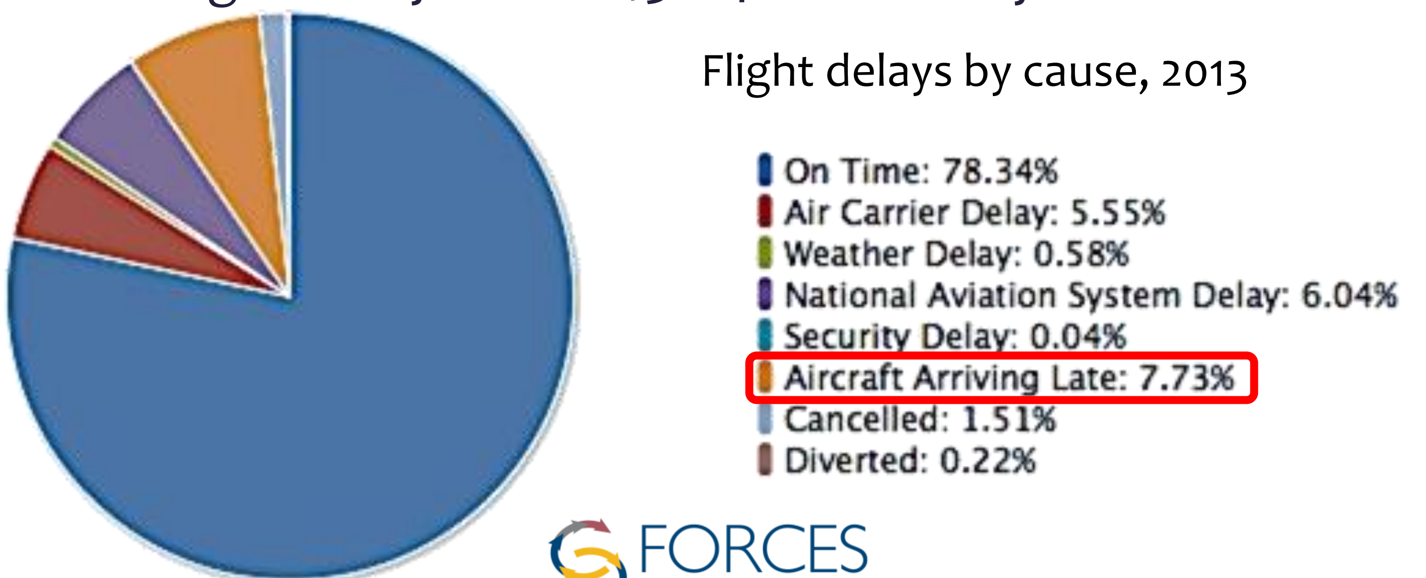
Towards a Resilient and Secure Air Transportation Infrastructure

Hamsa Balakrishnan
(with Karthik Gopalakrishnan & Sandeep Badrinath)
Massachusetts Institute of Technology

Resilient air transportation

- Delays propagate through the system
  - A delayed flight delays the aircraft, the crew, and the passengers
  - Large number of shared (airport and airspace) resources increase delay propagation
  - Domestic flight delays cost ~$30-40B annually

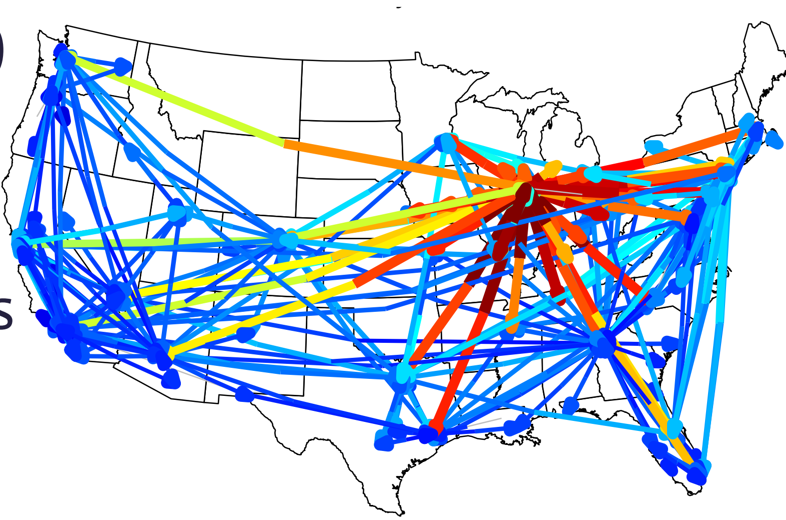
Flight delays by cause, 2013



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Air traffic delay networks

* Weighted, directed, labeled graphs
* Network built from Bureau of Transportation Statistics data (2011-12)
* Nodes: Airports; edges: OD pairs with more than 5 flights/day on average
* Weights: Departure delays on OD pairs
* Network with 158 nodes and 1,107 edges
* Characterizing networks using edge weights requires $\mathcal{O}(n^2)$ parameters



[Rebollo & Balakrishnan 2014]

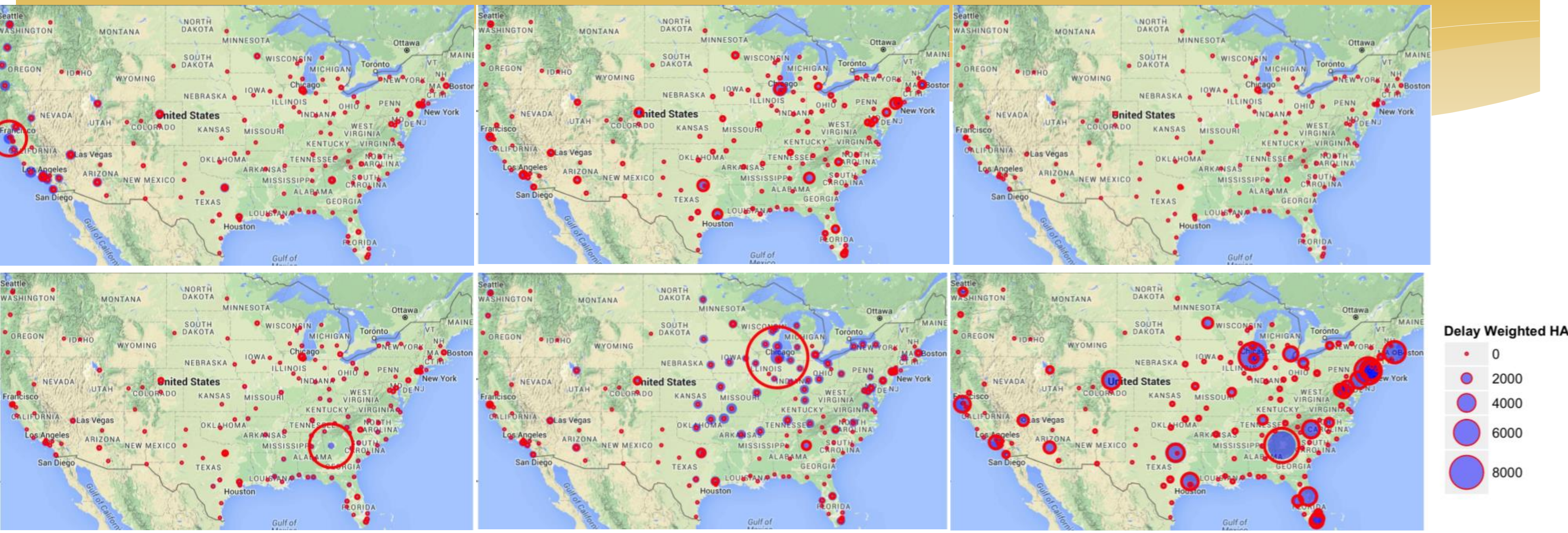
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Network centrality metrics for directed graphs

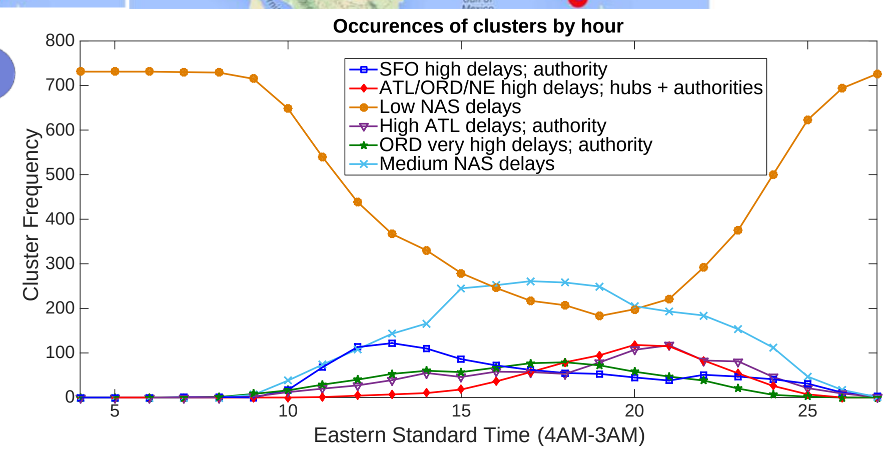
* Hub and authority scores for each node
* Strong **hubs point to** strong authorities ←→ Strong **authorities are pointed to** by strong hubs
* Extension of eigenvector centrality to directed graphs
* Characterizing a directed network by hub and authority scores, and node out- and in-degrees: $\mathcal{O}(n)$ parameters
  * Cluster networks using k-means or k-medoids algorithms
  * Silhouette plots to evaluate number of clusters

[Gopalakrishnan et al., submitted to ACC 2016]

Clustering delay-weighted hub and authority scores



* Hub scores: ○; Authority scores: ●
* Clustering of 731 x 24 data points (every hour for 2 years)
* Likelihood of "delay state" (discrete mode) occurrence varies by time-of-day



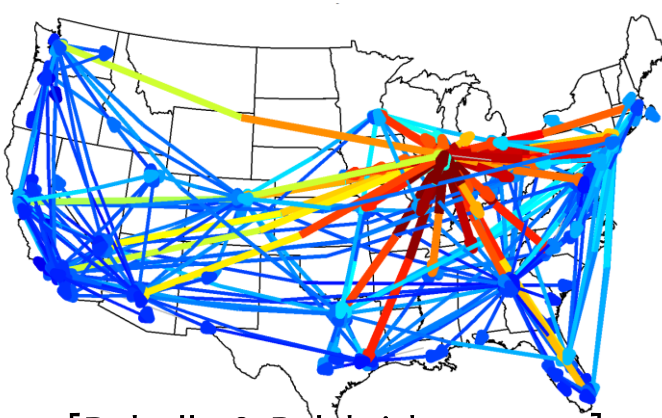
[Gopalakrishnan et al., submitted to ACC 2016]

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Modeling resilience: Delay propagation

$$x_i^{\text{in}}(t+1) = \alpha_i^{\text{in}} x_i^{\text{in}}(t) + \beta \sum_{j=1}^{n} a_{ji} x_j^{\text{out}}(t)$$

$$x_i^{\text{out}}(t+1) = \alpha_i^{\text{out}} x_i^{\text{out}}(t) + \beta \sum_{j=1}^{n} a_{ij} x_j^{\text{in}}(t)$$



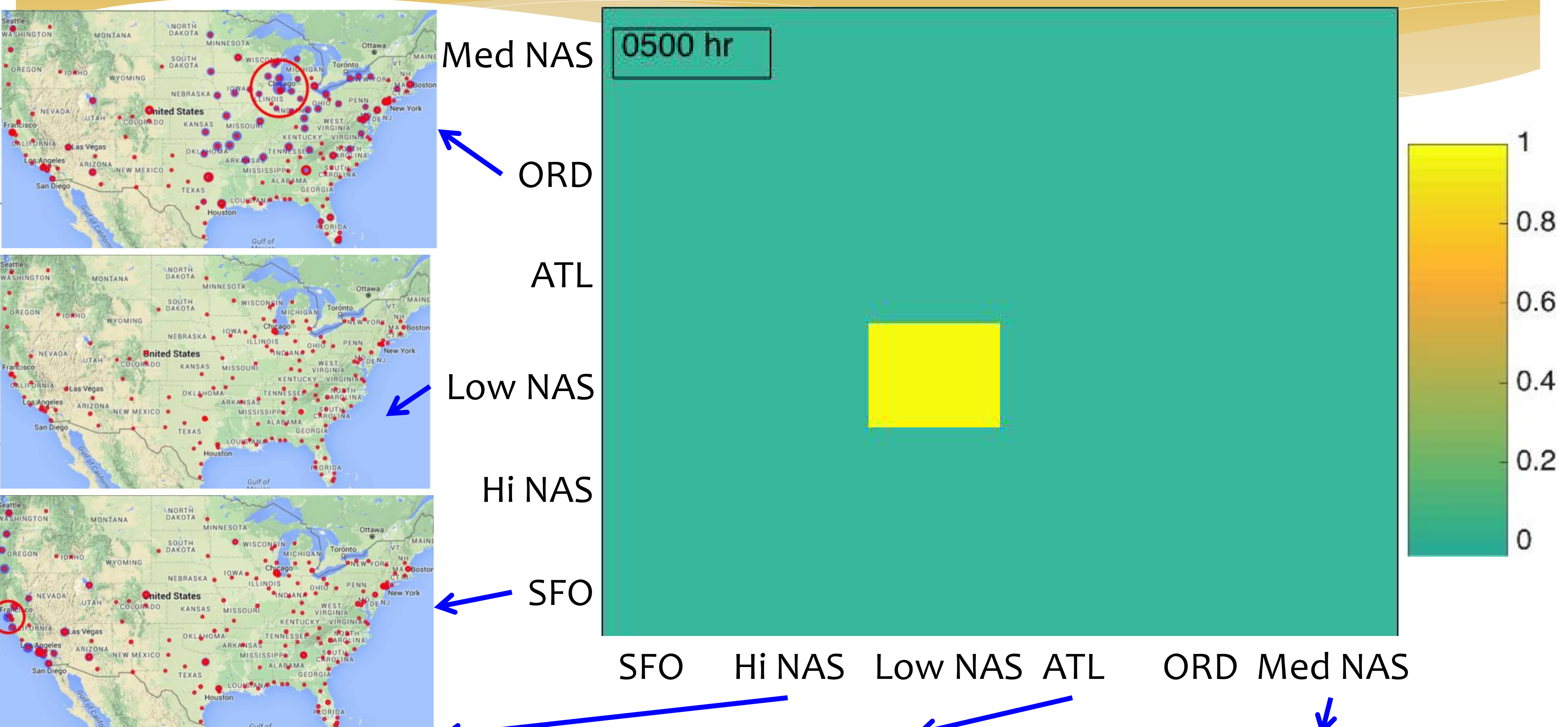
[Rebollo & Balakrishnan 2014]

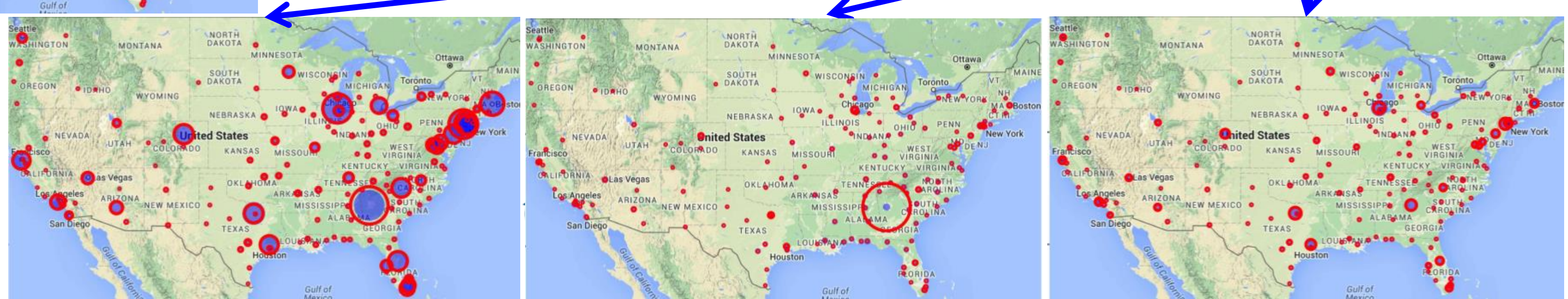
$$\bar{x}(t+1) = \tilde{A}_{i(t)} \bar{x}(t), \quad \text{where } i(t) \text{ is the discrete mode at } t.$$

* Conditions for system stability (i.e., attenuation of delays)
* Hybrid system: Switching between discrete delay modes

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Hybrid systems model with stochastic transitions between delay states





Securing the air transportation system

- Clearly, a rapidly growing concern worldwide…
  - Airlines step up efforts to tackle cyber security risks -Reuters, 10/26/15

GAO
United States Government Accountability Office
Report to Congressional Requesters

January 2015

INFORMATION SECURITY

FAA Needs to Address Weaknesses in Air Traffic Control Systems

GAO-15-221

GAO
United States Government Accountability Office
Report to Congressional Requesters

April 2015

AIR TRAFFIC CONTROL

FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen

GAO-15-370

GAO
United States Government Accountability Office
Report to Congressional Requesters

July 2015

NEXT GENERATION AIR TRANSPORTATION SYSTEM

Improved Risk Analysis Could Strengthen FAA's Global Interoperability Efforts

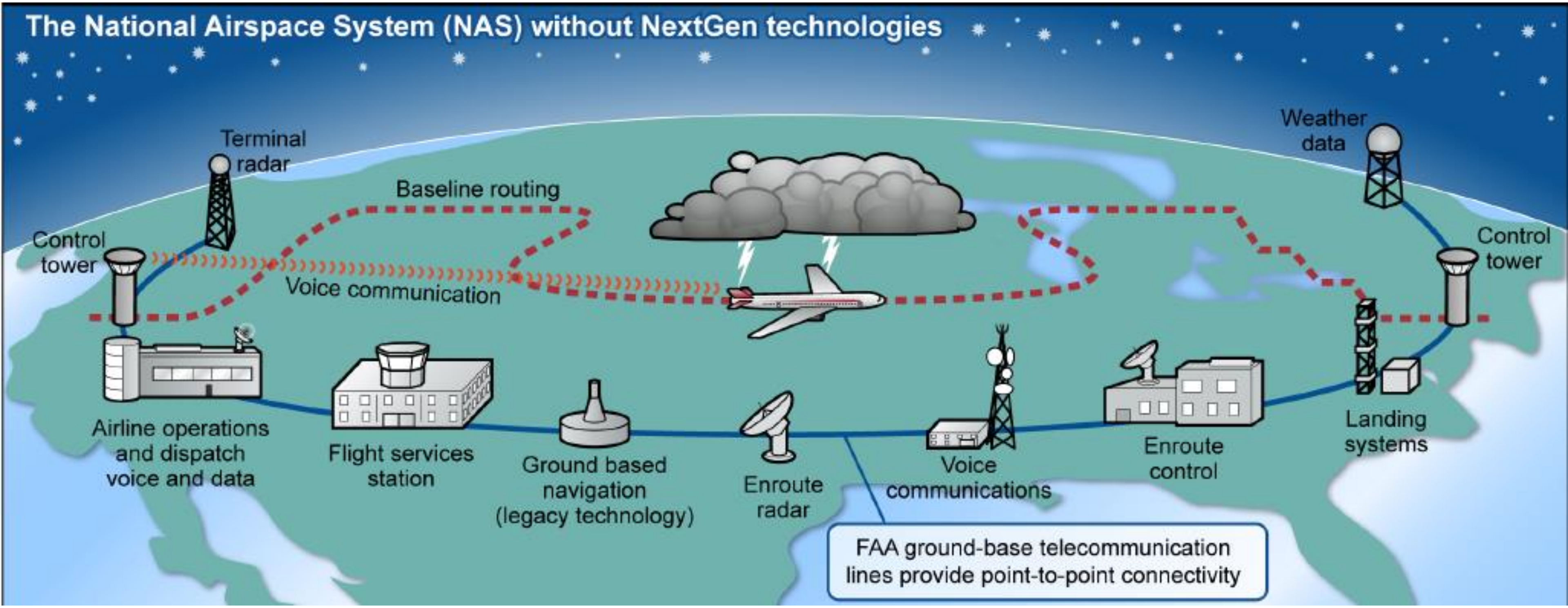
GAO-15-608

  - Cyber insurance premiums rocket after high-profile attacks -Reuters, 10/12/15

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

The NextGen transformation

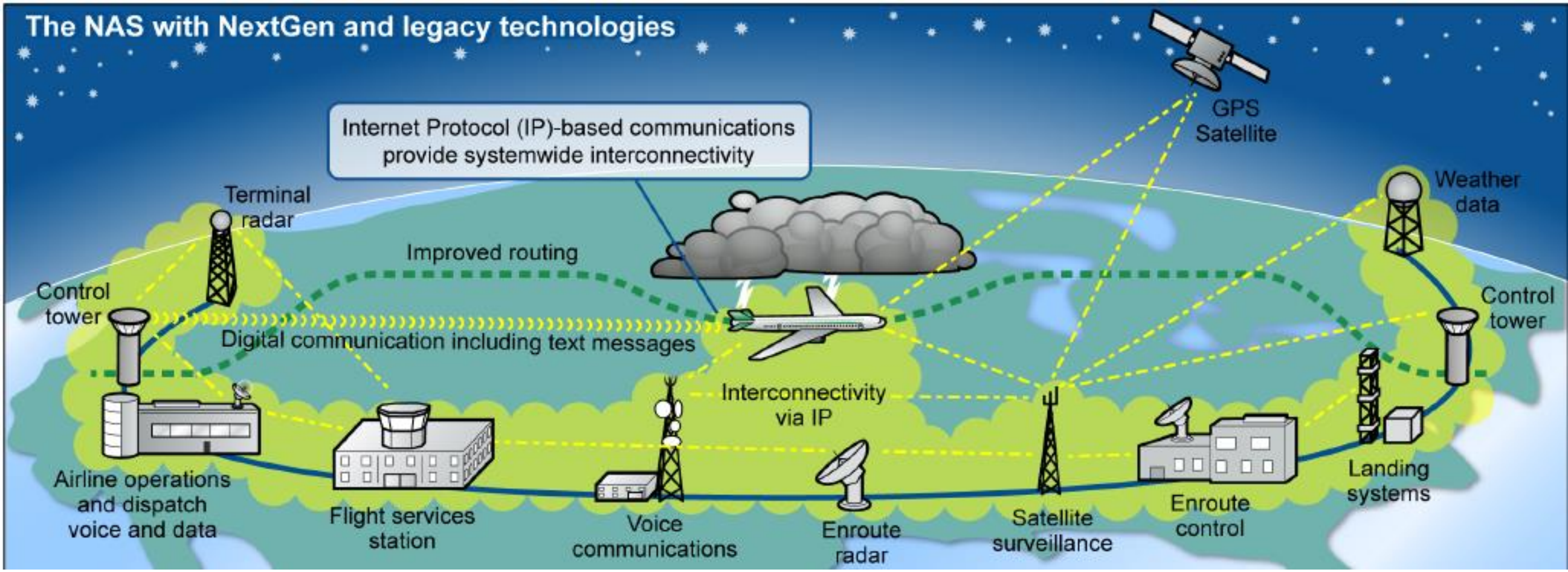
- Ground-based systems (radars, point-to-point communications) → satellite-based navigation + IP-based communications



[GAO-15-370, 2015]

The NextGen transformation

- Ground-based systems (radars, point-to-point communications) → satellite-based navigation + IP-based communications



[GAO-15-370, 2015]

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

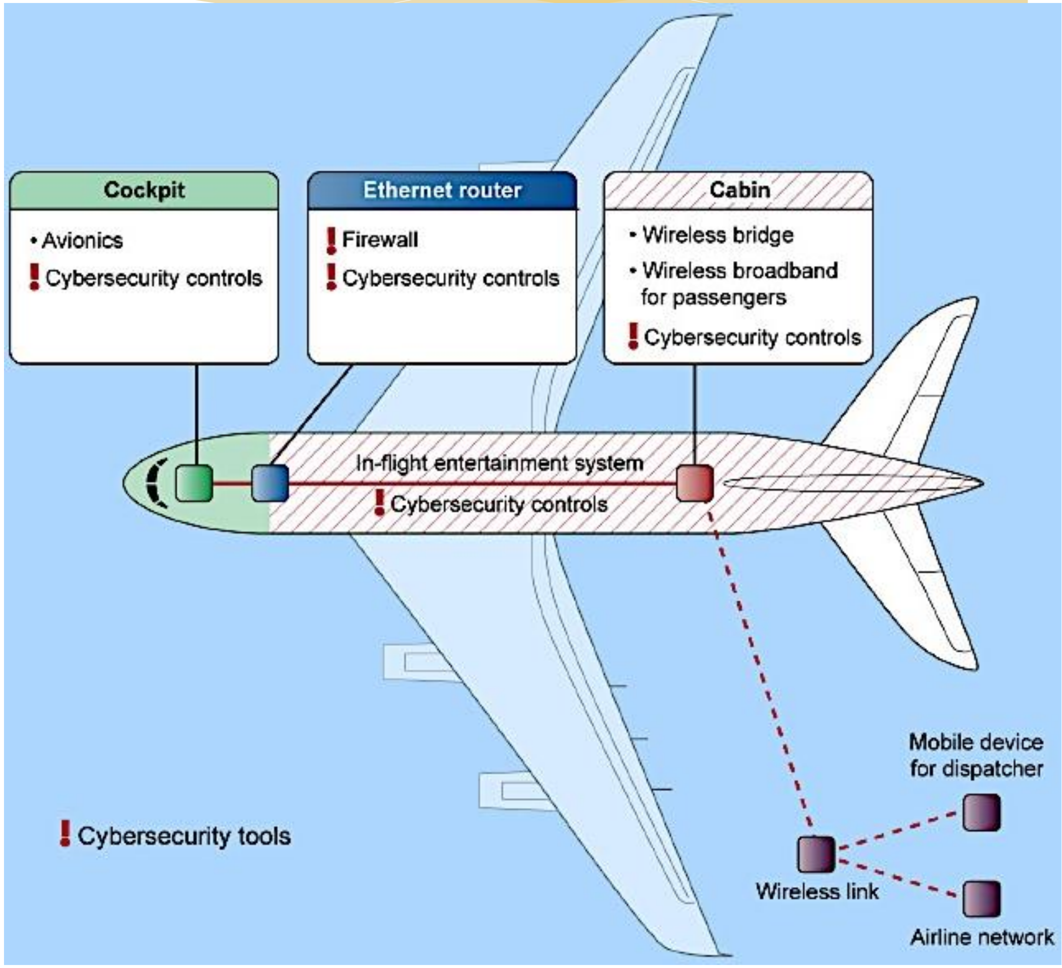
Many NextGen programs have security implications

* **Surveillance & Broadcast Services Subsystem (SBSS)**
  * e.g. ADS-B
* **System Wide Information Management (SWIM)**
* **Collaborative Air Traffic Management Technologies (CATMT)**
* Common Support Services Weather (CSS-Wx)
* Data Communications (DataComm)
* NAS Voice Switch (NVS)
  * Digital communications

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

And then there is the aircraft itself…

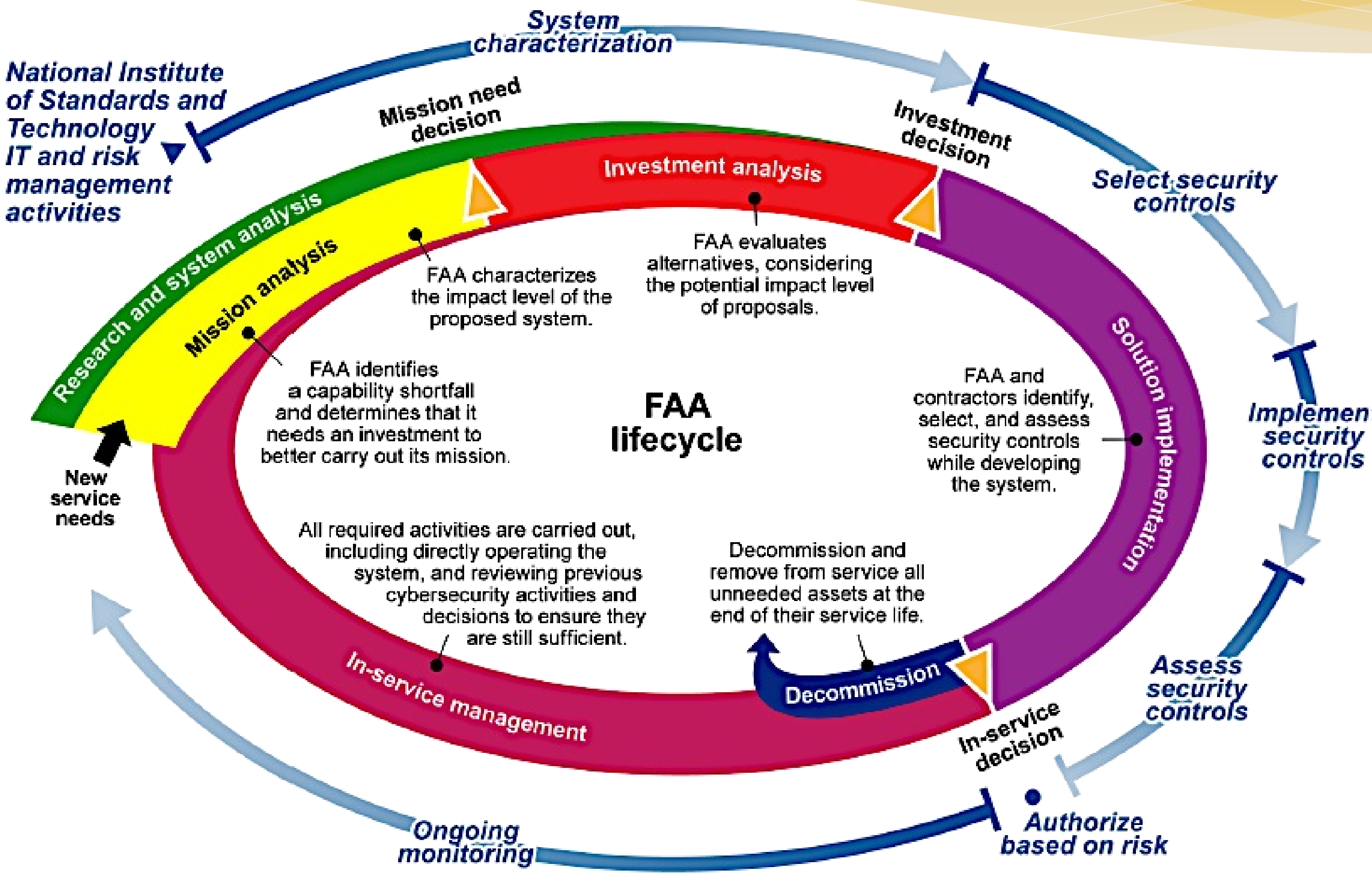
- Traditionally, aircraft G&C systems are isolated from other systems
- Change is on its way
  - Electronic Flight Bags
  - Proliferation of handheld devices
  - Firewall between cockpit and cabin systems
  - “Special Conditions” for Boeing 787 and Airbus A350
- Access control



[GAO-15-370, 2015]

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

FAA has adopted NIST guidelines



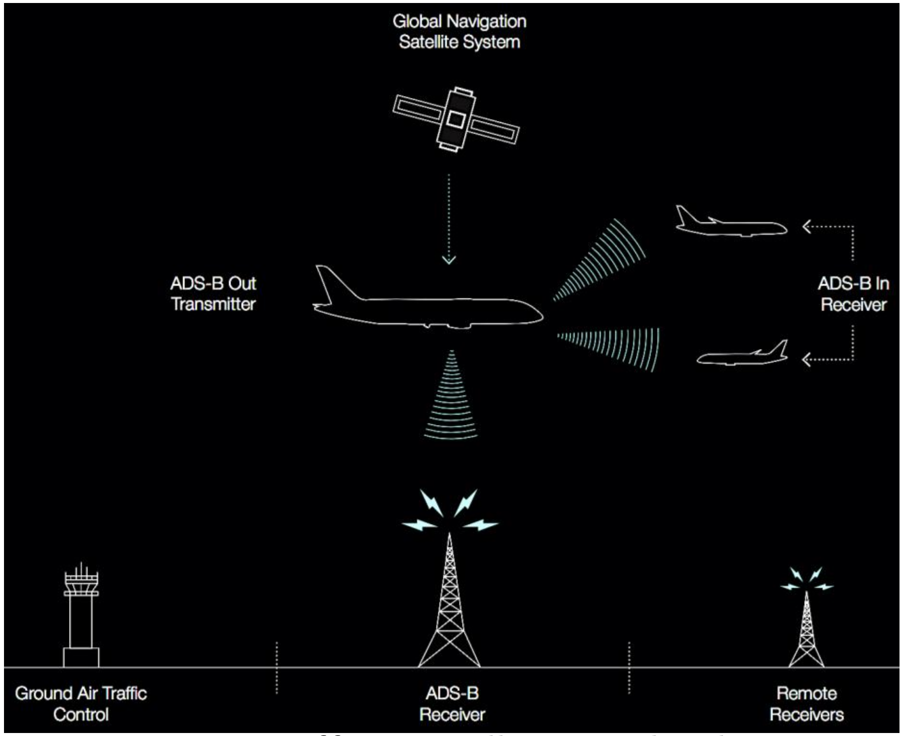
Sources: GAO and FAA. | GAO-15-370

Primary focus is on access control of IT systems, e.g., ensuring that only authorized users can access systems

NIST, *Guide for Applying the Risk Management Framework to Federal Information Sys.*, 2010

Secure ATC

- Focus on Surveillance and Broadcast Services Subsystem (SBSS)
  - Automatic Dependent Surveillance – Broadcast (ADS-B)
  - Satellite-based navigation
- Broadcasts of position, velocity, intent, flight number, etc.
- Sent through 1090 MHz datalink
- **Not encrypted**; range: >100 nmi
- Received by other aircraft as well as ground receivers
  - ATC surveillance
  - Collision detection & resolution
  - Efficient routing



New air traffic Surveillance technology.
Richards, O'Brien and Miller, 2010

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Taxonomy of attacks

* Parallels to other vehicular networks [e.g. Raya & Hubaux 2007]

	Attack/fault type	Impact	Ease	Mitigation mechanism
Passive	Eavesdropping	Privacy	H	-- current --
Active: DOS	Jamming 1090 MHz channel	Message deletion; ATC surveillance	M	Adaptive ADS-B transponder power [Park et al. 2014]; Robust CD&R protocols
Random	Message collisions			
Active: Deception	Ghost aircraft injection	Situational awareness	M	Public Key Infrastructure (Certificates) **UAS challenge**: Scalability
Active: DOS	Ghost aircraft flooding	System overload	M	
Random	Surveillance uncertainty	Situational awareness; conflict detection/resolution Geo-fencing		Leverage "physical" models & other sys [Park et. al 2014] **UAS challenge**: Diversity of dynamics
Active: Deception	Trajectory modification/ aircraft spoofing		L	

Taxonomy of attacks

* Parallels to other vehicular networks [e.g. Raya & Hubaux 2007]

	Attack/fault type	Impact	Ease	Mitigation mechanism
Passive	Eavesdropping	Privacy	H	-- current --
Active: DOS	Jamming 1090 MHz channel		M	Adaptive ADS-B transponder
Random	Message collisions			
Active: Deception?	**Ghost aircraft injection**			
Active: DOS	Ghost aircraft flooding			
Random	Surveillance uncertainty			
Active: Deception	Trajectory modification/ aircraft spoofing			

NBC News, 2014