Next Generation Air Transportation System
Joint Planning and Development Office

Workshop 3: Network Enabled Information Access to NGATS Report of Discussion May 3rd 2006

ICNS Conference 2006
2006 NASA ICNS Conference & Workshop
May 1 - May 3, 2006
Hyatt Regency Baltimore On the Inner Harbor
300 Light Street
Baltimore, MD 21202

Workshop Members

- Jim Dieudonne -FAA ATO-P.
- Chris Wargo – CNS
- Chip Meserole – Boeing Company
- Bob Beard – CSC
- Scott Landriau – LMTSS
- John Zuna – Lockheed Martin
- Bob Avjian – LMTSS
- Kevin Harnett – VOLPE
- Vince Rakauskas – VOLPE
- Aniket Bhat - CNS

Workshop Agenda

Net-centric and what it means to the Air-Ground wireless Communication System

- Background — Our Job Today
- Net-centric — NGATS Requirements
- NGATS Challenge — Top Issues for R&D
- Summary Report — Initiatives

Network Enabled Information Access for NGATS

Co-chairs: Chris Wargo, CNS Inc.,
Jim Dieudonne, FAA ATO-P

Overview: SWIM/NEO Activities

Potential WS Focus

Potential discussion Topics:

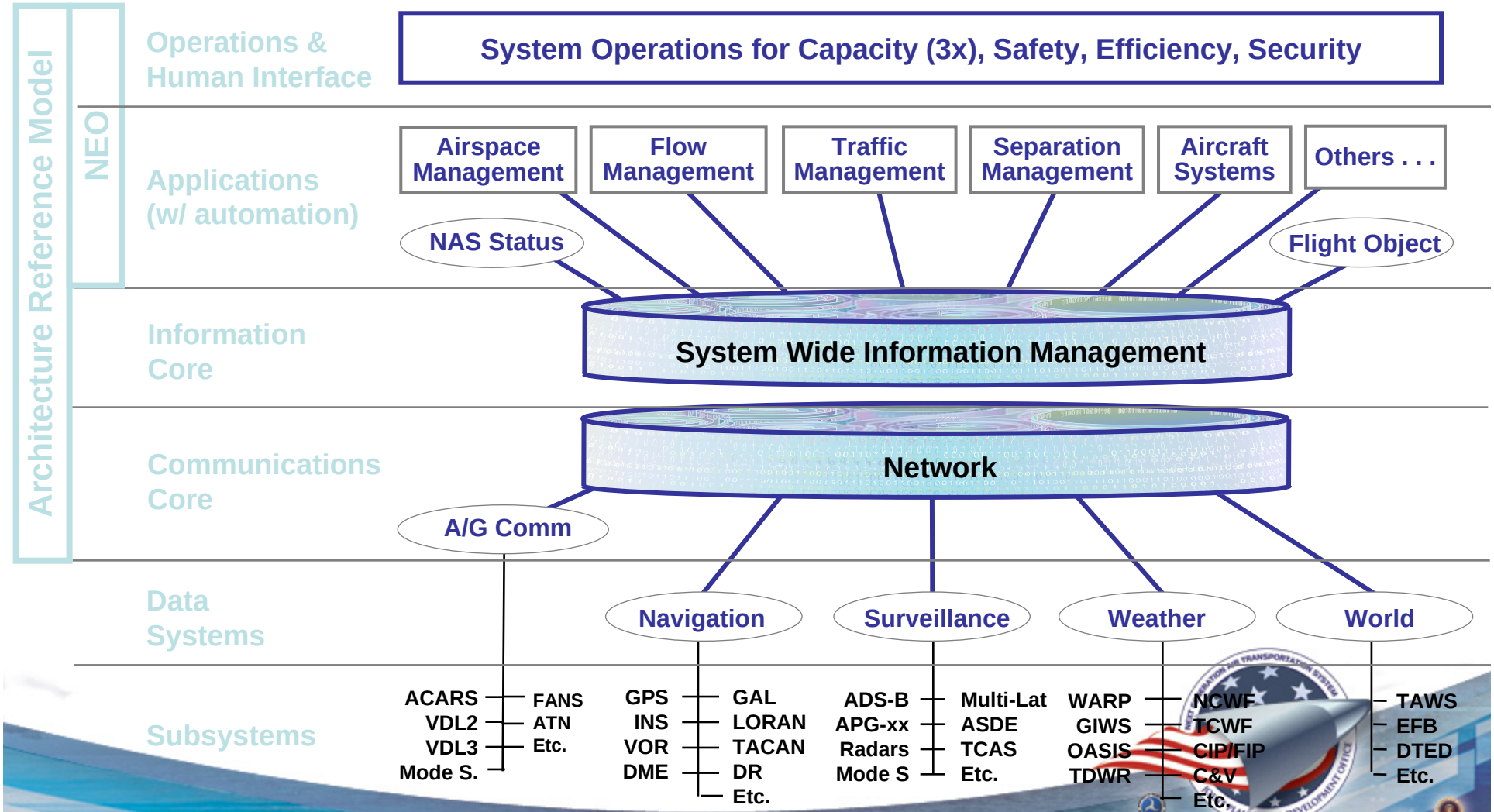
- Network-Centric Information Sharing Architecture Alternatives
- Impact of NEIA on Datalink and Spectrum Requirements
- Next-Generation Air Surveillance and Situational Awareness Needs

Report Issue List

- List the workshop developed research tasks:
  - How will the DoD air-ground link technology be translated to the civil aviation world?
    - Is this the issue, the JPDO should look into?
  - What management capabilities -- for communication, data, and information services -- are needed to support networked enabled operations?
  - What are the most important information services that must be implemented first for an FAA NEO capability?
  - What are we going to do to describe the net-centric security architecture and services?
    - It makes a difference choosing aircraft-centric security vs. net-centric security.
    - Emphasis on cyber security.
    - Requires certification criteria and policies.
    - What information security capabilities are appropriate to support interoperability with other Federal agencies?
    - Is the net-centric concept for JPDO going to force a multi-level security in the NGATS network?
    - How should the services be classified (for security, for safety)?
  - How do you make the air-ground communications implementation (equipage, infrastructure, ownership) cost-effective?
  - Should there be “GIG” for all aviation agencies/stake-holders?
  - Pursue MCNA with FCS requirements?
  - Development of large scale modeling and simulation tools.

The above issue list was developed by participants of the workshop to reflect their key research needs/issues with respect to net-centric architecture communications.

ATM Network Enabled Operations: *Exploiting Shared Precision Information*



Courtesy Boeing – for Workshop use only
Copyright © 2005 Boeing. All rights reserved.

Focus for discussion is Air-Ground

- Workshop Objective:
  - To achieve the vision of NGATS through a Net-centric architecture – what are the key research tasks required in CNS?
- Develop top list of key R&D Issues
  - Description of what is needed

Providers of Talking Points & Issues

- Col. David Rhodes, Chair JPDO SSA IPT
- Dr. Tim Rudolph, ESC
- Dr. Jerry Friedman, JPDO Chief Engineer
- Tom Nyman, MITRE
- Kevin Harnett, Volpe

Global Secure Access to Net Centric Information

Vision:

"Enable the development of an information sharing environment (framework), globally compatible, accessible, and secure when required, that allows Air Transportation System communities of interest to share relevant up-to-the second, accurate, and credible information to make possible informed decision making for routine, planned, or crisis events"

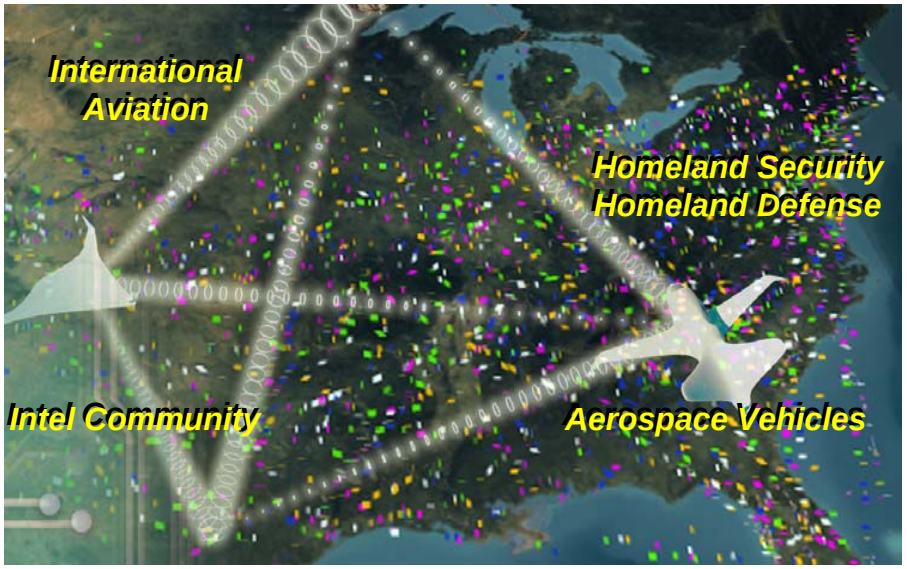
Net Enabled Information Sharing Way Ahead

- Objective: Interoperable, Interagency Net-Centric Architecture
- Leverage:
  - DoD, FAA, DHS, DOC commitments to net-centric architectures
  - Industry initiatives in information technology and spectrum availability
- Opportunity exists ***now*** to synchronize:
  - Data interoperability
  - Compatible network-to-network interface mechanisms
- Jump-Start NEIS FY07 Initiative

NGATS Information Sharing

Requirements

- Quality of Service
  - Priority Sequencing
  - Information Assurance
  - Data Integrity
  - Safety & Security Integration
- Spectrum Availability
  - Broad-area broadband
  - Data
  - Voice
- Weather & Surveillance Infrastructure
- Tailored, responsive, secured according to needs of users



Internodal Network
Terrestrial and Non-Terrestrial Components

Tailored, responsive, secure according to needs of users

Net Enabled Information Sharing Policy Tasks

- Presidential Directive on Air Security Strategy
  - Codify agency roles, authorities, responsibilities
- Information Sharing Council info-sharing governance stds & protocols
- Continuing oversight
- Address privacy and security issues
- Adopt common operating practices, definitions, terminology, interface mechanisms
- Adopt "performance-based" equipage standards (vice system-specific standards)
- Develop multi-layered security distribution processes
- Develop net-centric agency enterprise architectures
- Programming decisions to support NEIS

Presidential

"Define the information sharing environment"

Congressional

"Provide the legislative authorities"

Interagency

"Implement the concept"

Agency

"Execute the Programmatics"

What Can NGATS Learn of Significance from DoD Efforts to Create the GIG?

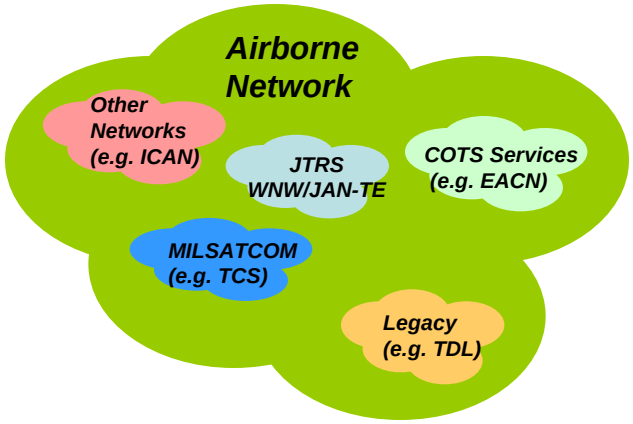
- **DoD strongly believes in the value of *Network Centric Operations* – sharing data and information as widely as possible throughout its life cycle -- consistent with operational security**
  - **Sharing unprocessed sensor date before filtering (low confidence)**
  - **Sharing early situation awareness data before confirmation and integration (intermediate confidence)**
  - **Sharing processed information after fusion, integration, and verification (high confidence)**
- **The first layer in solving this problem is to establish assured and trusted connectivity among all who will share – *the transport***
  - **Wideband CONUS-focused infrastructure build on fiber optic transmission media and "Black Core" economies of scale *(GIG-Bandwidth Extension and Teleport)***
  - **Augmented by COMSATs with advanced IP routing features *(TSAT)***
  - **Extended by radio based technology to the tactical forces *(Joint Tactical Radio System)***
  - **Monitored and serviced via capable distributed network management *(Net ops JNMS)***
- **The second layer is to ensure that information to be shared can be "discovered" and "properly used" by the consumer community -- *consumer focus vice supplier focus***
  - **Understandable definitions, meaning, and context**
  - **Indexing and content tags that make library retrieval less painful**

What Can NGATS Learn of Significance from DoD Efforts to Create the GIG?

- **The third layer is to assist users with "i*nformation agent services*" through "Service Oriented Architectures"**
  - **Core services and standardized shared use mechanisms *(NCES)***
- **And the final layer that impacts all others is "*authority to access*" and the access control mechanisms to protect the info and the system from disruption and compromise**
  - **Need-to-know management**
  - **Cross-classification accesses to help getting the job done**
- **Having identified the "NEED TO DOs" -- *how to make it happen*?**
  - **Governance at the enterprise level is not well understood and making things happen in an appropriate way has been difficult**
  - **Directives, policies, and procedures are NECESSARY BUT NOT SUFFICIENT – need incentives and a technical framework that frames the solutions but does not overly prescribe the solutions**
  - **A minimum essential set of standards at the core framework level are essential -- other emerging standards can ride on as they compete and evolve**

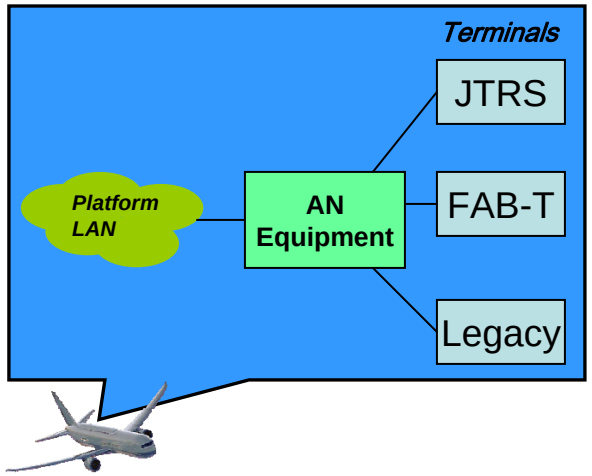
Airborne Network is more than a new link technology

Enterprise Networking Capability



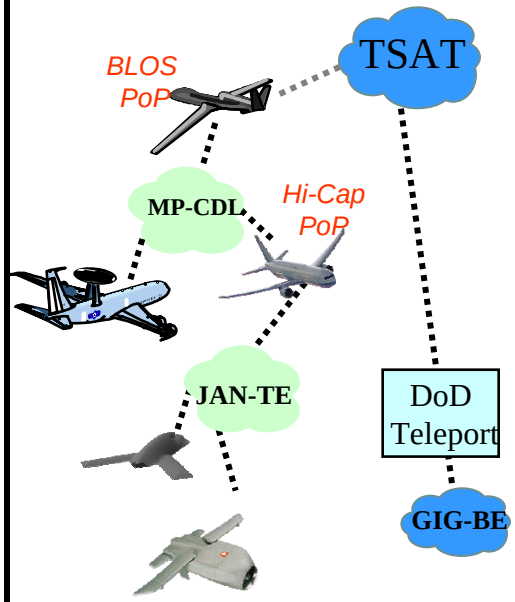
- AN provides network connectivity as a network of networks
- AN provides not only network connectivity, but also IA, network management, network services (e.g., DNS) and network planning overlays

Platform Capability



- AN provides single network service delivery point for platforms with multiple radios
- AN provides guidance and standards for platform LAN implementations
- Potential for common product acquisition

Infrastructure Capability

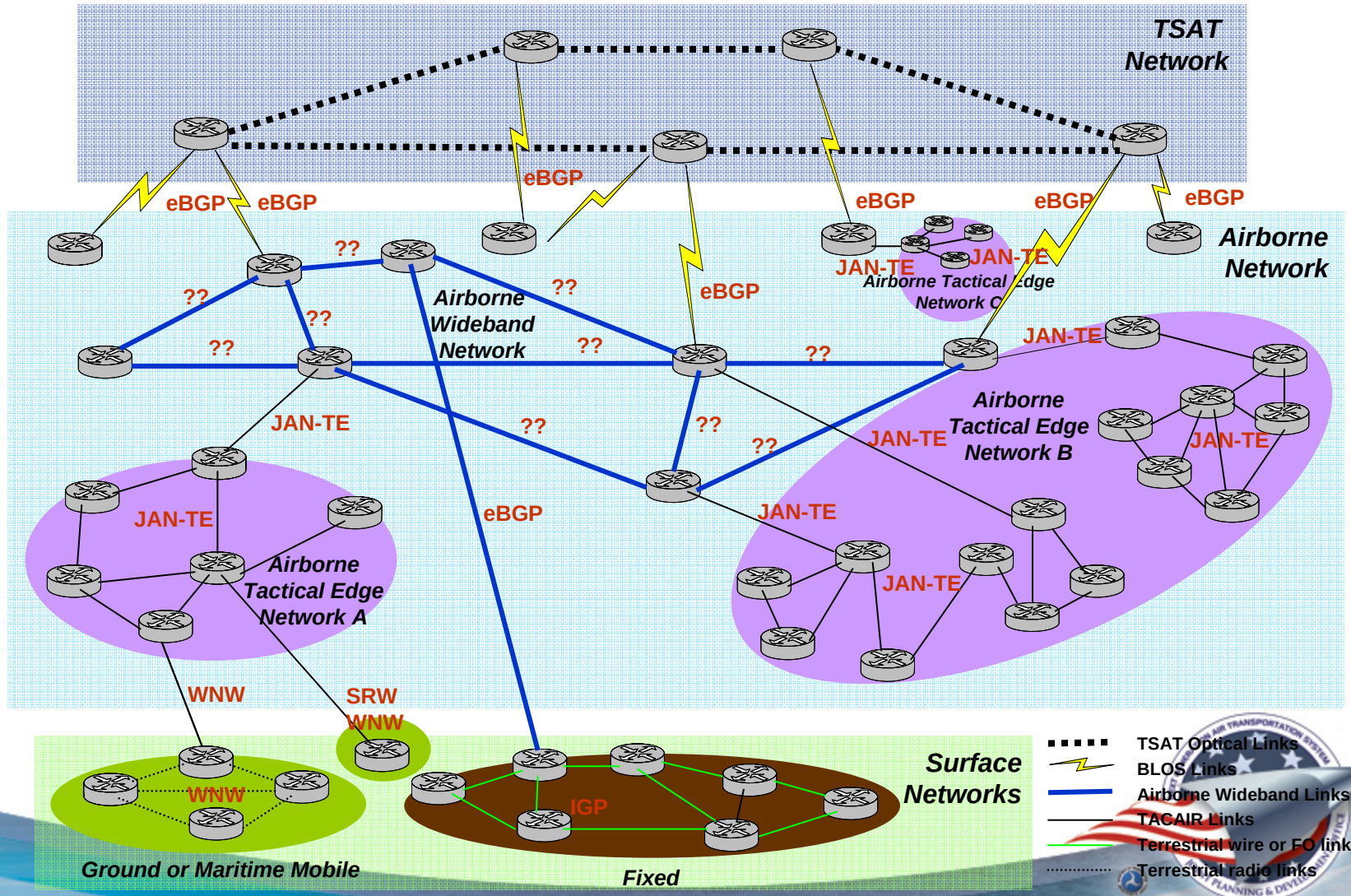


- AN provides infrastructure products to extend network service
- AN provides standard packages for BLOS and/or Hi-Capacity Airborne Points-of-Presence

Assumptions Made for Internet Links Do Not Apply to AN Links

Link Attribute	Terrestrial Internet	Airborne Network	Networking Impacts
Bandwidth	Infinite – can add more fiber and routers as needed	Constrained by available spectrum in a geographic region Function of distance, antenna gain, power levels, interference	Routing performance
Bit Error Rate	10^{-9} to 10^{-12}, fairly constant	10^{-5} to 10^{-7}, highly variable due to distance, fading, EMI	End-to-end reliable transport
Stability	Generally long periods (days) of availability	Short periods (minutes, seconds) of availability the norm	Routing performance (convergence)
Threat	Generally few (e.g., backhoe)	Highly exposed to EMI and intentional jamming	Network capacity
Directionality	Bidirectional	May be unidirectional (e.g., different power levels) Receive-only nodes	Protocol algorithms
Latency	Constant based upon link length	Variable over time as link length changes	Synchronized applications

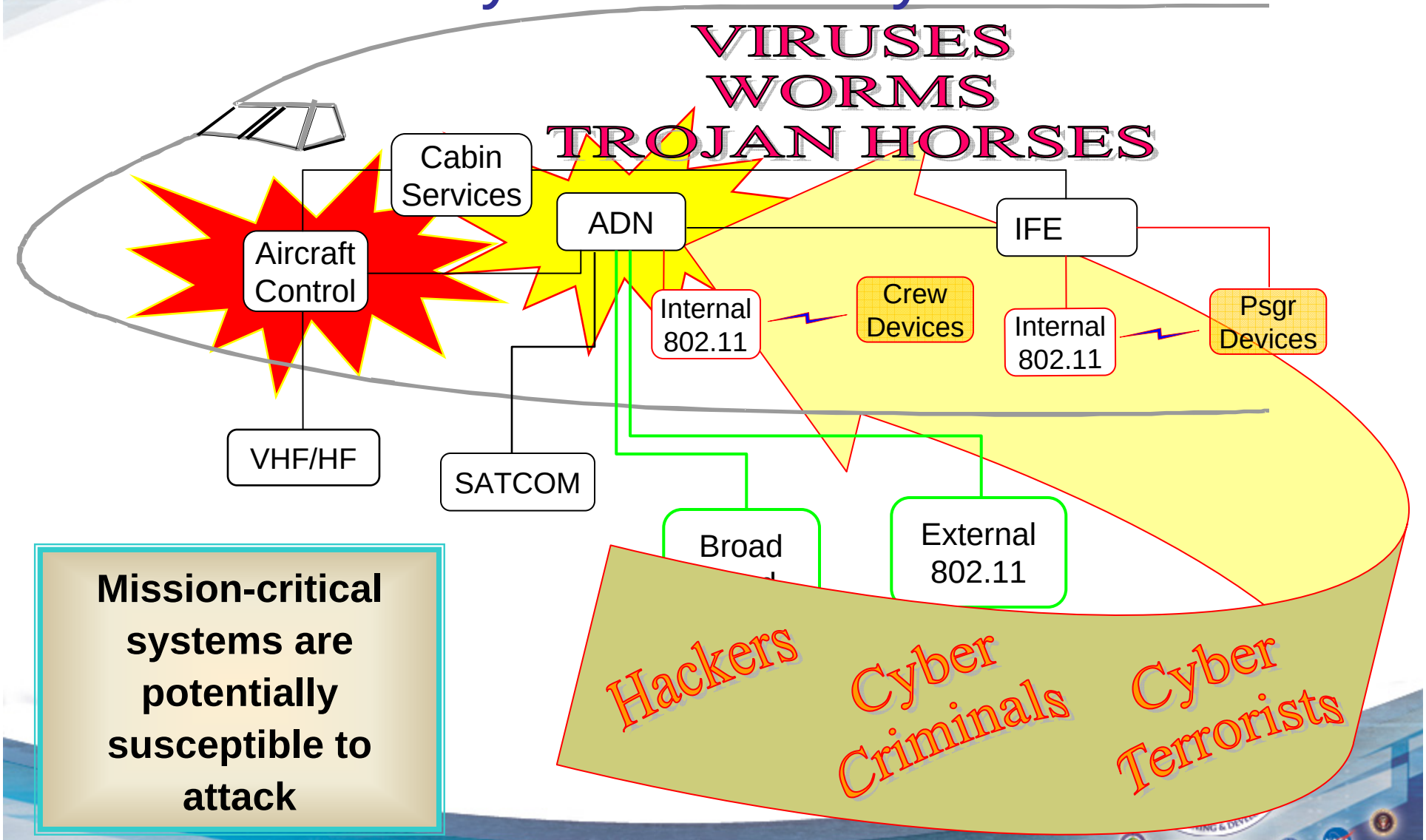
Integration of Mobile and Static Autonomous Systems - Routing



Issues from JPDO Chief Engineer

- What information security capabilities are appropriate to support interoperability with other Federal agencies?
- What management capabilities -- for communication, data, and information services -- are needed to support networked enabled operations?
- What are the most important information services that must be implemented first for an FAA NEO capability?

ADN Cyber Security Issues



Mission-critical systems are potentially susceptible to attack

ADN Cyber Security Issues

- **These cyber security vulnerabilities are not only new but have not been anticipated.**
- **Since it has not been a concern in the past, the existing Code of Federal Regulations does not specifically address cyber security vulnerabilities**
- **Consequently, there are no existing Policies, Certification Criteria or Procedures that provide assurances that cyber security vulnerabilities will not cause unsafe flight conditions**
- **Cyber security vulnerabilities in the ADN will be irrevocably bound to the safety of flight.**
- **Unmitigated, these vulnerabilities will have a definite negative effect on the safety of flight.**

Workshop Discussion

- Group exercise – establish subgroup of interest
- Short breakout and reports