



Secure Airspace and Urban Air Mobility

Secure Airspace and Urban Air Mobility



- o NASA and Aeronautics
- o Traditional National Airspace
- o Mobility Challenges
- o Urban Air Mobility
- o Threat Landscape
- o Cybersecurity Framework
 - Identify
 - Protect
 - Detect
 - Respond
 - Recover



Aviation is vital to our nation's economy



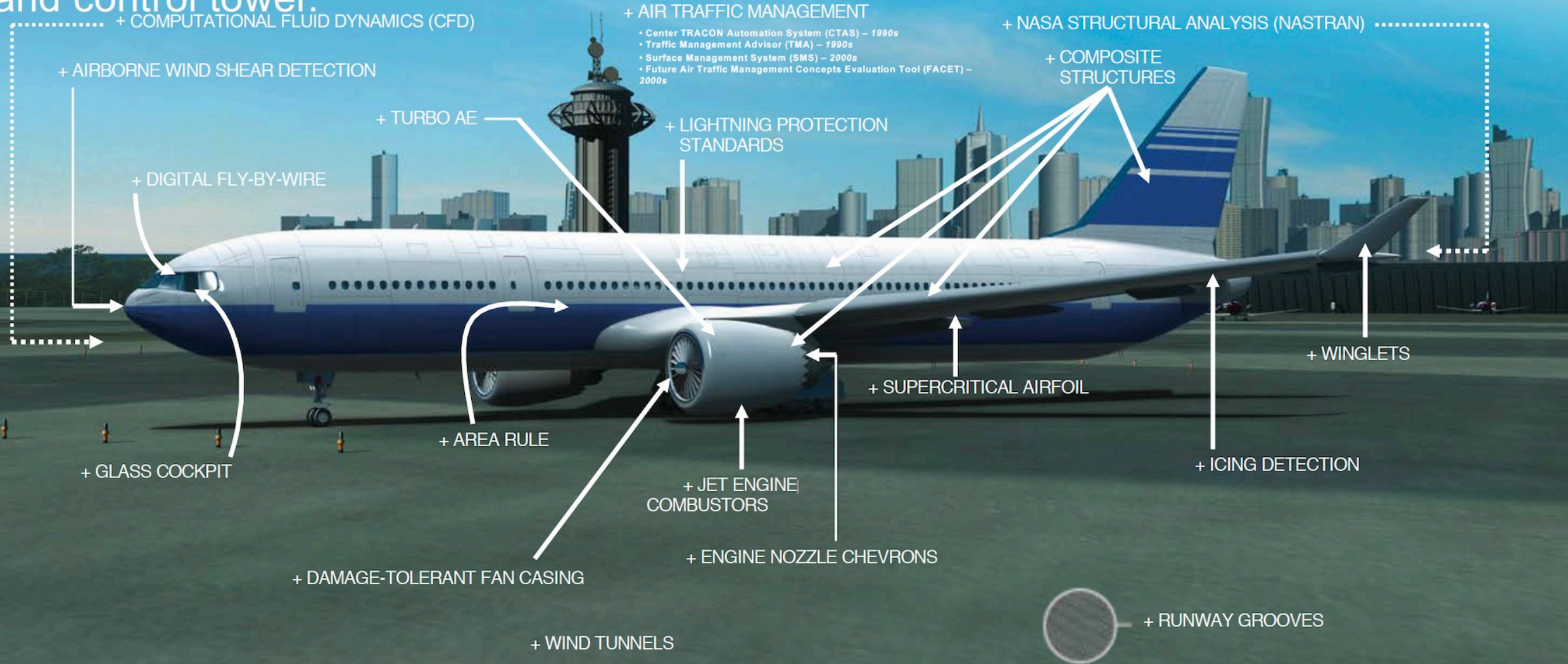
- \$82.5 billion positive trade balance
- \$1.6 trillion total U.S. economic activity
- 10.6 million direct/indirect jobs
- \$771 billion spent by air travelers in U.S. economy
- 18.1 million tons of freight transported by U.S. airlines

(Sources for statistics listed at <https://www.nasa.gov/aero/infographics.html>)



NASA has made decades of contributions to aviation

NASA-developed technology is on board every U.S. commercial aircraft and control tower.





QUIET SUPERSONIC FLIGHT



AIR TRAFFIC



ELECTRIC PROPULSION

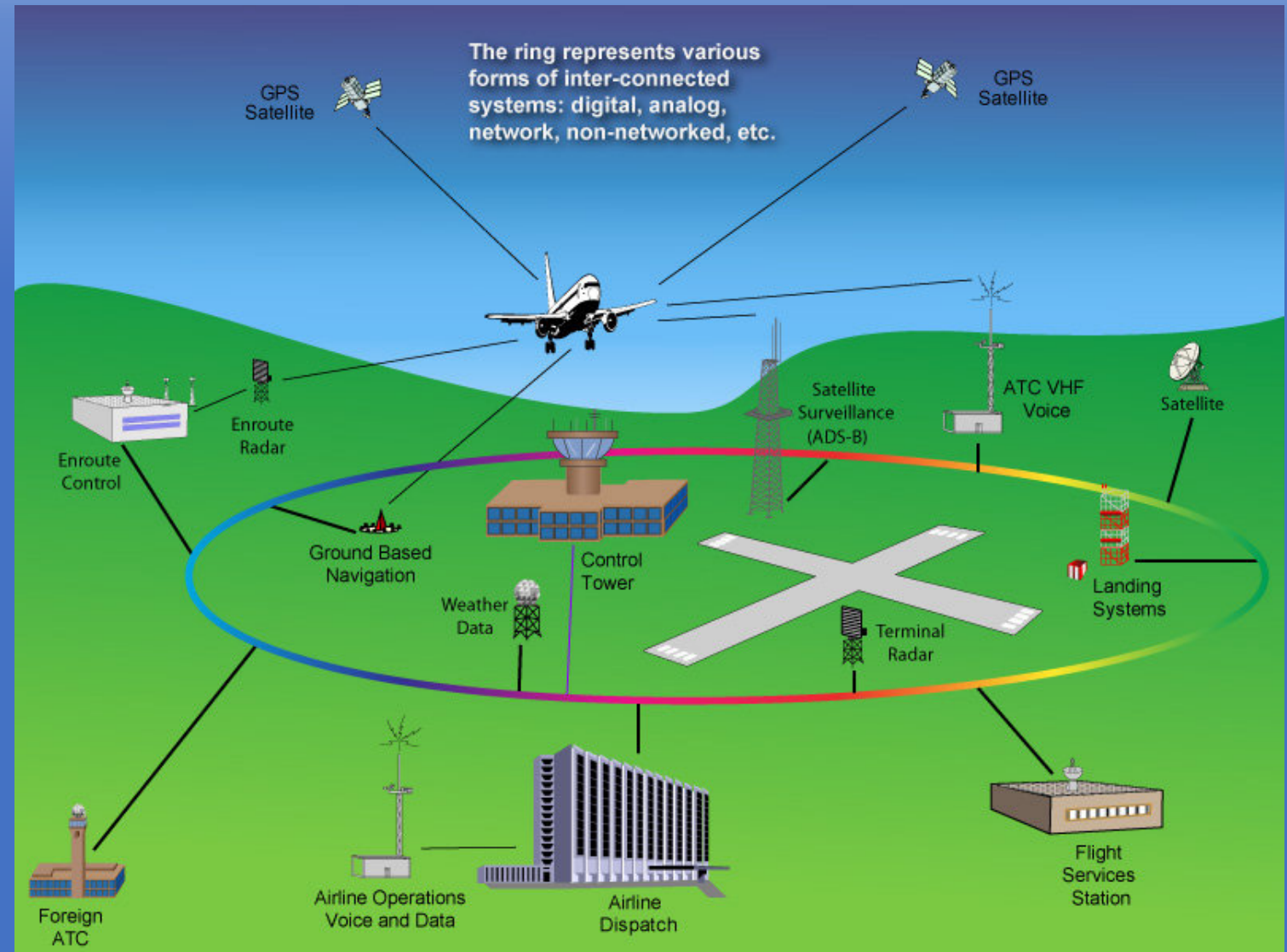


URBAN AIR MOBILITY

Traditional National Airspace



The National Airspace System (NAS) is the airspace, navigation facilities and airports of the United States along with their associated information, services, rules, regulations, policies, procedures, personnel and equipment



https://www.researchgate.net/figure/Major-Components-of-US-FAAs-National-Airspace-System-NAS-Source-Williams-and-Signore_fig1_274123014

Traditional National Airspace

Air Traffic Control (ATC)



Air Traffic Control System Command Center (ATCSCC)

The ATCSCC balances air traffic demand with system capacity in the National Airspace System (NAS)

The Command Center, as it is commonly known, is committed to managing the NAS in a safe, efficient, and cohesive manner

Air Route Traffic Control Centers (ARTCC)

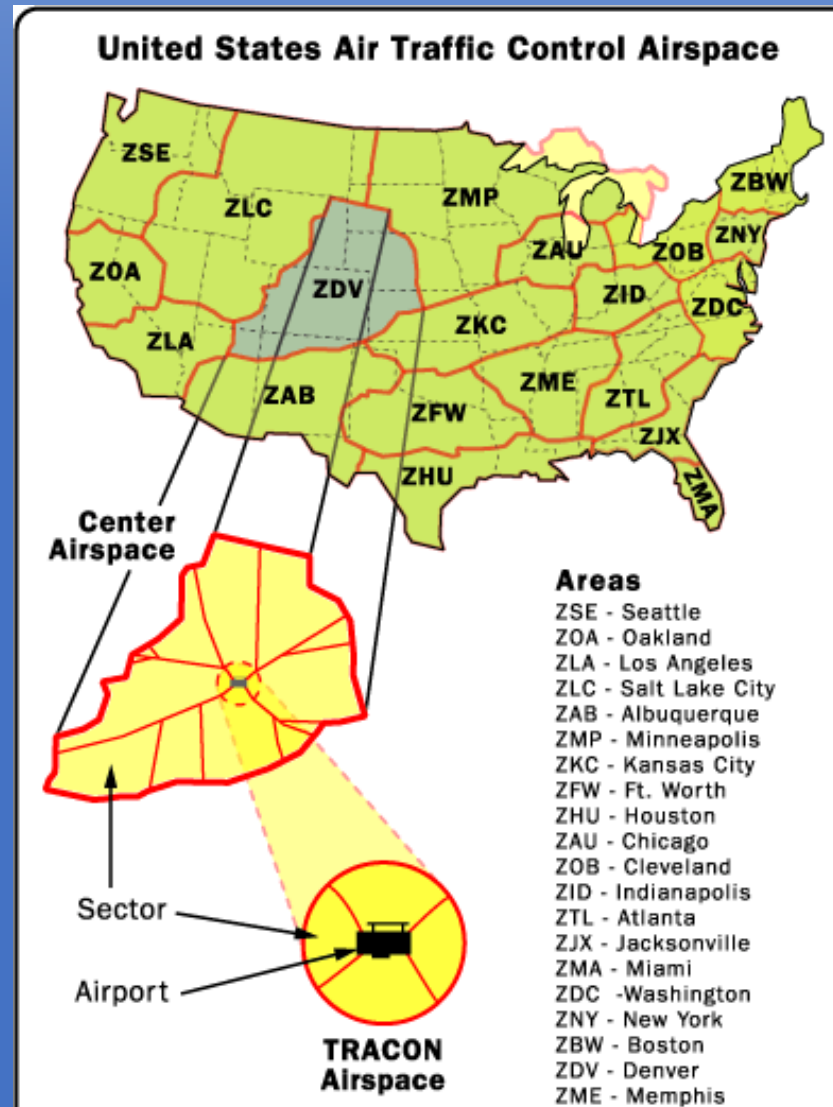
One per zone managing all air traffic except for TRACON and local airport airspace

Terminal Radar Approach Control (TRACON)

Controls departing and approaching aircraft within its airspace

Air Traffic Control Tower (ATCT)

Controls all takeoff, landing, and ground traffic from a specific airport



The United States airspace is divided into 21 zones (centers), and each zone is divided into sectors

The shape and size of zones is determined by the volume of air traffic

Sectors and TRACON (Terminal Radar Approach Control)

Within each zone are portions of airspace, about 50 miles in diameter, called TRACON airspaces

Within each TRACON airspace are a number of airports, each of which has its own airspace within a 5 mile (8-km) radius

Traditional National Airspace Airspace Classification



Controlled Airspace is a generic term that covers the different classifications of airspace and defines the dimensions within which the air traffic control (ATC) service is provided in accordance with the airspace classification.

Controlled airspace consists of: Class A, Class B, Class C, Class D, Class E



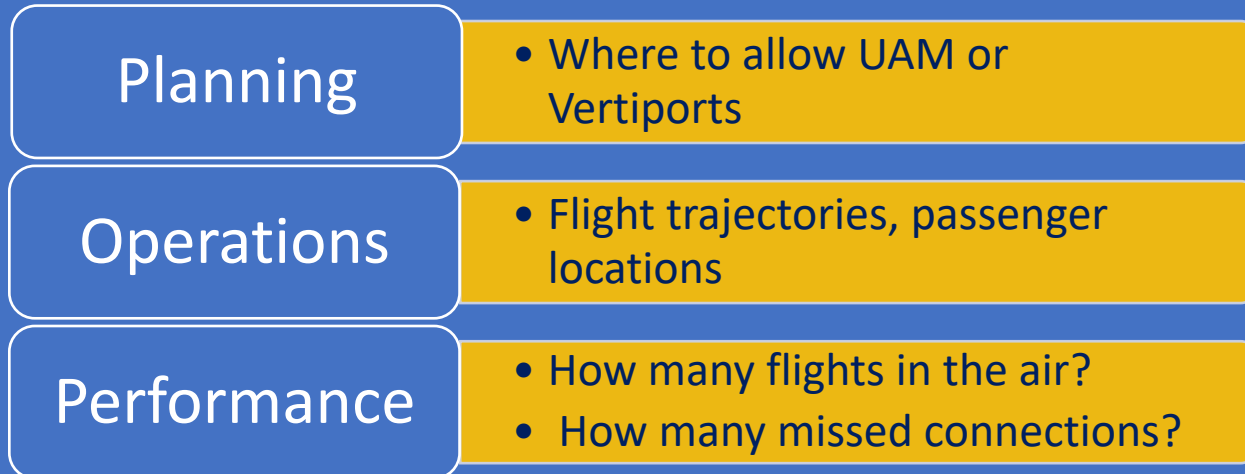
AGL – Above Ground Level
FL – Flight Level
MSL – Mean Sea Level

Mobility Challenges



- Transportation shapes society, enabling economic and social interactions
- The quality of life is impacted by ever growing commute time.
- Transportation is increasingly driven by door-to-door challenges.
- Air Mobility can convert our 2D mobility system to a 3D mobility system, increasing mobility options for both people and goods.

Air Mobility Challenges



Multiple technology areas (e.g. autonomy & cybersecurity) will need to be explored to address the planning, operations and performance requirements of the Urban Air Mobility (UAM) environment

Air Mobility Challenges



FAA has completed a cybersecurity strategic plan However, FAA has not completed a comprehensive and strategic cybersecurity framework.

DoT OIG 2019

Recent designs for aircraft systems have included connectivity to “non-governmental services” such as the internet, portable electronic devices, and commercial-off-the-shelf technologies that have not been certified and accredited for secure operations by a government authority.

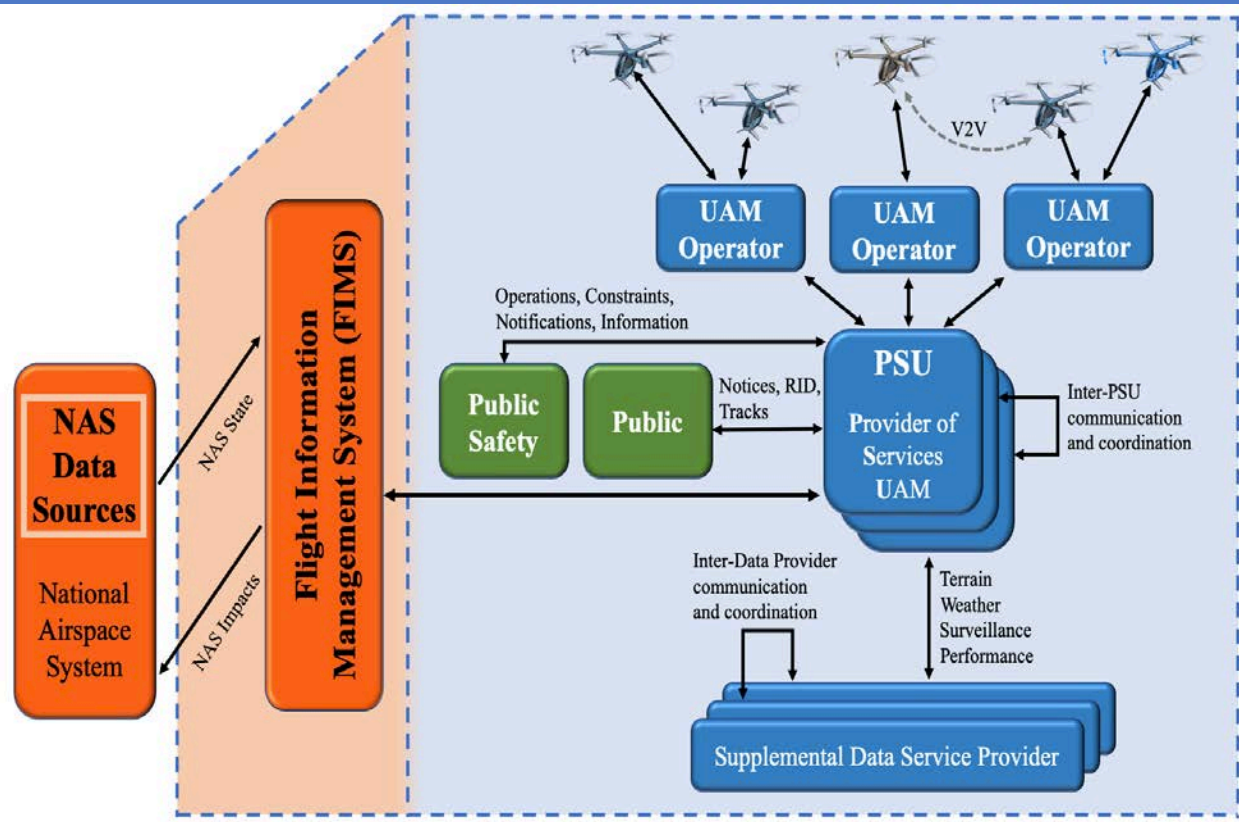
U.S. DoT FAA Policy Statement 2014

“The cyber world of interconnected and interdependent systems has increased the vulnerability of aircraft and systems”

Cyber Security in Civil Aviation August 2012

In order to ensure mission safety and success, cybersecurity will need to be embedded into the UAM operations

Urban Air Mobility (UAM) will leverage a service-based architecture operational services



UAM Environment :

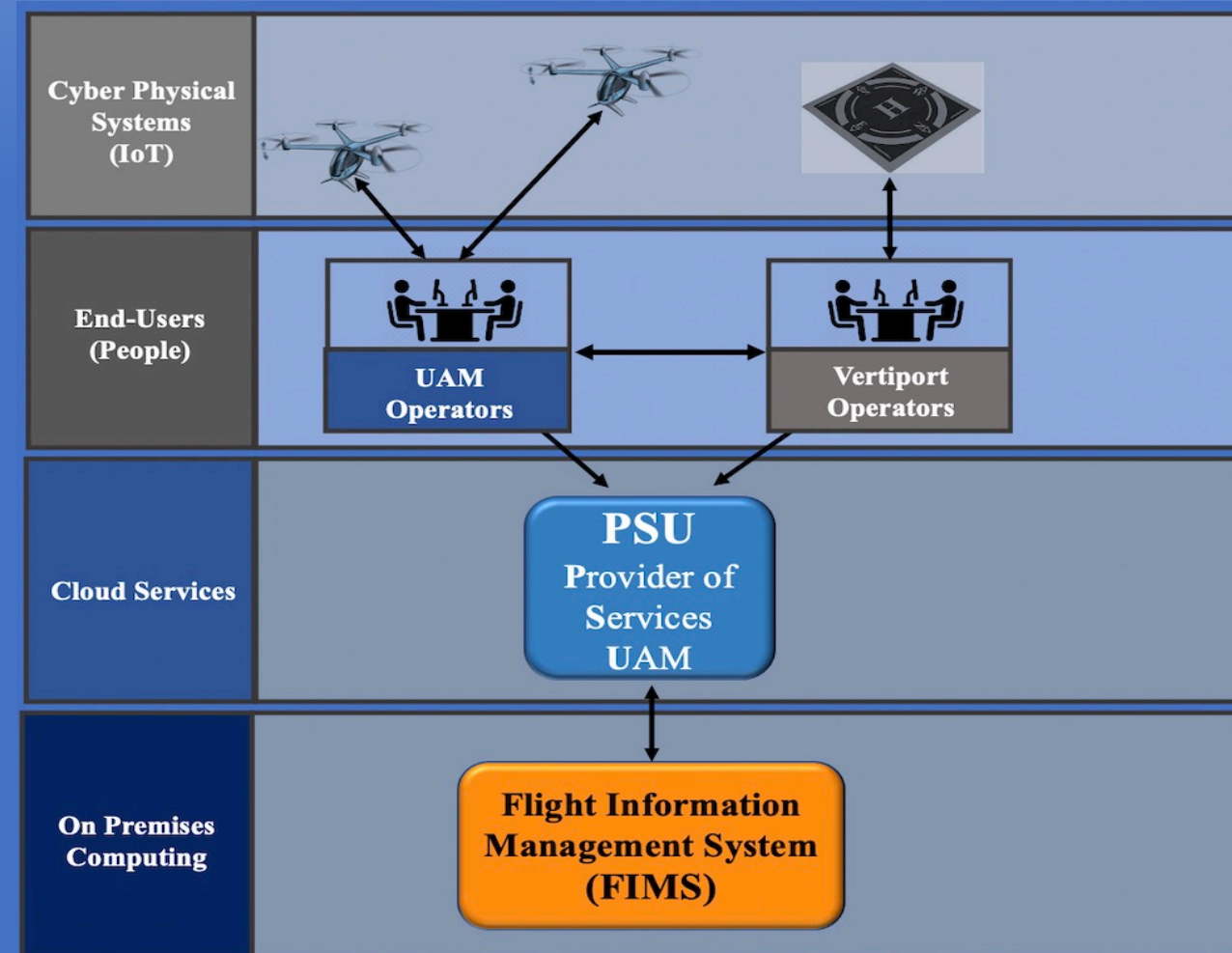
- Independent UAM operators leveraging diverse communications
- Independent service providers (PSU)
- Secure IoT, local computing and cloud environments
- Interactions between multiple operators and service providers

Threat Landscape

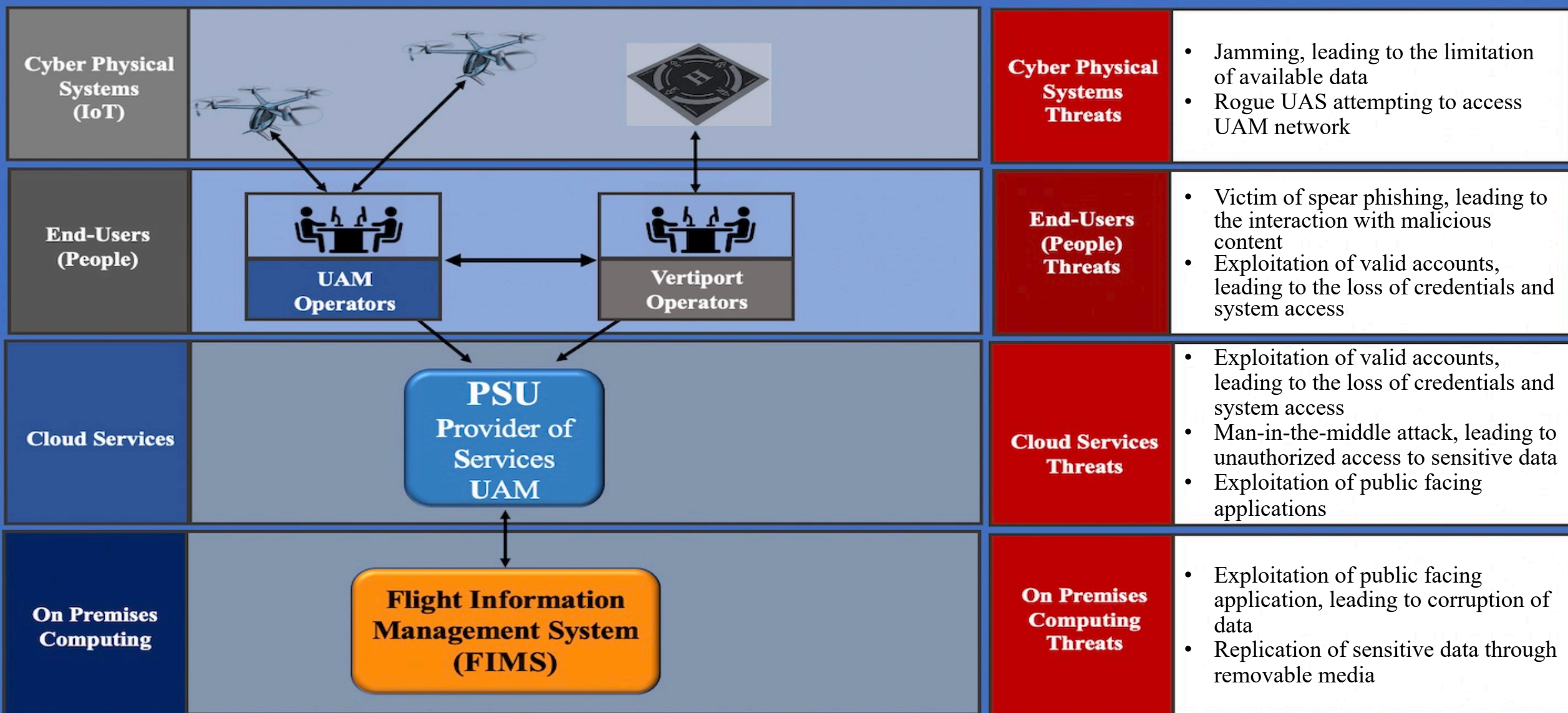


Cyber and physical threats to the service-based UAM architecture

- Cyber Physical Systems
 - UAS vehicles, vertiports and the associated data processing components
- End Users
 - Operators of UAS, public safety entities, the public and vertiports operators, their associated systems and data communications
- Cloud Services
 - Providers of UAM services leveraging cloud services for compute and storage
- On Premises Computing
 - Legacy on-premises computing integration into the future service-based UAM architecture



Threats Landscape



Cybersecurity Framework (Core Functions)



Identify

- Identify the risks associated with operating the systems, assets, data and capabilities

Protect

- Provide the appropriate safeguards to ensure delivery of critical services

Detect

- Identify the occurrence of a cybersecurity or disruptive event within ecosystem

Respond

- Determine the activities to take regarding a detected cybersecurity or physical event within an ecosystem

Recover

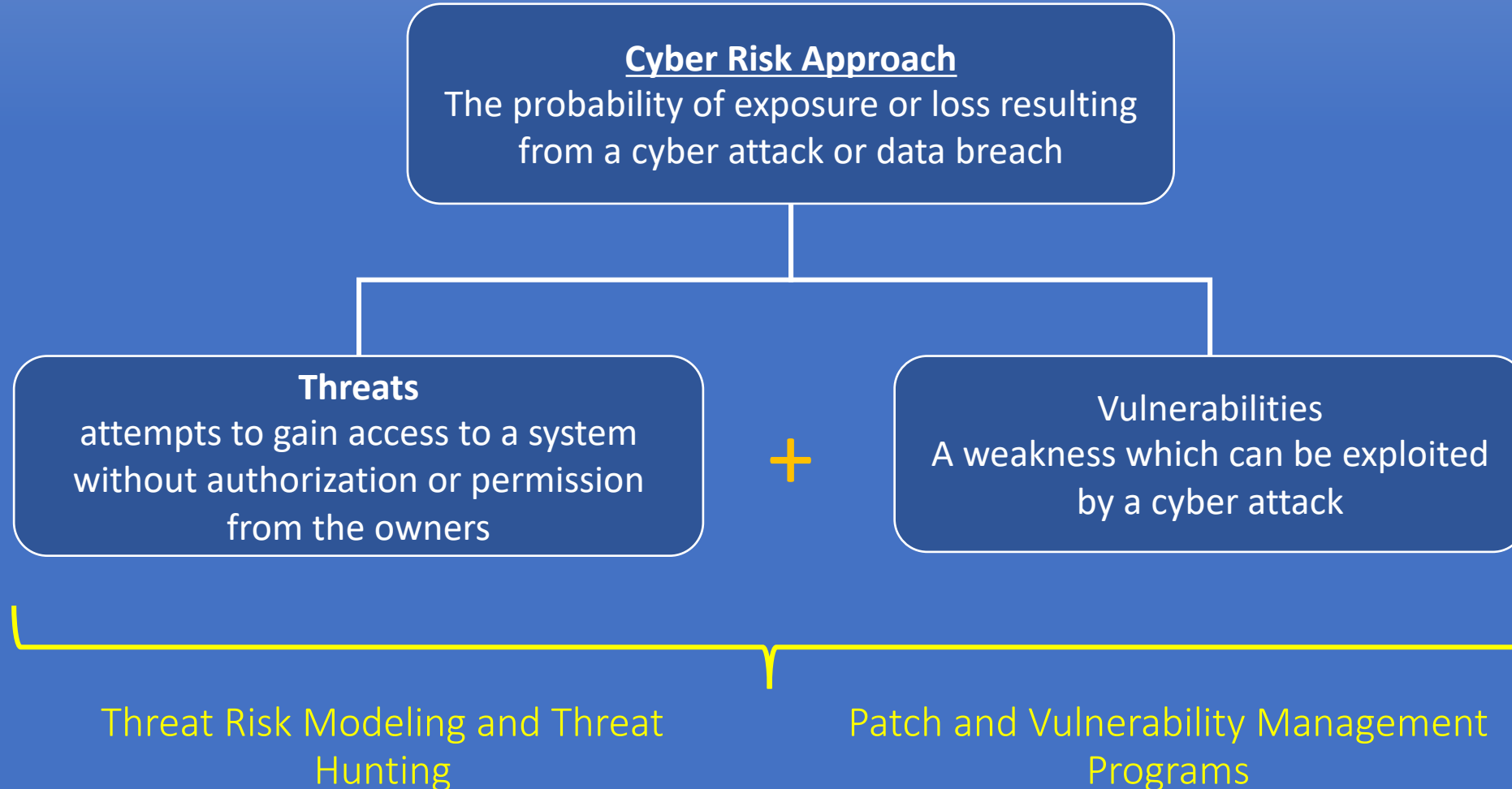
- Develop and implement the appropriate activities to maintain plans for resilience

The Cybersecurity Framework was developed by the National Institute of Standards (NIST)

Identify: Cyber Attack Risk



Identify the occurrence of a cybersecurity or disruptive event within UAM ecosystem

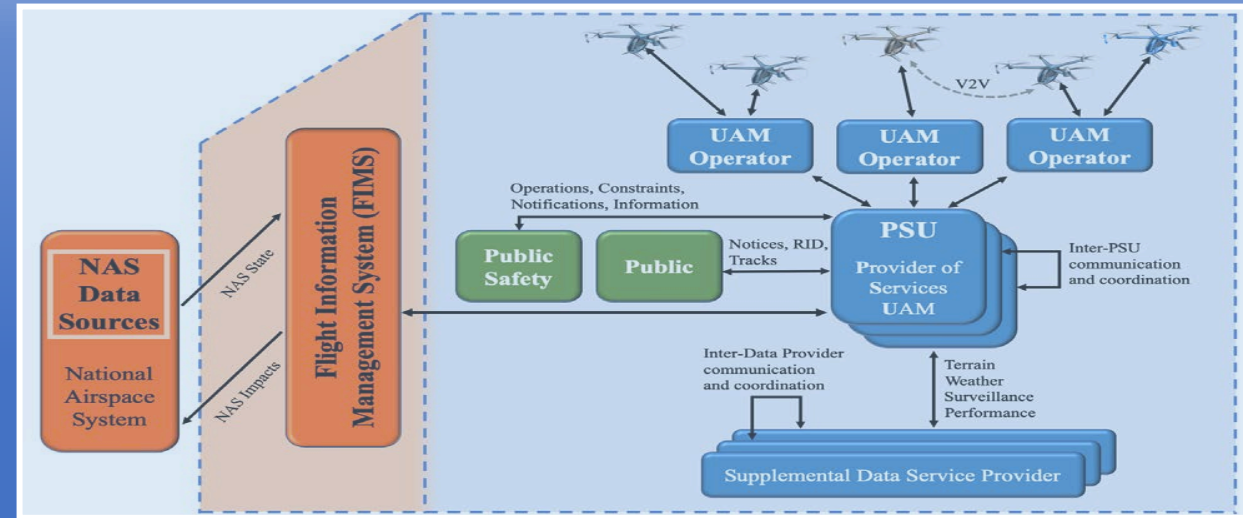


Identify: Threats to the UAM Air Space



Examples of Types of Threats

- **Eavesdropping**
 - Sniffing or snooping attack
- **Man in the Middle Attacks (MITM)**
 - Attack takes advantage of unencrypted and unsecured network communications to access data.
- **Account or Credentials Compromised**
 - Adversaries may steal the credentials of a specific user or service account
- **Spearphishing**
 - Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization, or business.
- **DDoS**
 - The aim of a DDoS attack is to overwhelm the website or online service with more traffic than the server or network can accommodate. Thus making the website or service inoperable.



Vulnerability Assessment

- The process of identifying, quantifying, and prioritizing the vulnerabilities in a system.

Asset Management

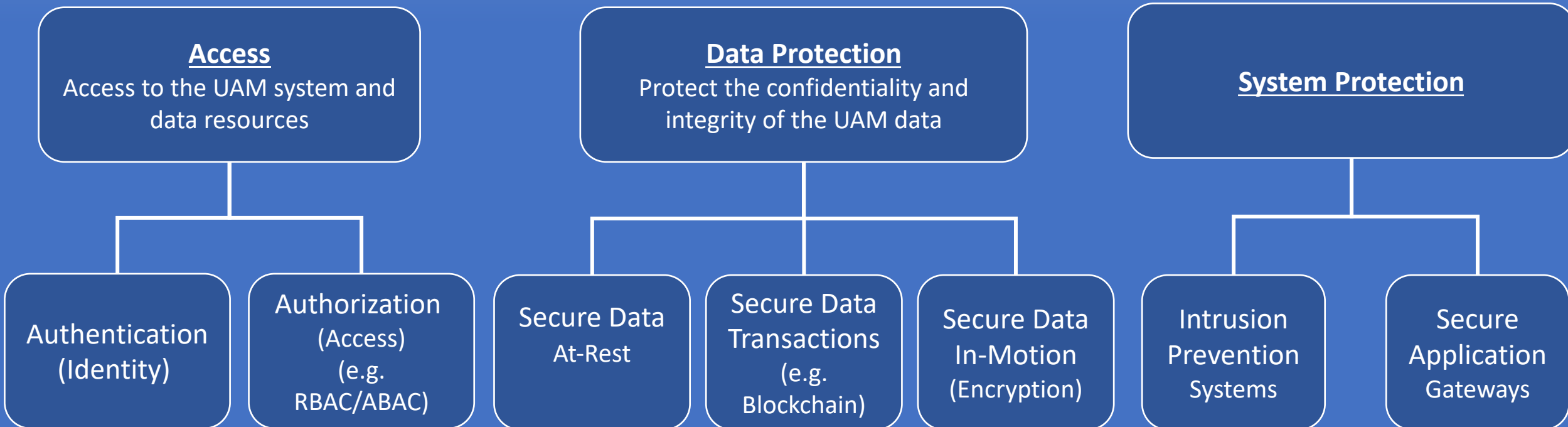
- The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed



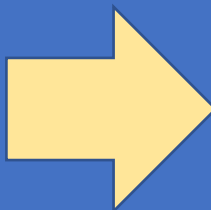
Logging

- A security log keeps a digital record of all your device activity and can provide an IT security admin a centralized view to better log and track who has made what changes, as well as if there are any issues with the data or system.

Provide the appropriate safeguards to ensure delivery of critical Secure Airspace services



Protect: Data Protection



Secure Data
In-Motion
(Encryption)

As data is transmitted between entities, within the environment, it is encrypted, in order to protect confidentiality

Secure Data
Transactions
(Blockchain)

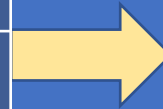
Data transactions can be stored in blockchain ledgers in order to support integrity and provide immutability

Secure Data
At-Rest

Data stored on the blockchain is encrypted to protect confidentiality

Based on threats, provide the appropriate safeguards to ensure delivery of critical UAM services

Cyber Threats	Protection Options
Eavesdropping	Encryption and VPNs are essential to thwart eavesdropping attacks.
Man in the Middle Attacks (MITM)	Encryption and public key pair-based authentication can be used in various layers of the stack to help ensure data confidentiality and integrity.
Targeted Messaging Attacks	Messaging protection will include encryption, anti-malware, and anti-spam security controls.
Distributed Denial of Service (DDoS)	A multi-level protection strategy that includes advanced intrusion prevention and threat management systems, which combine firewalls, VPN, anti-spam, content filtering, and load balancing.



Term	Definition
Data and Message Encryption	A security method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key.
Data Loss Prevention (DLP)	Data loss prevention software detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while in use, in motion, and at rest.
Load Balancers	Load balancing refers to the process of distributing a set of tasks over a set of resources, protects against DDoS attacks
Redundant Networks	A process through which additional or alternate instances of network devices, equipment and communication mediums are installed within network infrastructure, in order to support resiliency.
Web Application Firewall (WAF)	A web application firewall filters, monitors, and blocks HTTP traffic to and from a web application.
Zero-Trust Network Architecture	A security model based on the principle of maintaining strict access controls and not trusting anyone by default, even those already inside the network perimeter.

Identify the occurrence of a cybersecurity or disruptive event within UAM ecosystem

Host-Based Intrusion Detection System (HIDS)

Monitor and
analyze
internals of
UAM computing
systems

Monitor
and analyze
the UAM
system packets

Anomaly Detection

Monitor and
control incoming
and outgoing
traffic of UAM
systems

Implement
security rules
for the UAM
systems

File Integrity Monitoring (FIM)

Monitor and
analyze file and
system registry
settings of
UAM systems

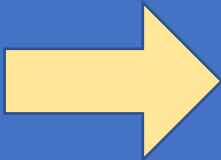
Maintains
a forensic copy
of the data on
UAM systems

Detect function as the development and implementation of activities "to identify the occurrence of a cybersecurity event," with a focus on supporting the timely discovery of such events.



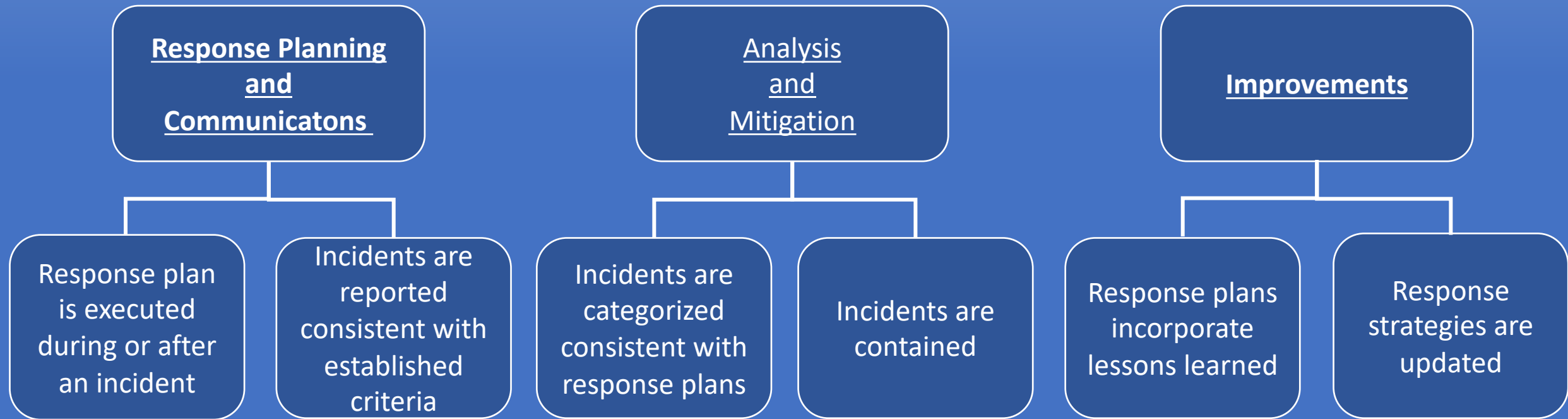
Identify the occurrence of a cybersecurity or disruptive event within UAM ecosystem

Cyber Threats
Eavesdropping
Man in the Middle Attacks (MITM)
Targeted Messaging Attacks
DDoS



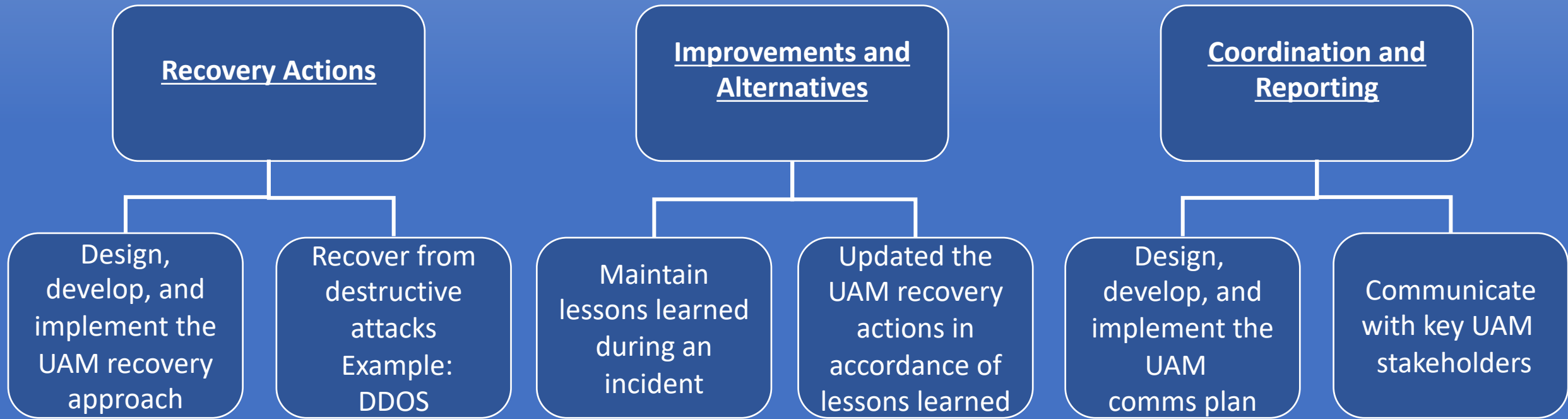
Term	Definition
Intrusion Detection System (IDS)	The IDS functions as an alarm system for the network that is used to detect and alert on suspicious activity.
Security Information and Event Management (SIEM)	Security information and event management is a subsection within the field of computer security, where software products and services combine security information management and security event management. They provide real-time analysis of security alerts generated by applications and network hardware.

Respond – Steps to be taken when something goes wrong



The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.

Recover – Resiliency for UAM environments



The Recover function is imperative, and the ability to carry the associated actions quickly can help reduce the overall impact and prevent damage to the organization's reputation.

Follow our Story



www.nasa.gov/aero



[@NASAAero](https://twitter.com/NASAAero)



[@NASAAer](https://www.instagram.com/NASAAer)



[@NASAAero](https://www.facebook.com/NASAAero)

