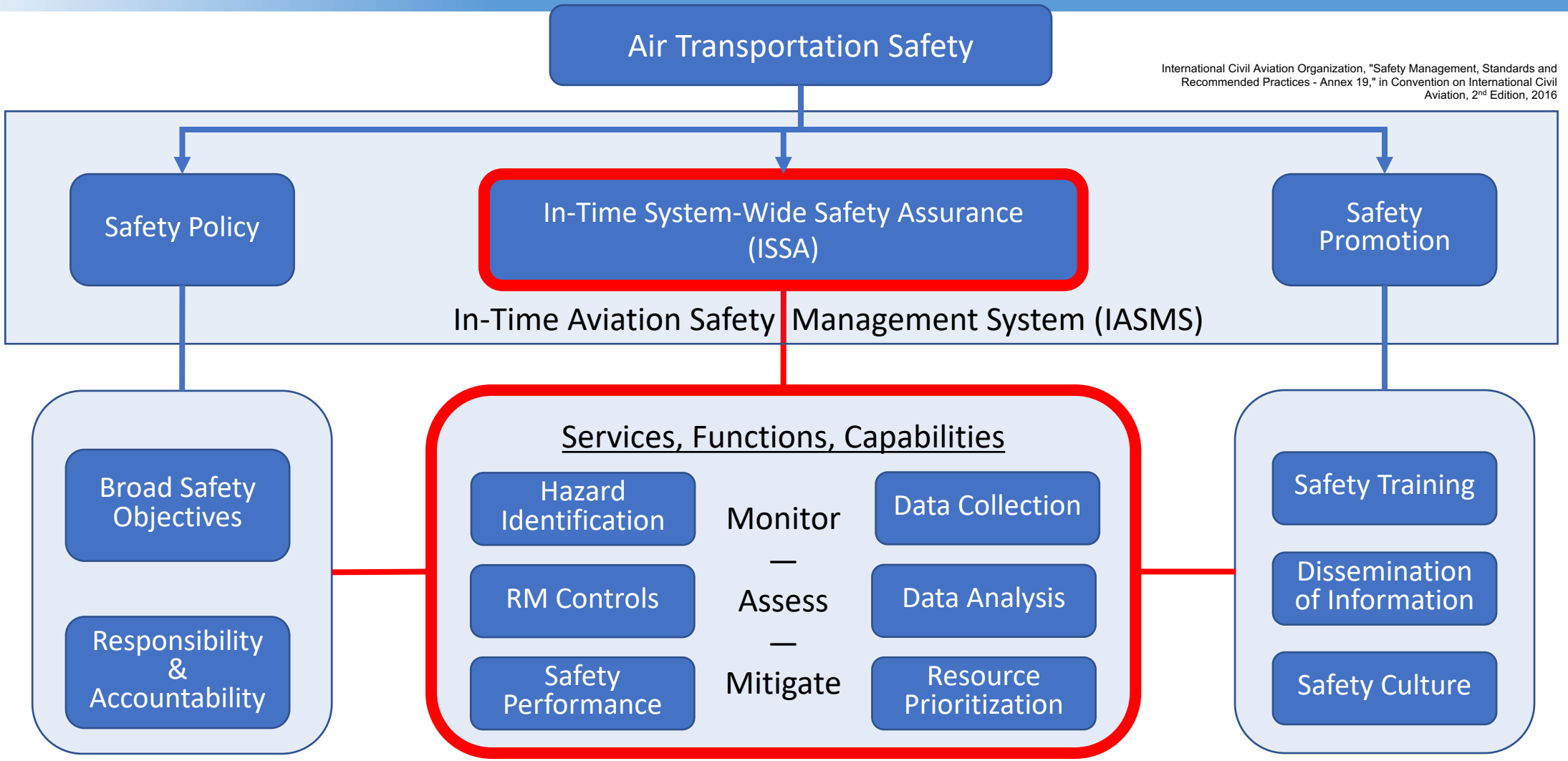


System-Wide Safety

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

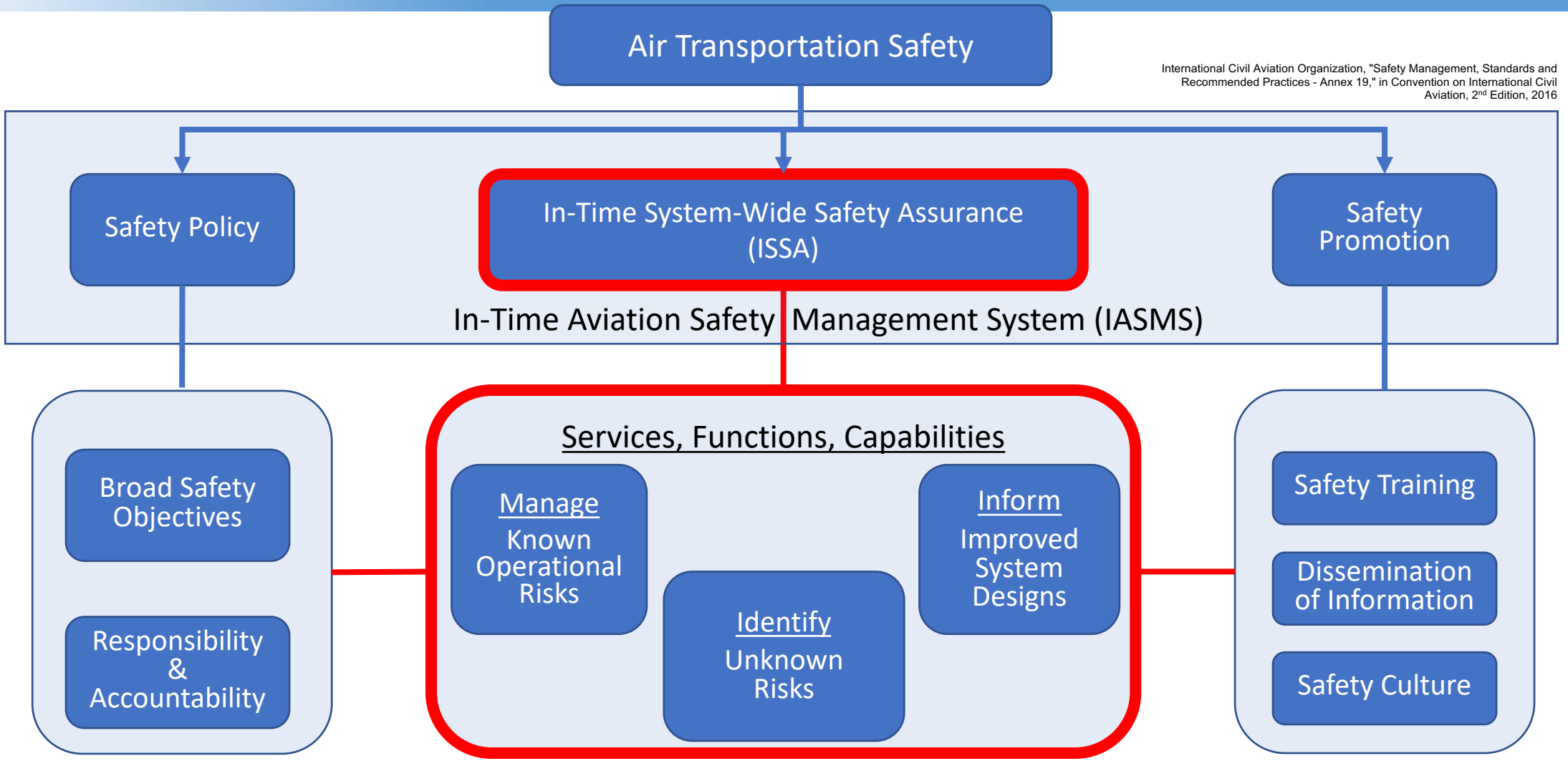


How We Achieve Aviation Safety Tomorrow



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

How We Achieve Aviation Safety Tomorrow

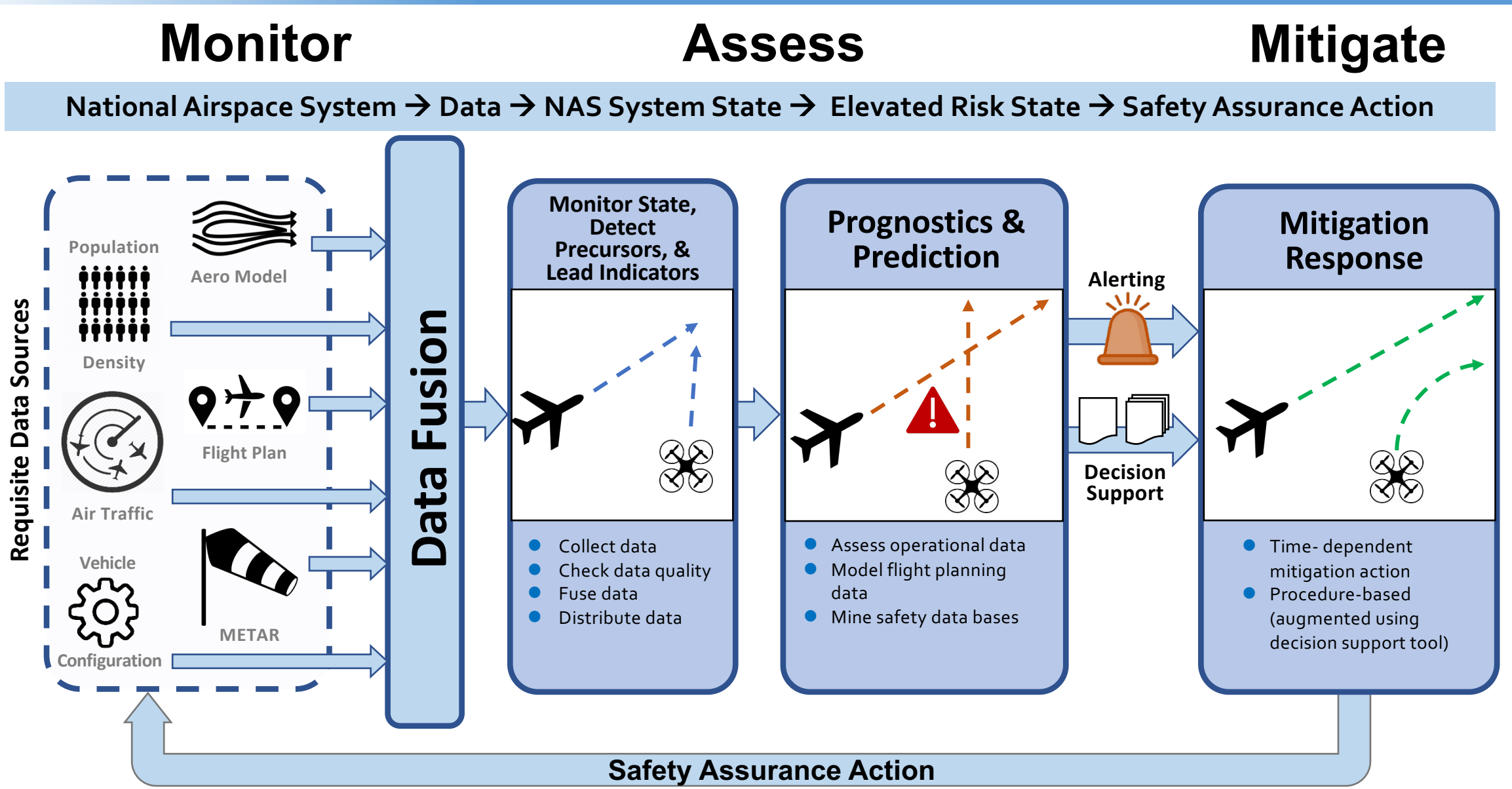


Quickly manage known operational risks at scale

Quickly identify unknown risks

Quickly inform design

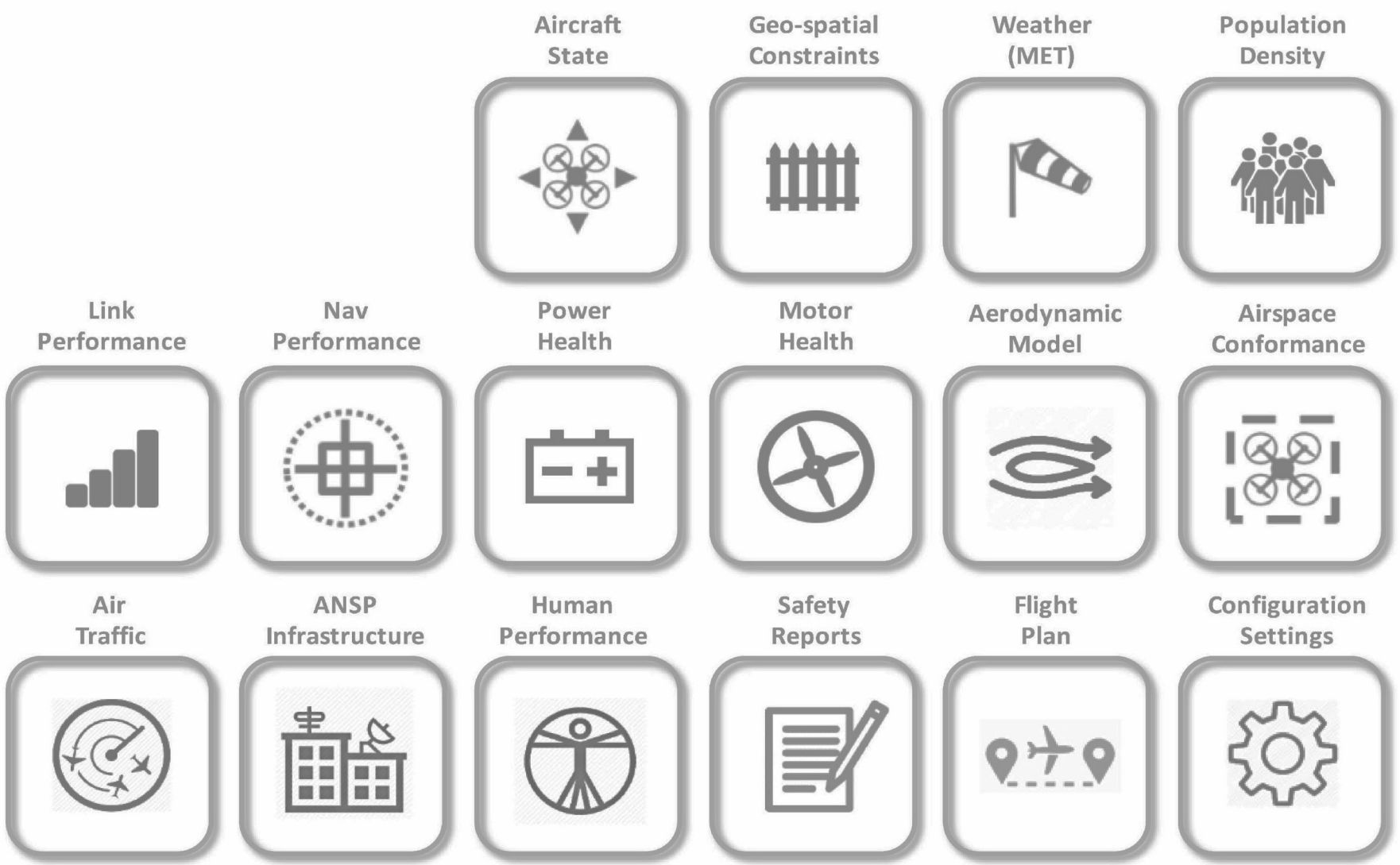
Services, Functions & Capabilities (SFCs)



It All Starts with Data…

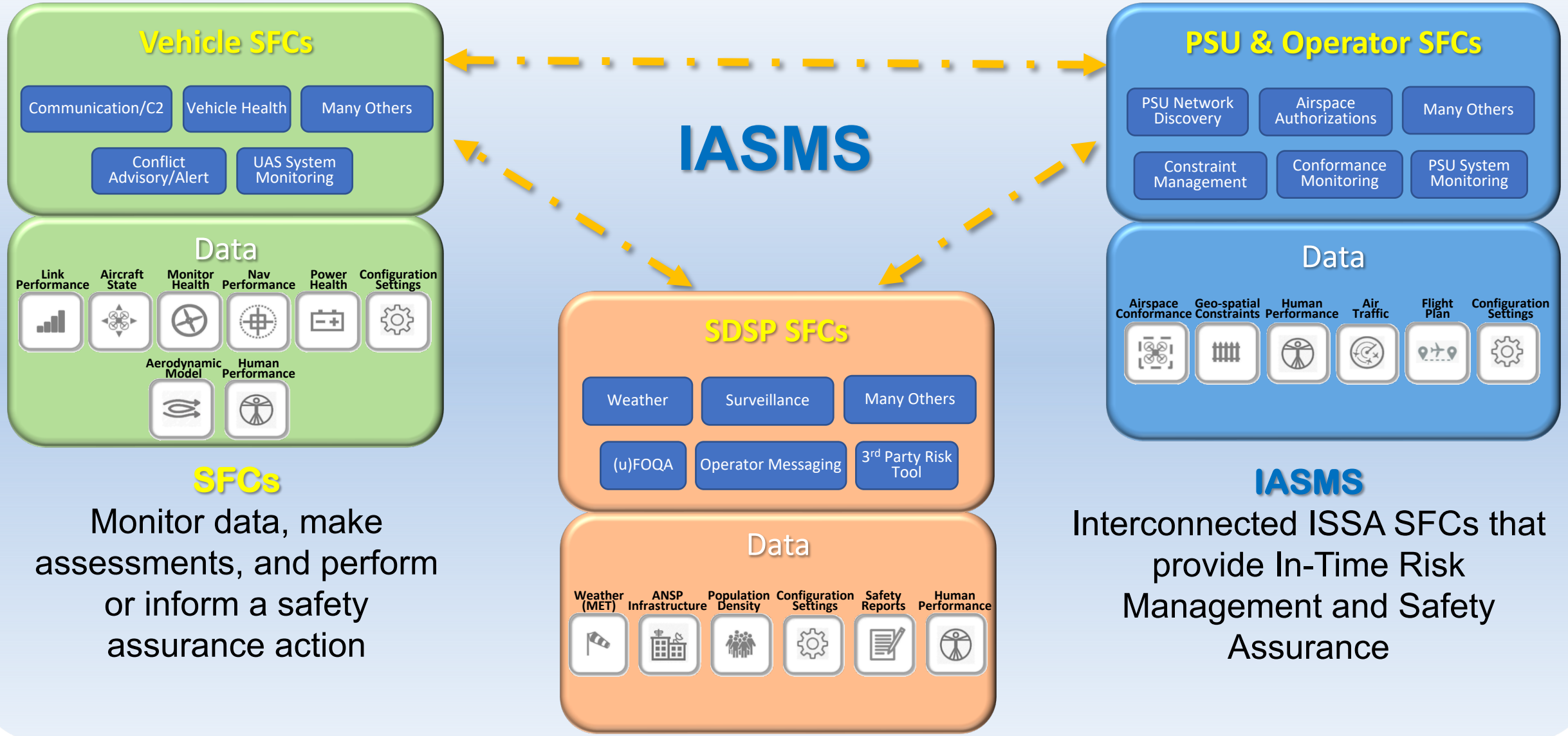
Information classes useful to enable IASMS SFCs

- 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

How Does IASMS Help With Cybersecurity

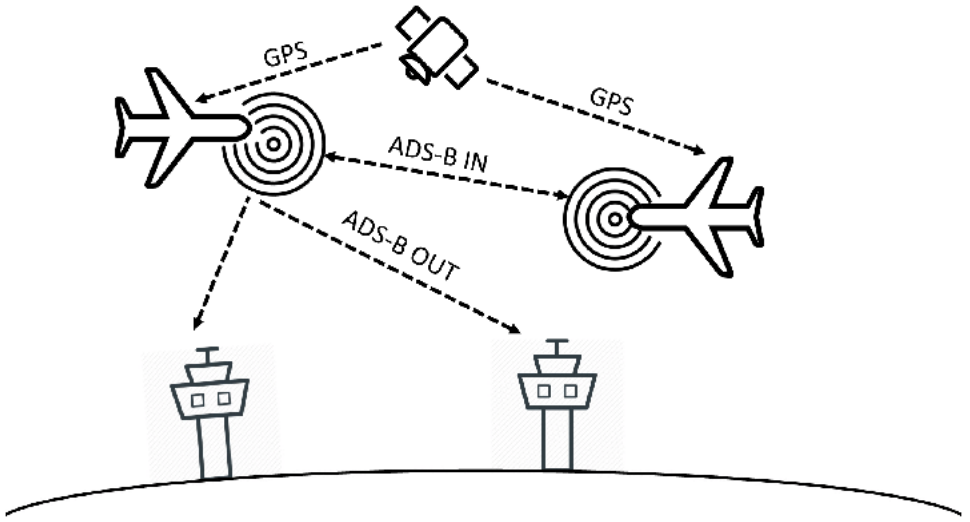
- This is not a typical business Information Technology (IT) environment. It is exchanging largely operational technology (OT) data and directing the operations of physical vehicles.
- The new IASMS system is focused on hazard detection and mitigation. Those hazards with cyber influences represent an opportunity for bad actors.
- The interrelationships between the various operations will be well understood and relatively predictable.
- Analysis of this data from a security perspective may allow identification of Indicators of Compromise (IoC) that would not be identifiable using normal IT security methodologies.
- This OT data largely describes the real world. This will behave according to our understanding of physics.

Research Question

Can in-time warning of cybersecurity incidents be predicted from ISSA data feeds?

Example ADS-B Out/GPS Attack

- ADS-B Out works by broadcasting information about an aircraft's GPS location, altitude, ground speed and other data to ground stations and other aircraft.
- It is built on the Global Positioning Satellite System (GPS) and GPS is known to be vulnerable to spoofing and jamming.
- Some forms of attack cause aircraft position to deviate many miles from the real position.
- Analyzing ADS-B data for an aircraft can determine vectors and speeds.
- This position data must follow physics.



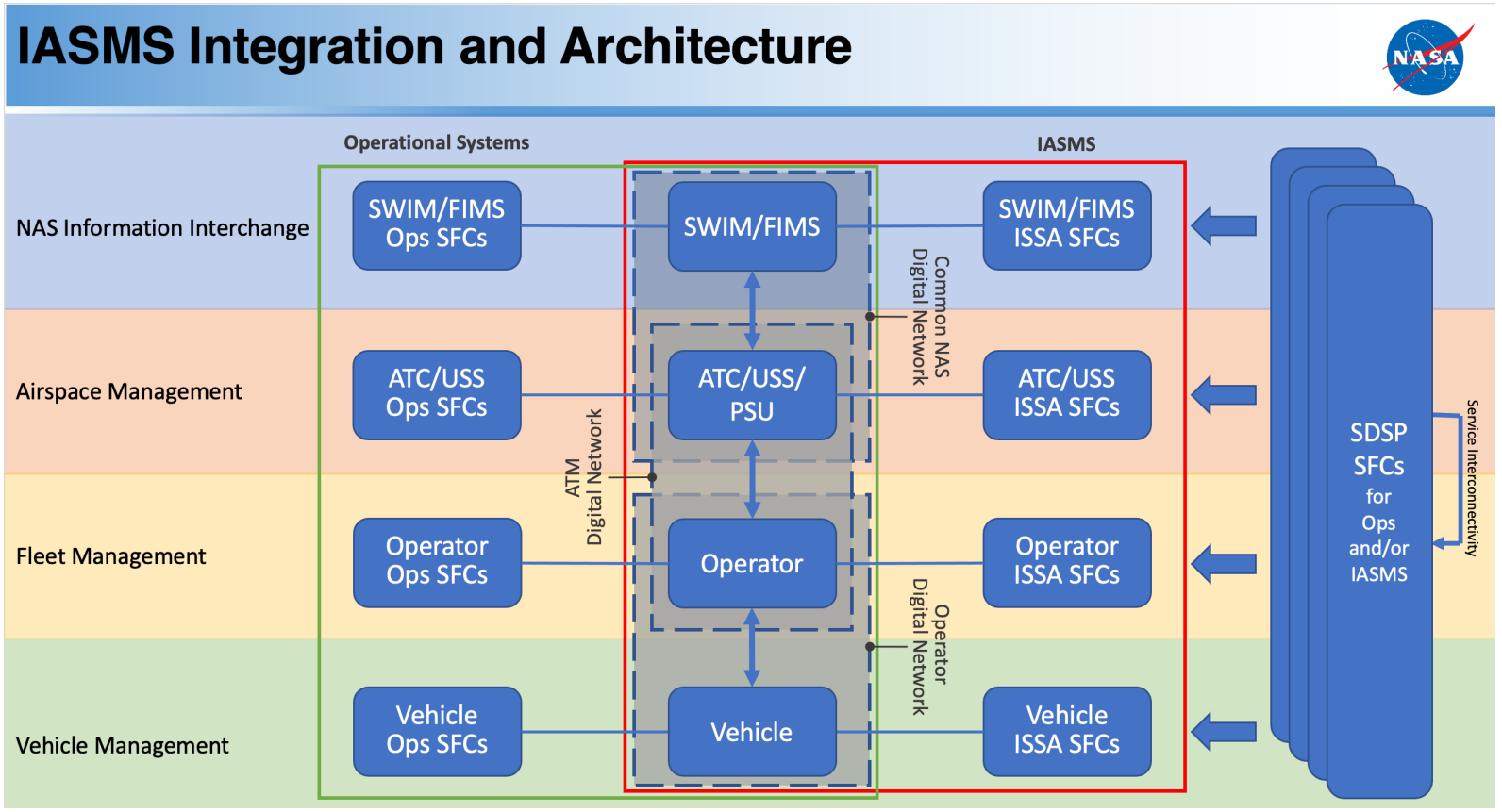
- The type of aircraft has an operational envelope. It has a maximum and minimum speed, climb rate and decent rate. Identifying vehicles that are exceeding their physical limits may identify compromise ($IoC^{vehicle}$).

Example Weather Data Attack

- Aviation weather data provides forecasts, analysis and observations at all altitudes, and while weather can change rapidly and violently, the causes are well knowns and relatively predictable.
- Vehicles and aircrews use this data to navigate in collaboration with air traffic control.
- Attacks on the data service could result in significant loss of efficiency in the National Airspace System (NAS) through delays, cancellations and other normal weather mitigation mechanisms.
- Identifying a data attack is possible using a fusion of different data:
  - Air crew observations
  - Vehicle performance data
  - Ground observations
  - Vehicle sensor data
- Fusing this data for a given sector of airspace should allow identification of a data attack (IoC^{data}).
- Conceptually, data fusion of this type could be used in many scenarios.

IASMS Analysis

- The IASMS will be doing its own safety analysis focused on the in-time mitigation of hazards
- Some hazards can have a cyber trigger component to them and offer attractive remote attacks on the NAS.
- Analysis of NAS hazards and mitigations for cyber triggers may identify attacks earlier than traditional IT security mechanisms (IoC^{system})



Identification of a cyber triggered hazard for one operation may be a leading indicator for a larger NAS attack!

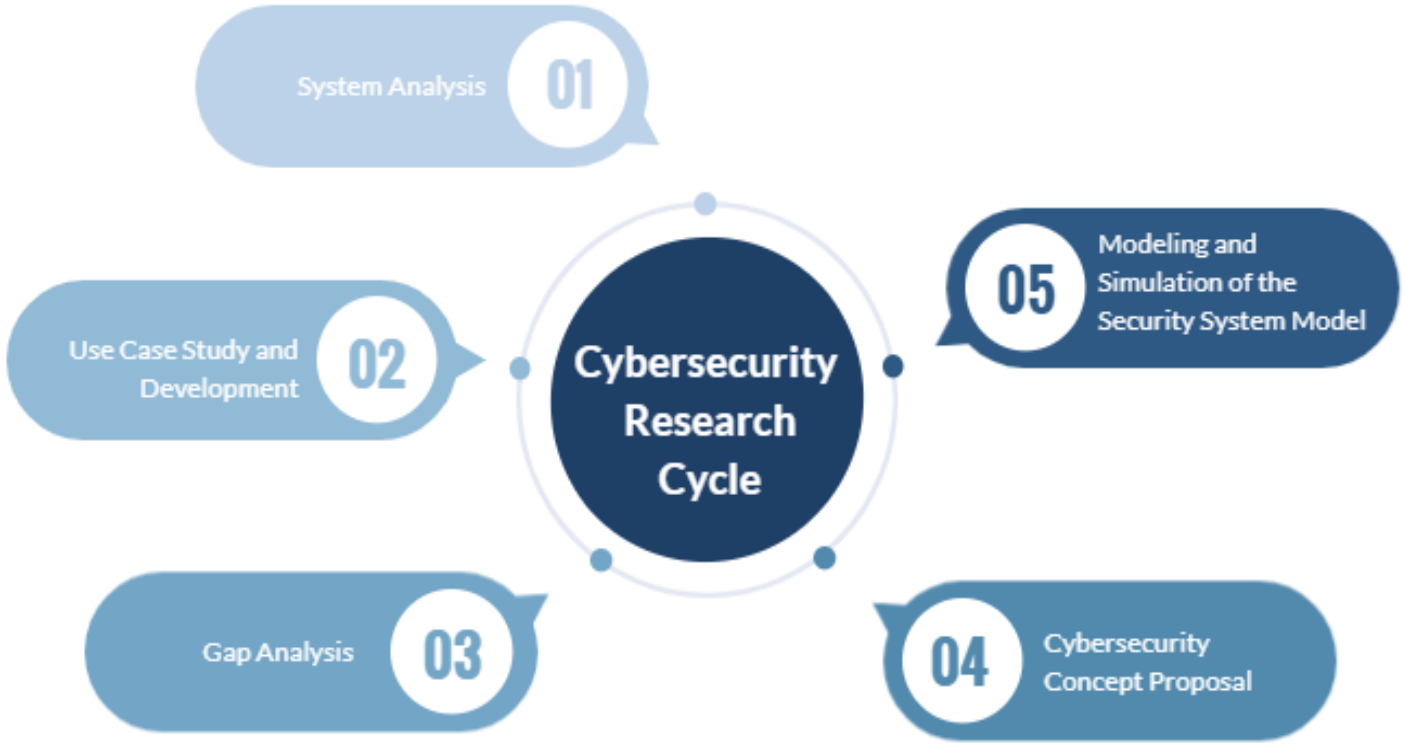
IASMS Security Analysis and Modeling

Motivation and Objective

- Can we predict evolving cybersecurity incidents time to mitigate safety impacts.
  - Develop a clear understanding of the security pc for the system.
  - Continue to expand the computational modeling capability for security concepts.
- Goal is to develop a security analog to IASMS.

Approach

- Applying an iterative approach to continuously integrate security analysis into the IASMS architecture.



Questions