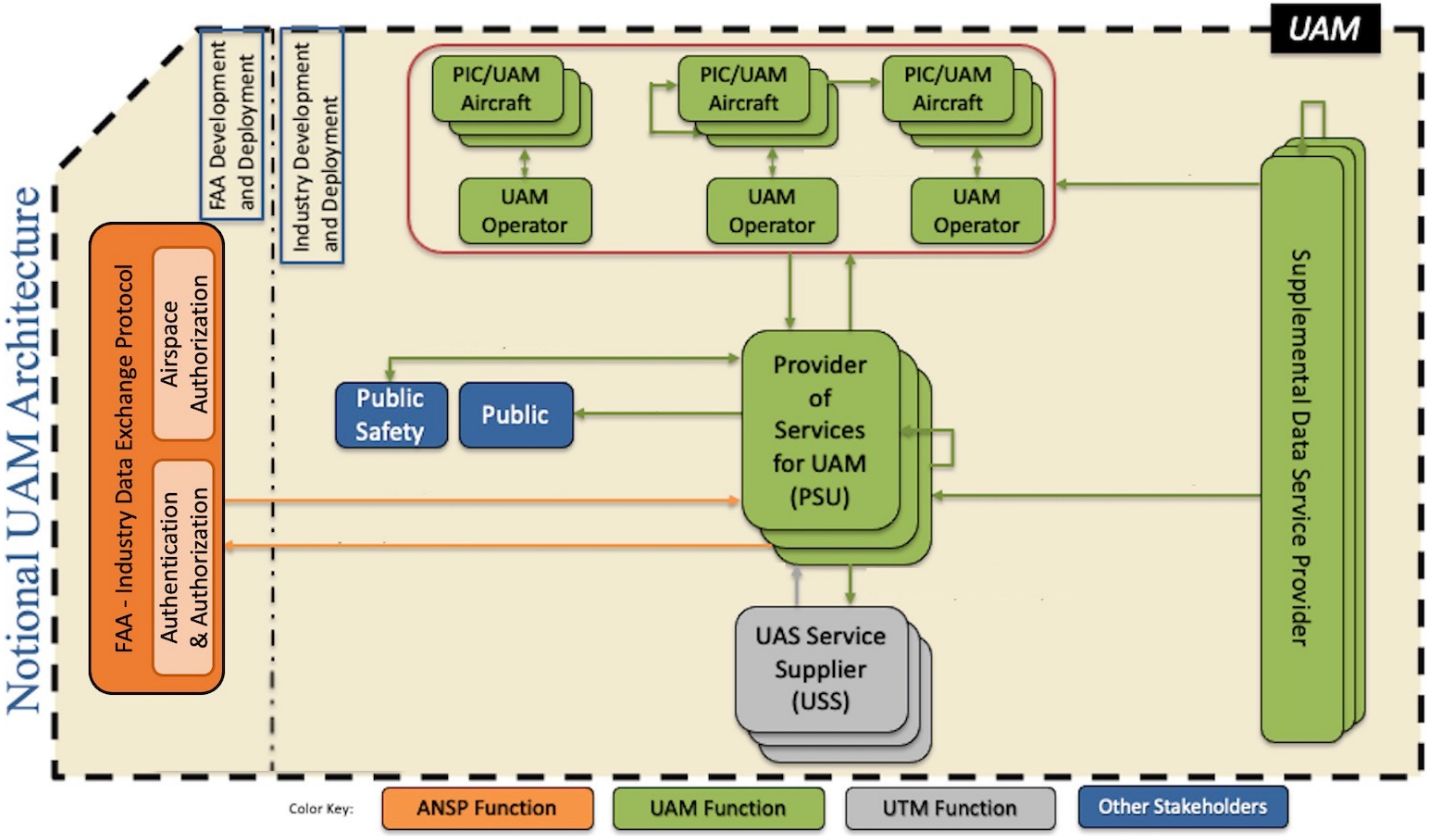
Challenges in Securing UAM Operations


UAM
Notional UAM Architecture
FAA Development and Deployment
Industry Development and Deployment
FAA - Industry Data Exchange Protocol
Airspace Authorization
Authentication & Authorization
PIC/UAM Aircraft
PIC/UAM Aircraft
PIC/UAM Aircraft
UAM Operator
UAM Operator
UAM Operator
Public Safety
Public
Provider of Services for UAM (PSU)
UAS Service Supplier (USS)
Supplemental Data Service Provider
Color Key:
ANSP Function
UAM Function
UTM Function
Other Stakeholders

Kenneth Freeman
NASA Ames Research Center

Definitions

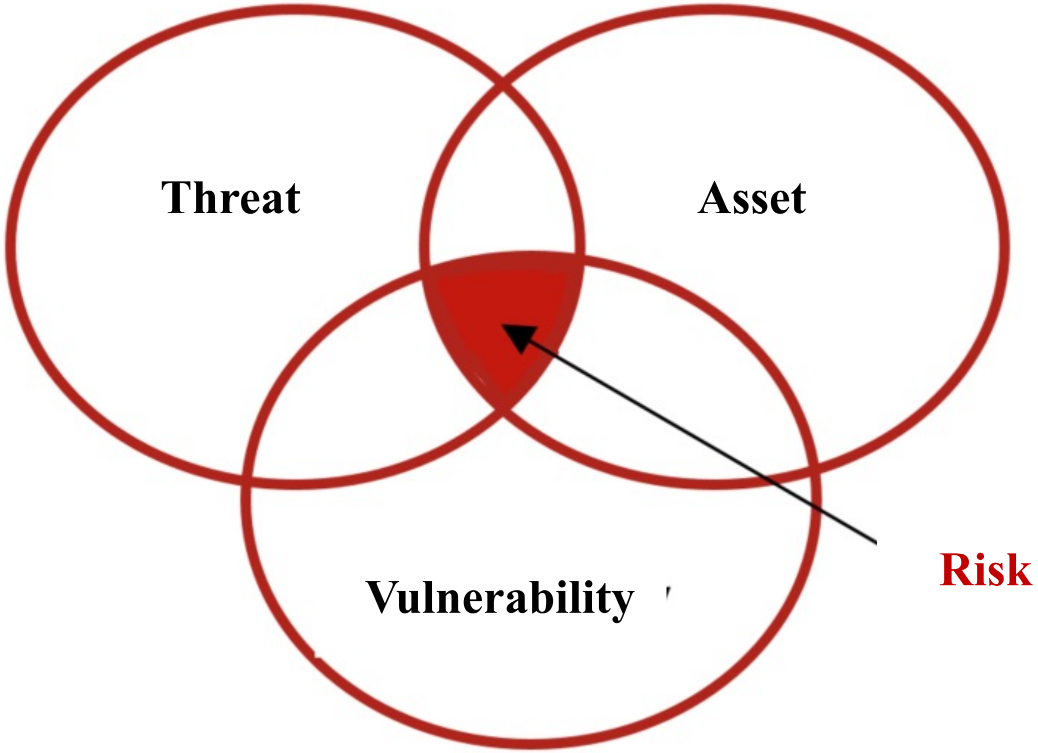
Threats may be intentional or unintentional

Threat	Any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, or through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerabilities include but are not limited to software flaw vulnerability is caused by an error in the design or coding of software.

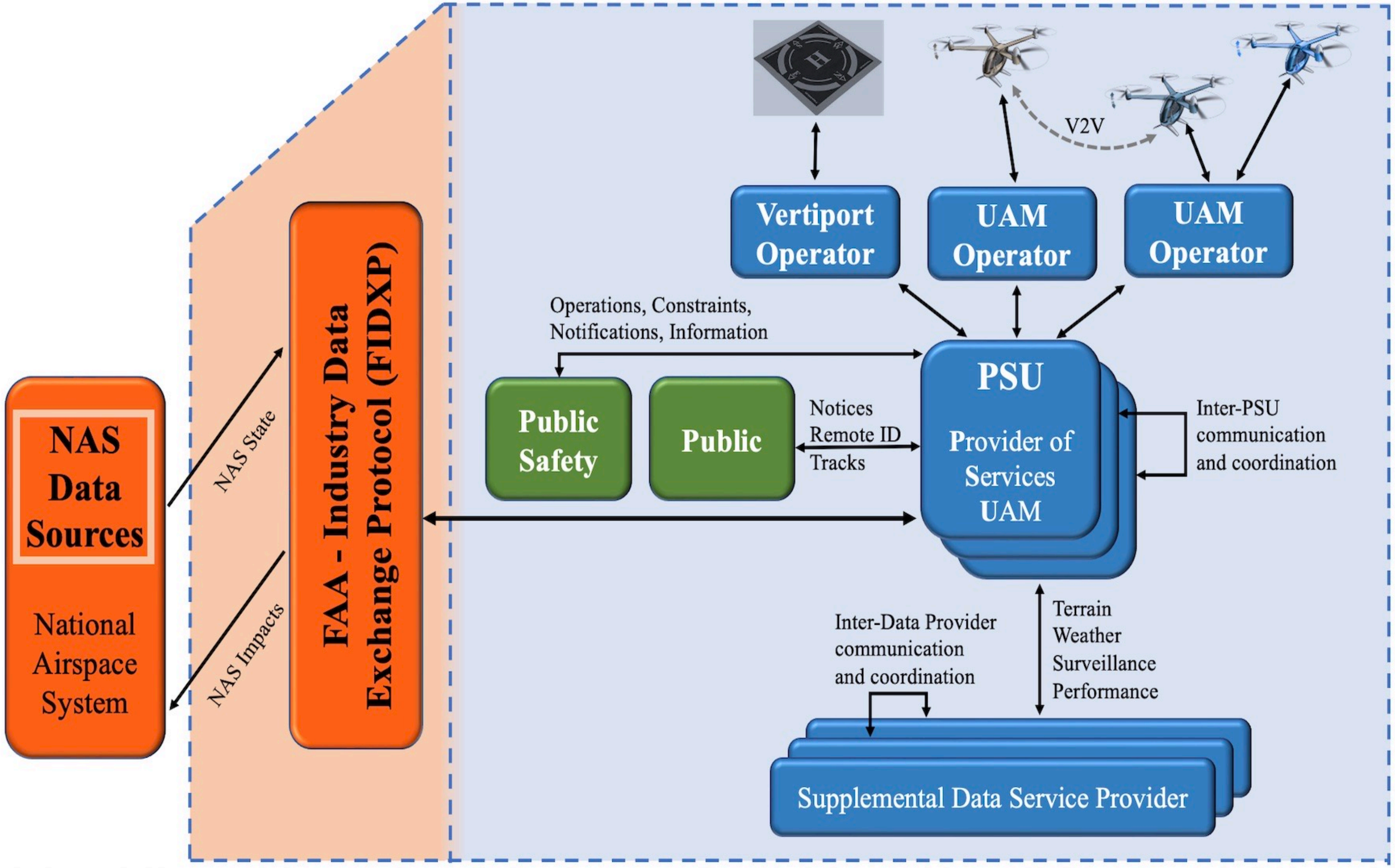
Definitions

Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: 1. The adverse impacts that would arise if the circumstance or event occurs; and 2. The likelihood of occurrence.



Risk = Threat X Vulnerability

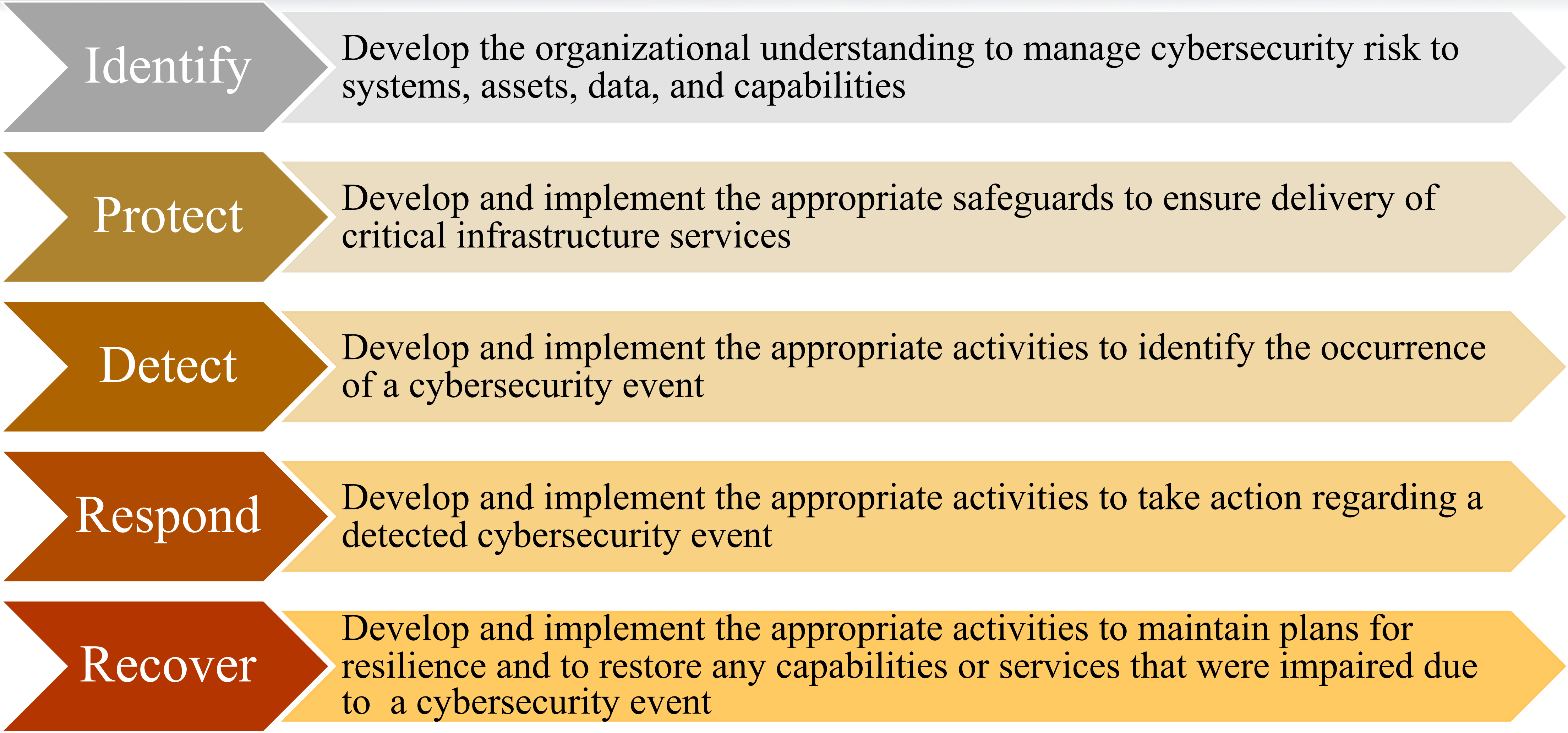
UAM Environment



V2V
Vertiport Operator
UAM Operator
UAM Operator
Operations, Constraints, Notifications, Information
Public Safety
Public
Notices
Remote ID
Tracks
PSU
Provider of Services UAM
Inter-PSU communication and coordination
NAS Data Sources
National Airspace System
NAS State
NAS Impacts
FAA - Industry Data Exchange Protocol (FIDXP)
Inter-Data Provider communication and coordination
Terrain
Weather
Surveillance
Performance
Supplemental Data Service Provider

- The UAM environment has a service-oriented architecture where UAM operators and service providers work independently to mange aerial vehicles in the urban environment.
- The UAM operators, vertiport operators, services and the FAA are supported by local computing and cloud services, which are interconnected across various networks

NIST Cybersecurity Framework



Identify Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities

Protect Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services

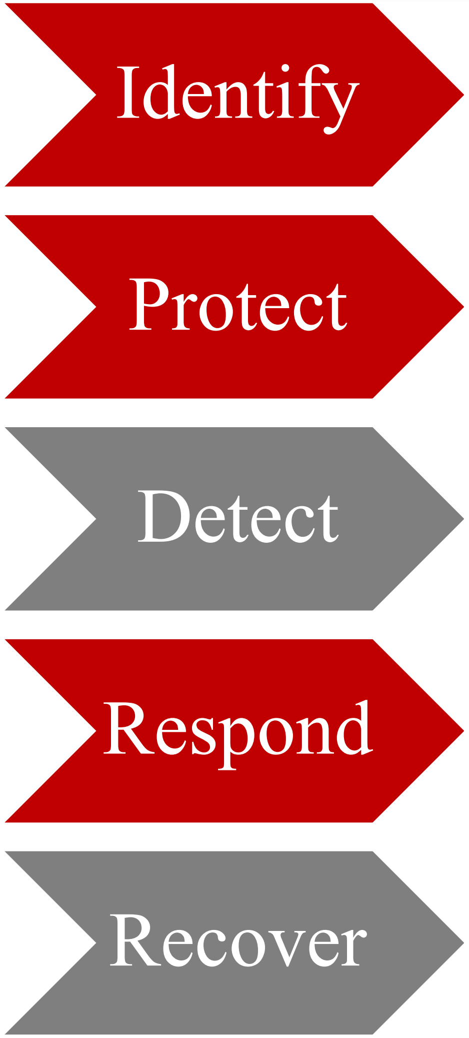
Detect Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event

Respond Develop and implement the appropriate activities to take action regarding a detected cybersecurity event

Recover Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event

NIST – National Institute of Standards and Technologies

Challenge: Decentralized UAM Operations

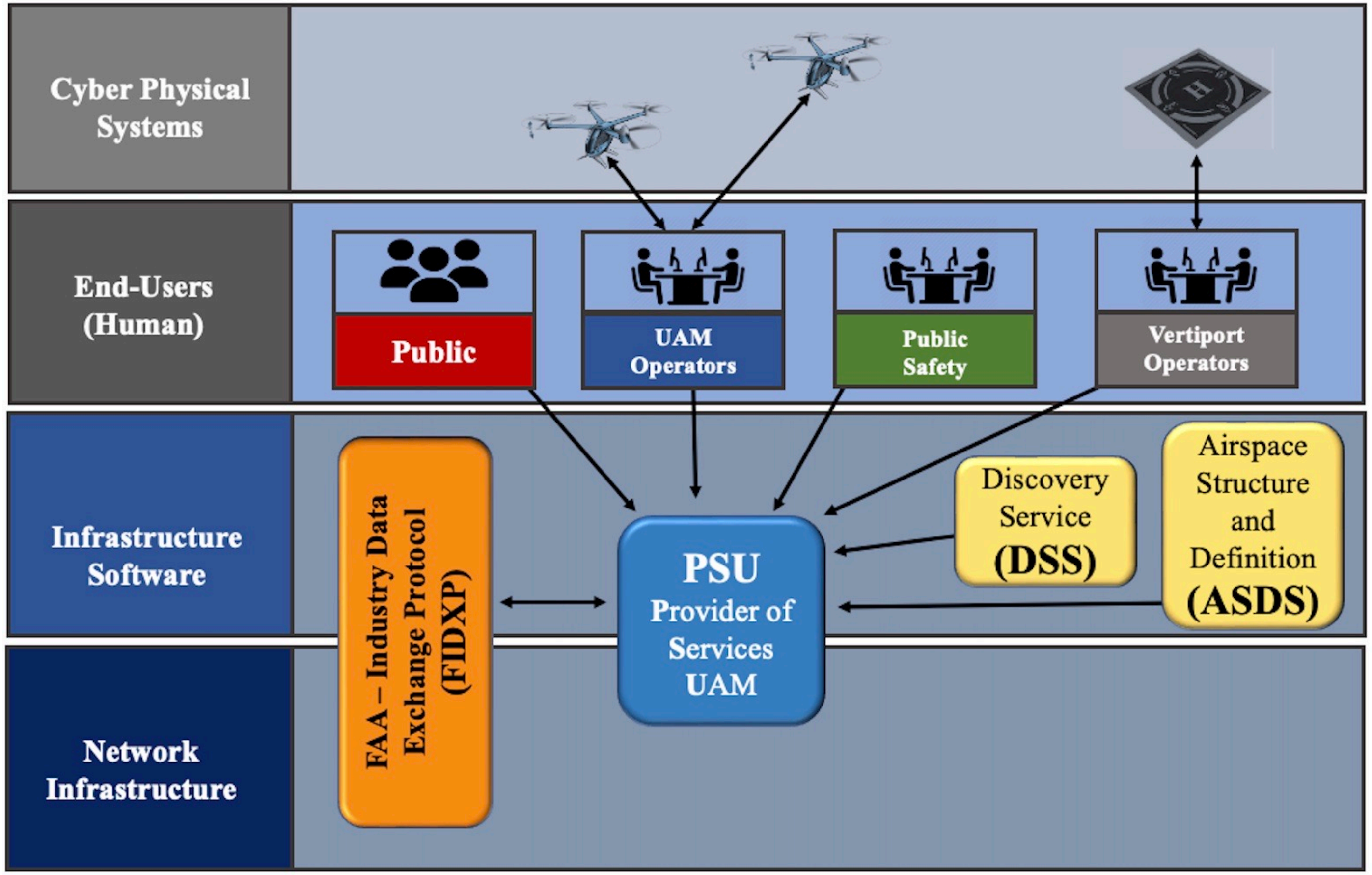


Governance	• Will need to determine the overall cybersecurity governance policy across decentralized UAM environments ○ Will there be common guidance for vulnerability management? ○ Will cyber attacks and compromises be shared across the UAM ecosystems? ○ Will there be coordinated incident response plans
Operations	• A trust model needs to be established across the UAM operators and service providers • Need to determine how identities for people and systems will be managed across a decentralized UAM operations

UAM Environment

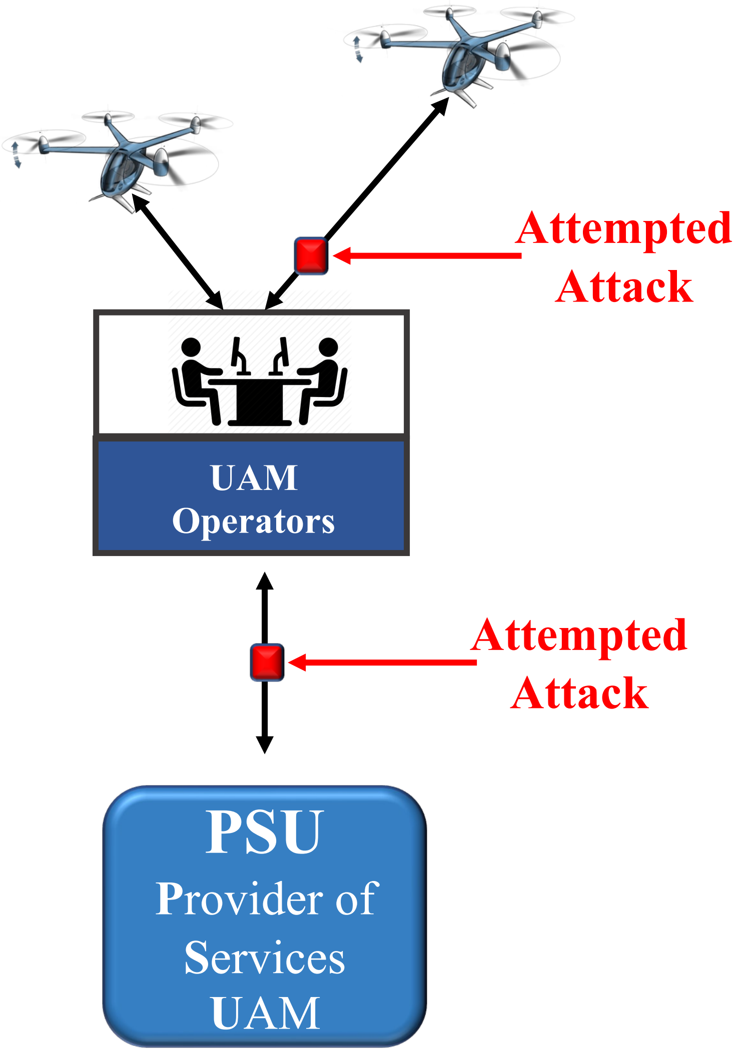
UAM environments will consist of a wide range of diverse systems supporting flight missions

- The UAM environment can be viewed from the perspective of four significant high-level components, cyber-physical systems, end-users, infrastructure software and network infrastructure.
- Threats, vulnerabilities, weaknesses, and security controls for the UAM environment, are studied from these four components' perspective.
- The applicable threats, vulnerabilities, and weaknesses of the UAM environment's four component areas will differ due to the cyber-physical, cloud, and on-premise architectures.

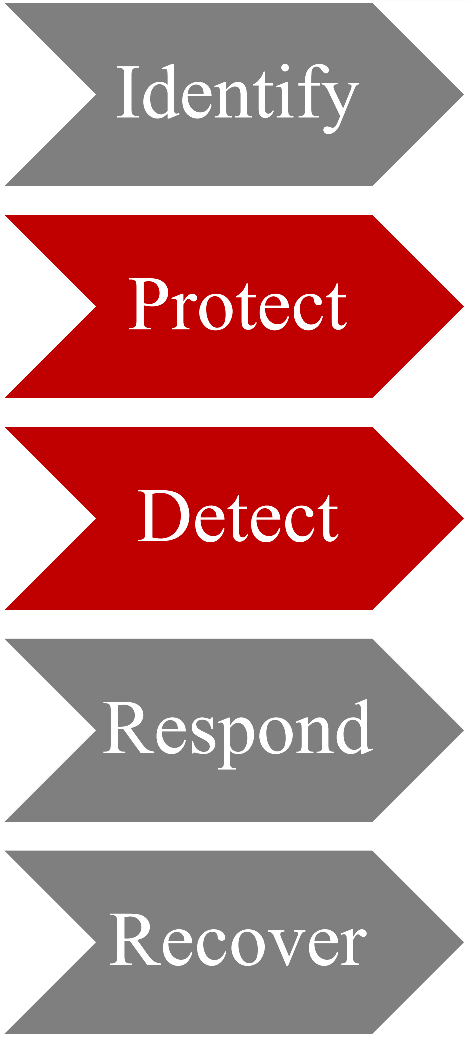


Selected Threats to the UAM Environment

Jamming	• Jamming, leading to the limitation of available data • For UAM, jamming attacks could hinder the communications between a vehicle and the UAM operator
Denial of Service	• The purpose of the attack is to degrade or block the availability of services to users. • One of the most common ways is to leverage a botnet to bombard a website or API with more requests than it can handle. • Denial of service attacks do not have to render an application unusable to be a success; simply slowing the application down can often still be harmful.



Challenge: Protecting Cyber Physical Systems



Identify

Protect

Detect

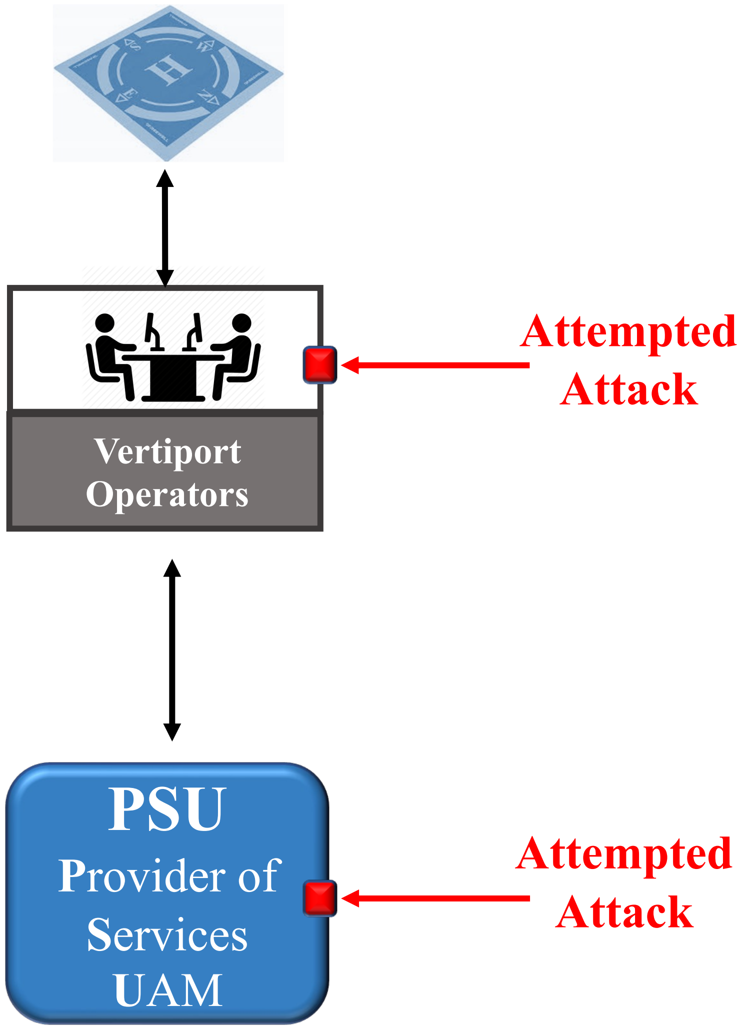
Respond

Recover

Threats	• Jamming communications signals • GPS spoofing • Denial of Service (DoS)
Mitigations	• Encrypted communications • Alternate communications options • Alternate position systems • Anomaly detection

Selected Threats to the UAM Environment

Social Engineering	• Social Engineering is the umbrella method for attempting to deceive users into giving away sensitive details. • Social Engineering is the act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust.
Ransomware	• Ransomware is malware that employs encryption to hold a victim's information at ransom. • A user or organization's critical data is encrypted so that they cannot access files, databases, or applications. • A ransom is then demanded to provide access. Ransomware is often designed to spread across a network and target database and file servers and can thus quickly paralyze an entire organization.



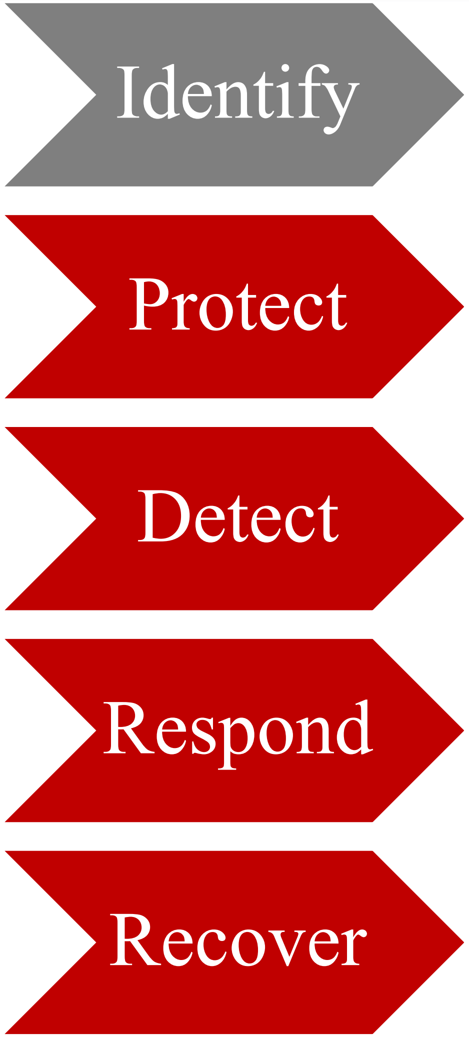
Vertiport Operators

PSU Provider of Services UAM

Attempted Attack

Attempted Attack

Challenge: Human Error (Witting or Unwitting)



Identify

Protect

Detect

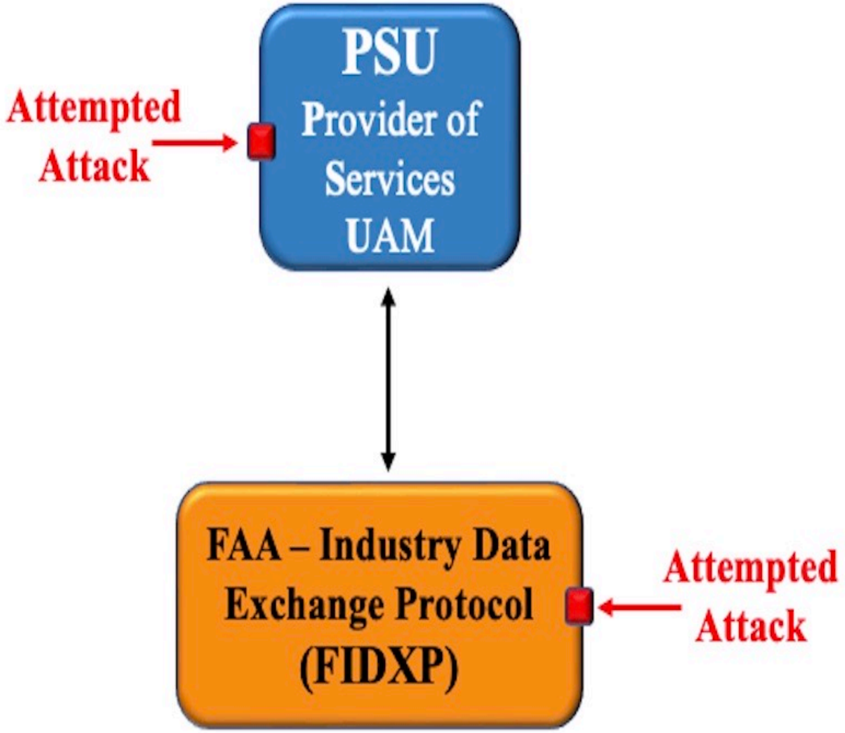
Respond

Recover

Threats	• Social engineering (including voice, text message, email phishing) • Ransomware • Insecure design or system misconfigurations • Insider Threats
Mitigations	• Education • Zero Trust • Network segmentation • Continuous monitoring • Ransomware response and recovery planning

Selected Threats to the UAM Environment

Broken Access Control	• Access control, or authorization, is the mechanism in place to control who has access to some resource such as a website or an API. • Attacks include replaying authentication information like a stolen security token, modifying website code to make invalid requests, or sometimes simply making a request the developer did not expect the user of the application to make.
Botnets	• Botnets are a network of computers that have been hijacked to carry out some unified cyber-attack or some other coordinated result. • Due to the advancement of automated computing and distributed systems botnet attacks have become more sophisticated and are also able to operate in a more distributed and automated fashion.



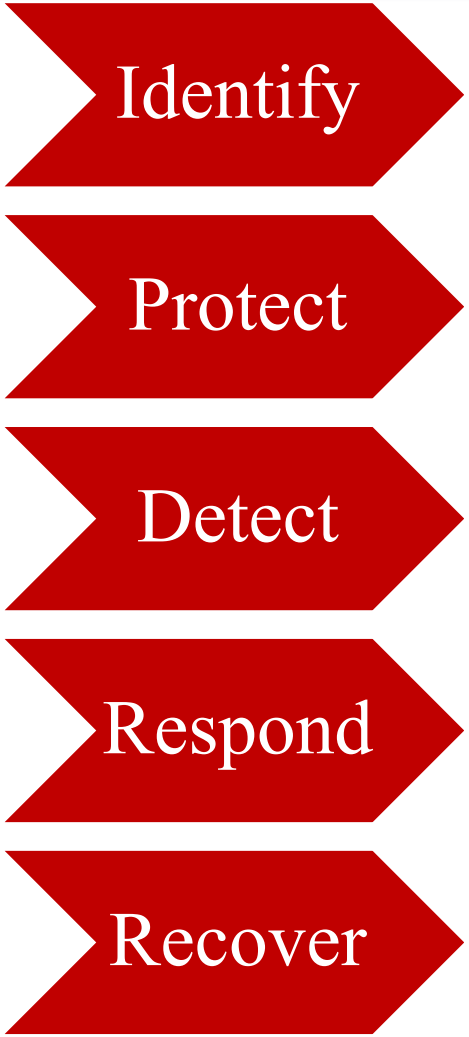
Attempted Attack

PSU Provider of Services UAM

FAA – Industry Data Exchange Protocol (FIDXP)

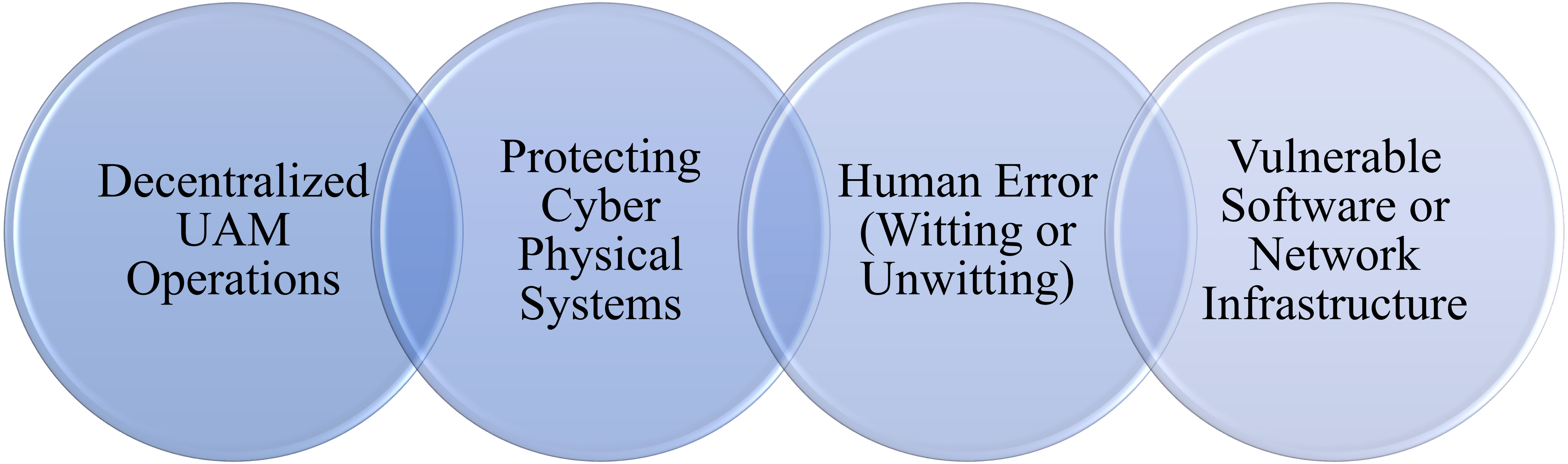
Attempted Attack

Challenge: Vulnerable Software or Network Infrastructure



Threats	• Broken access control • Cryptographic failures • Vulnerable and outdated components • Injection • Identity and authentication failures
Mitigations	• Construct a pre-incident strategy that includes backup, asset management and restriction of user privileges • Build post-incident response procedures • Strengthen identity proofing and identity recovery (Expand multi-factor authentication (MFA)) • Vulnerability assessments and patching

Challenges in Securing UAM Operations



Decentralized UAM Operations

Protecting Cyber Physical Systems

Human Error (Witting or Unwitting)

Vulnerable Software or Network Infrastructure