



Secure Mobile Networking Virtual Mission Operations

Phillip E. Paulsen

Project Manager: Secure Network Centric Technologies

NASA Glenn Research Center

August 24th, 2004



What is the TCA?



- The **Transformation Communications Architecture (TCA)** is a joint DoD / NASA communications concept that aims to provide an unprecedented level of data integration across a wide variety of platforms (i.e. network centric operations)
 - **Seamless integration of terrestrial, shipboard, airborne, and space-based assets**
 - Conventional Internet Protocols (IP) will be the glue that ties the network together
 - Allow secure, autonomous, shared, distributed tasking and data handling
 - On-the-fly response to real-time events (predictive analysis versus post analysis)
 - Allow field access to sophisticated systems by “unsophisticated” users
 - NASA’s “farmer in the field”, DoD’s “warfighter”
 - Designed specifically to minimize infrastructure costs
 - Use of common interfaces and open standards for all platforms and infrastructure
 - Use of low cost, commercial devices / shared infrastructure to collect and disseminate data
 - Built-in platform flexibility to accommodate future changes in the state-of-the-art
 - Built-in system transparency to eliminate the need for extensive user training and minimize the number of “people in the loop” to configure and maintain systems

The FAA is a key member of the TCA consortium



Why Change the NAS?



- The FAA seeks a consistent and single point of entry to publish and subscribe to NAS data (System Wide Information Management [SWIM])
 - SWIM will replace a number of existing focus networks
 - **SWIM will provide context-sensitive information to the NAS elements that require it**

To the Cockpit:

- Flight objects (flight plan support from pre-flight to post-flight)
- Aeronautical information (PIREPS, NOTAMS, dynamic flight constraints, NAS status, etc...)
- Real time route and weather information
- Surveillance data objects (situational awareness, cockpit-based separation, virtual traffic management, and dynamic re-sectorization)
- SWIM may also accommodate:

To the Ground:

- In-flight maintenance data
- “Virtual” black box data
- Real time voice and video to assess current status and intent
- **SWIM will also need to interoperate with systems fielded by other countries and the DoD**



Why Change the NAS?



- Following the **September 11th** attack on the United States, **issues with the current data systems** were uncovered:
 - **Disaster coordination was largely a distributed activity**
 - Major events were spontaneous and generally confined to a single region
 - No central control authority (to counter a coordinated attack) was needed or envisioned
 - Data exchange from region to region and agency to agency was stymied by the **lack of available infrastructure and incompatibility of systems**
 - Generation of a **common operational picture and coordinated defense** were accomplished largely **through voice communications**
 - Prior to September 11th continental United States air defense systems were positioned along our borders to cover the air space from the shoreline to 250 miles outward
 - The events of September 11th created a sudden military need to cover the airspace over the United States as well (i.e. CONUS combat air patrol)
 - The USAF had to rush scientists, engineers, equipment, and radar fusion software to the Air Defense Sector Operations Centers to **integrate military and FAA data for real-time situational awareness of all air traffic in the United States**



A Network Centric NAS?



- A network centric NAS represents a fairly radical departure from today's systems:

Today

- **Highly optimized, voice-driven, stove-piped operation with dedicated ground stations**
- Limited throughput
- Security through obscurity
- Limited interoperability / no common operational picture
- Dedicated infrastructure
- Unique equipment and custom software

Tomorrow

- **Shared operations through common, integrated, networked communications path**
 - Mix of government and commercial ground stations
 - Air-to-ground, air-to-air, or air-to-satellite links based on performance, cost, and availability
 - Autonomous fault detection, isolation, & recovery
- High performance links and improved throughput
- Security through established Government standards (NSA's HAIPIS)
- Seamless interoperability and common operational picture
 - Ability to share voice, video, and data between any and all
 - Survivable, central command authority with links to the DOD, USCG, FBI, CIA, Secret Service, and foreign governments
- Shared Infrastructure, autonomous service on demand
- Affordable, common equipment, software, and services



TCA Lessons Learned



- For the Future NAS to succeed a number of key architecture requirements must be addressed:
 - All systems must be **seamlessly integrated**
 - Eliminates the inclusion of proprietary systems
 - AT&T and Sprint drive the boat
 - IPv6 has been selected as “the” protocol for the new, integrated architecture
 - Issues with IPv4 interoperability and mobility need to be nailed down
 - Architectures must be highly **scalable**
 - Thousands of mobile users
 - Architectures must offer **high system assurance**
 - Availability, integrity, authentication, confidentiality, auditing, countermeasures, and non-repudiation
 - Architectures must offer **high availability**
 - 99.99xxx?
 - Architectures must support a large user population with **highly diverse needs**
 - US command authority, ATC, pilots, foreign ATC, FBI, civil aviation, USCG, etc...
 - Architectural elements must be designed to allow future **reprogrammability** to keep up with changes in the SOA
 - Drives the need for software-based devices
 - Creates issues with configuration management
 - **The integrated system** must be **survivable and compromise tolerant**
 - Individual system attacks or failures must not promulgate throughout the system
 - **Security** will involve **national and international partners**
 - Systems will need to be designed end-to-end (networks and security cannot be decoupled)
 - Protocol conversions / performance enhancing proxies cannot be used
 - NSA’s HAIPIS comes in 3 strengths: Type 1 (TS), Type 2 (S), & Coalition
 - Depending on the task, all three strengths will need to be incorporated into the design



The Future NAS Customer Base



- Who are the **technology customers**?
 - GA aircraft
 - Commercial airframes
 - Airlines (domestic and foreign)
 - Commercial service providers (domestic and foreign)
 - Government (civilian and military) aircraft
 - Civilian Air Traffic Controllers
 - Military Air Traffic Controllers
 - Foreign Air Traffic Controllers
 - US Command Authority
 - Coalition partners

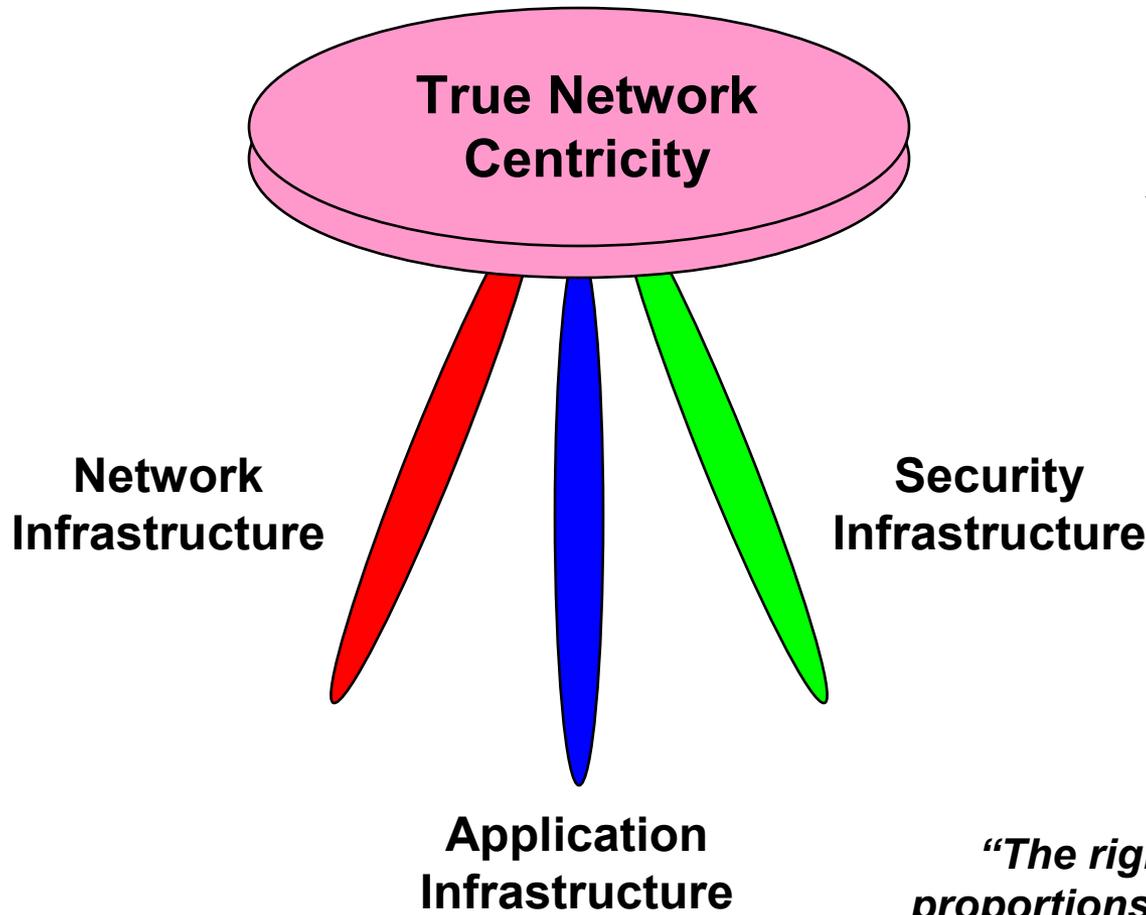
- What are their **primary drivers**?
 - **System cost / economic viability**
 - System complexity
 - Infrastructure availability
 - Interoperability
 - Security
 - Scalability
 - Data types
 - Data rates
 - Politics
 - Policy / doctrine

Anything that flies or communicates with or monitors things that fly



Secure Mobile Networking

The Network Centric Interdependence Triad



Policy



Culture

“The right elements, in the right proportions, built correctly to the right plans, and used in the most effective way”

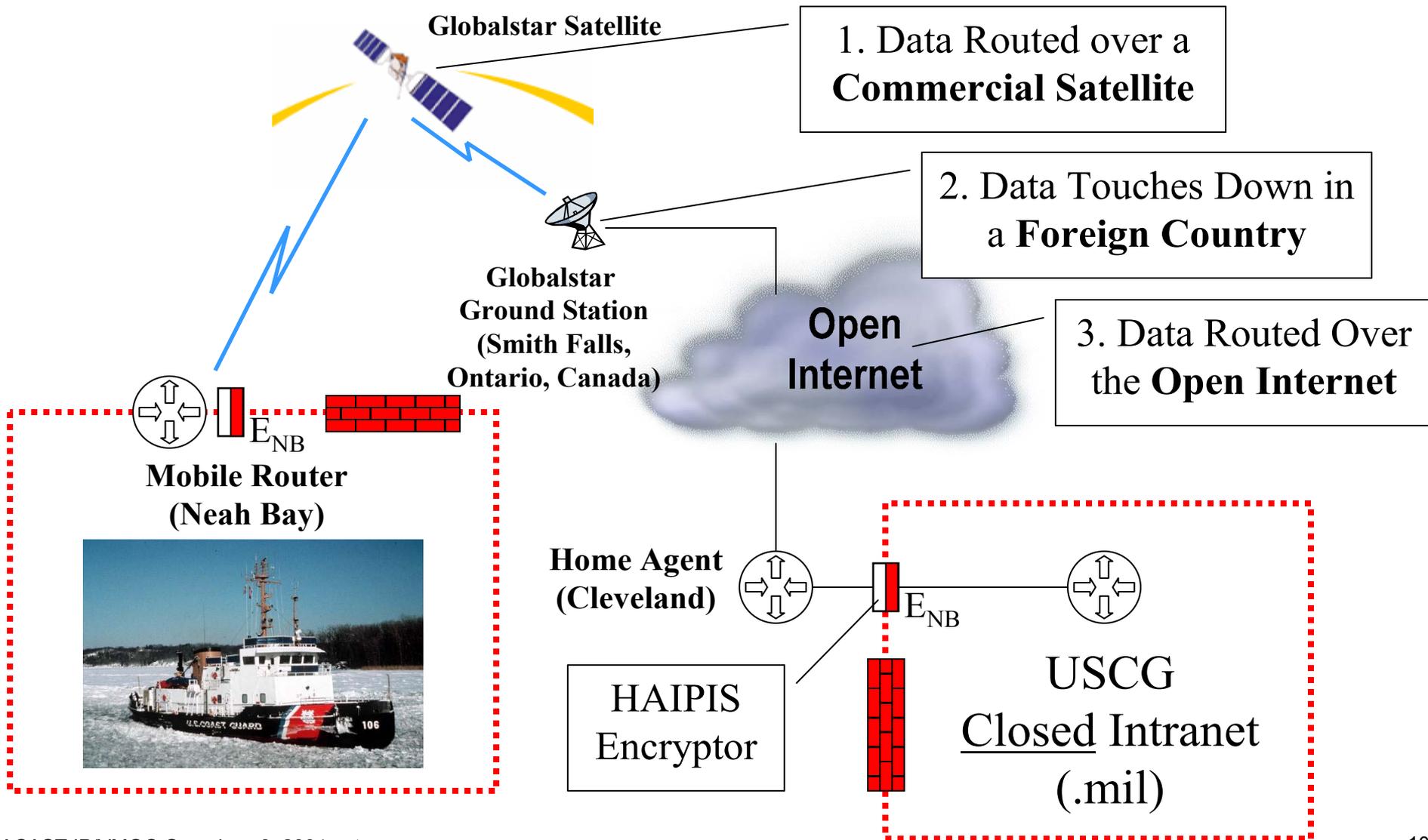


Neah Bay Secure Mobile Networking Demo





Neah Bay Satellite Communications Path





- VMO provides a framework (a common way of doing business) for mission partners to define, test, validate, and field an IP-based command and control system capable of supporting secure, distributed mission operations of any IP-based platform or sensor
 - NSA Approved **Autonomous Intrusion Detection and Countermeasures**
 - External **Session Scheduling**
 - Electronic Certificate Control
 - External User **System Access Control**
 - **Biometric-based User Authentication**
 - Data Encryption
 - User Prioritization and Contention Control
 - Internal User Command Access Control
 - Biometric-based Command Authorization Checks
 - **Command Verification and Appropriateness Checks**
 - **Command Prioritization and Queuing**
 - Command Archive (User **Non-Repudiation**)
- VMO is truly “virtual” and can be housed in any location that has sufficient network bandwidth (e.g. fixed & mobile sites, trucks, aircraft, ships, spacecraft, etc...)
- VMO is **platform independent** and can be used by any IP-compliant device (satellites, aircraft, ships, etc...)



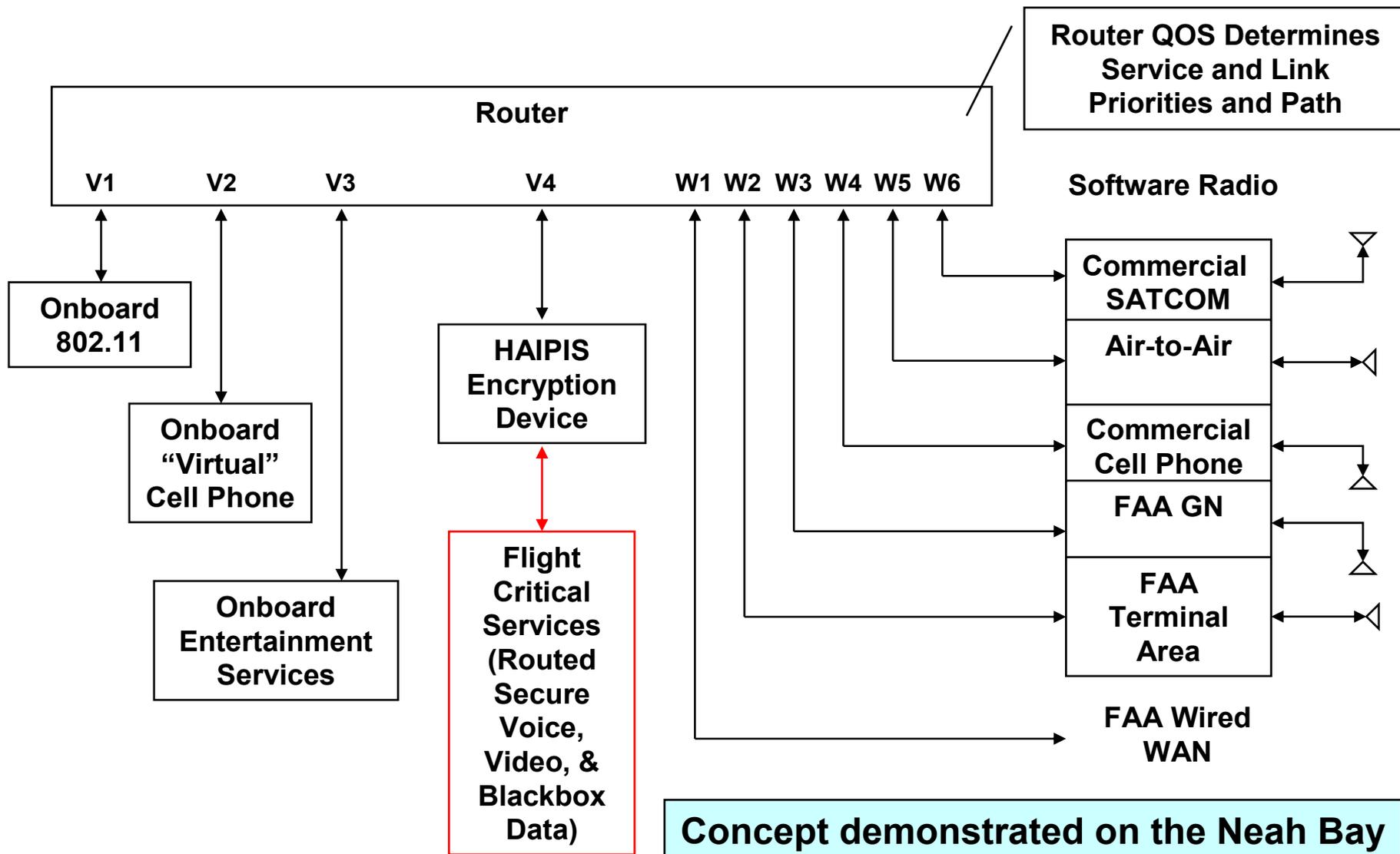
Virtual Mission Operations Field (Cockpit and ATC) User Interface



- JAVA-based (utilizes a generic web browser for access)
 - Truly “virtual”, **no mission unique software on-board the aircraft**
 - Nothing to steal or compromise post-session
 - **Survivable** system which includes **multiple, mirrored command elements**
- **Cockpit** user provided with **information keyed to GPS location**
 - Local terrain
 - Weather
 - Traffic
- **ATC** user input defines **area of interest**
 - Position and velocity of moving objects at infinite granularity levels
 - Changes over specified time period
 - Ad hoc warning messages based on real time events
 - Virtual black box data
 - Virtual manifest data
 - Handoff points / times (positive control assurance)



Future NAS Onboard Network Architecture

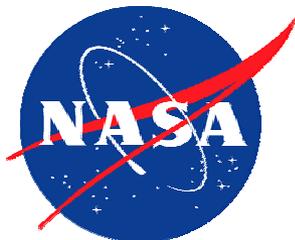




IP Compliant Satellite Experiment

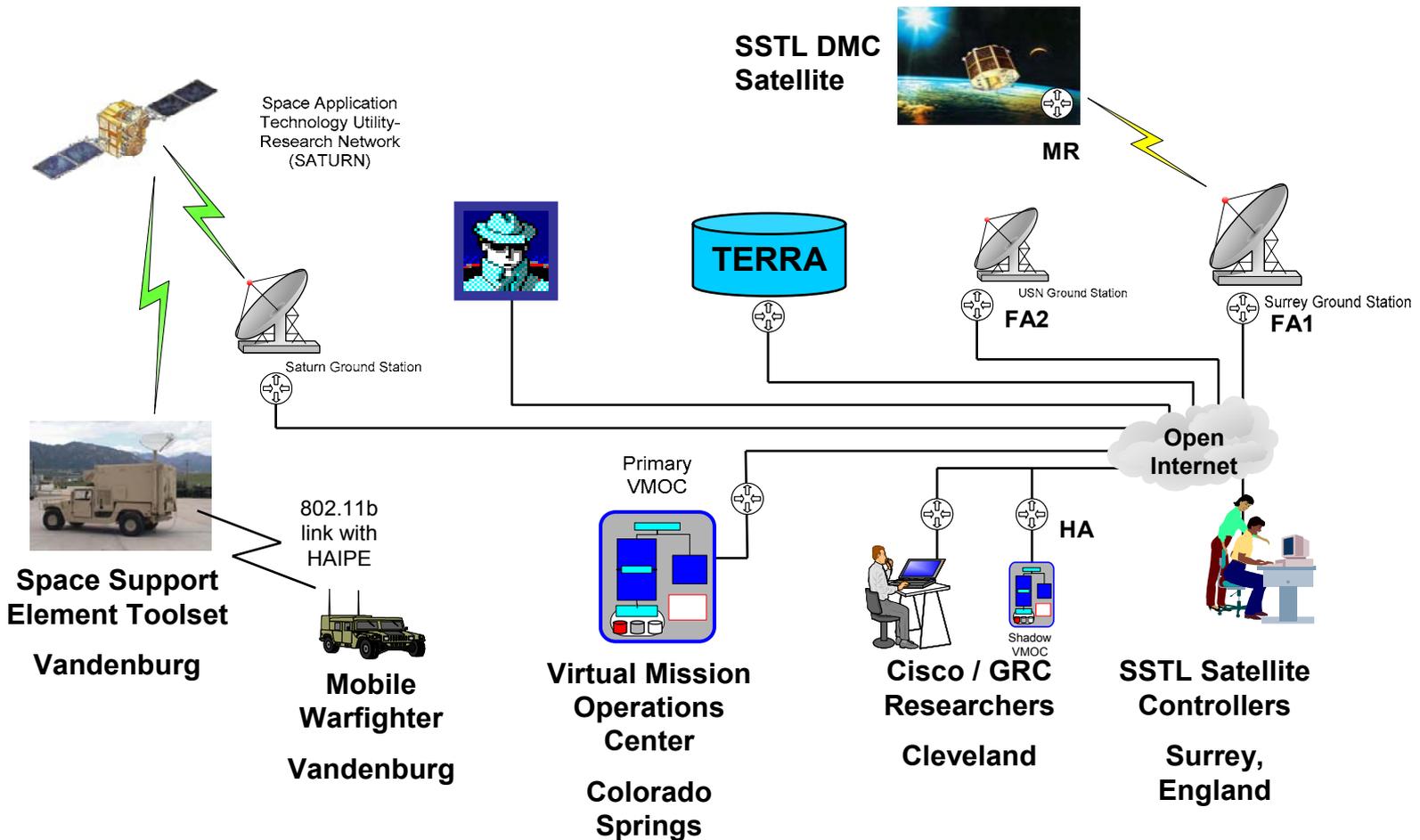


- NASA
- OSD C3I (RAI-NC)
- 14 Air Force (14 AF)
- Air Force Space Battlelab (AF SB)
- Army Space and Missile Defense Battle Lab (SMDBL)
- 50 Space Wing (50 SW)
- National Security Agency (NSA)
- Space and Missile Center (SMC) / CERES
- Naval Research Lab (NRL)
- Cisco
- General Dynamics
- Western DataCom





CLEO / VMOC Demonstration



This demonstration will be re-performed in the Metro D.C. area later this Fall



Summary / Way Forward



- A strategic plan must be formulated which takes into account everything that has been learned:
 - The Future NAS will be packet-based
 - The Future NAS will be fully interoperable with commercial, military, and foreign systems
 - The network solution will apply to all phases of aircraft operations (not just flight)
 - The network solution will apply to all types of aircraft (not just commercial aircraft)
 - The security solution cannot be decoupled from the network solution
 - Generic data (voice, entertainment, email) will commingle with data from secure systems
- NASA GRC is interested in developing a comprehensive, secure, scalable, survivable, mission operations system
 - Bandwidth considerations will need to be integrated into the security solution
 - We will need to understand exactly what can be flown with all sources of overhead
 - A demonstration incorporating all elements of aircraft operations (gate-to-gate plus anomalies) would be useful for establishing a future baseline architecture
 - Tools, techniques, and policies will all need to be developed and proven as a part of the demonstration
 - A sound business case will also need to be developed (the business case should speak to the estimated costs that will be incurred by all)
 - General aviation, commercial aviation, etc...
 - Path to system certification identified and costed



Contact Information



Phillip E. Paulsen
M.S. 54-6
NASA Glenn Research Center
21000 Brookpark Road
Cleveland, Oh 44135
Phone: (216) 433-6507
E Mail: phillip.e.paulsen@grc.nasa.gov

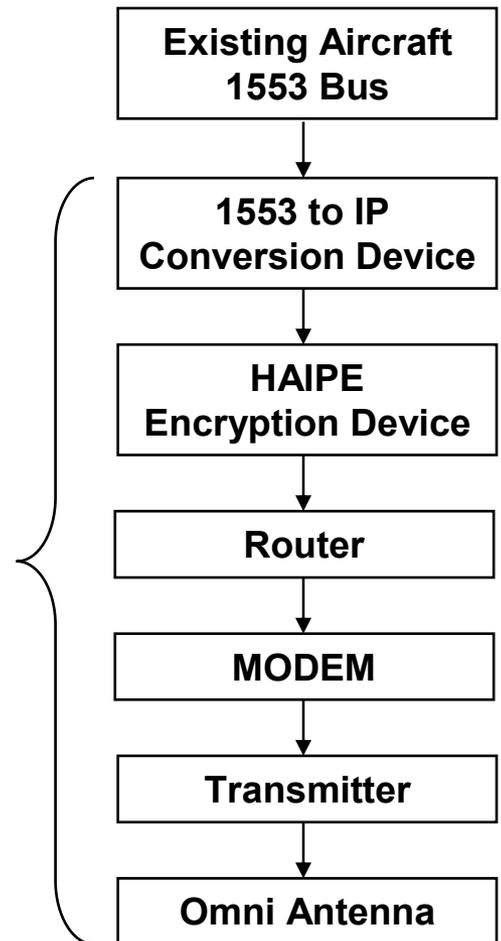
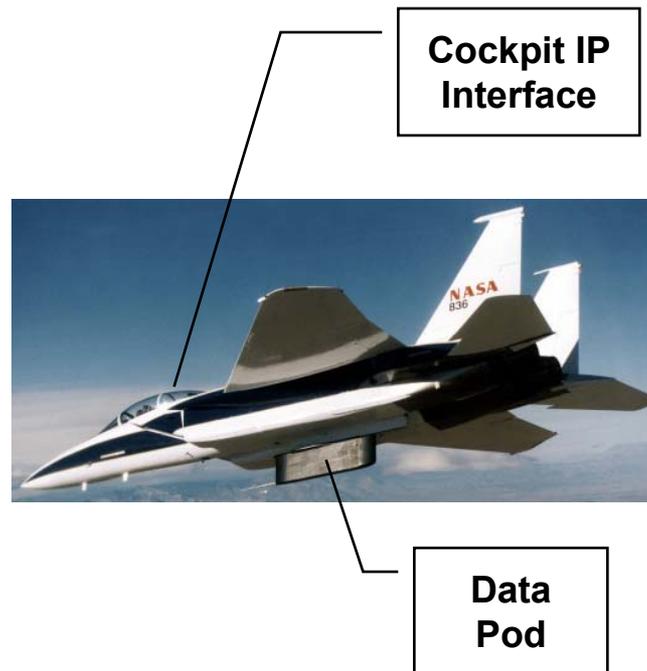
Publications

<http://ctd.lerc.nasa.gov/5610/repubs.html>
http://roland.grc.nasa.gov/~ivancic/papers_presentations/papers.html
<http://siw.gsfc.nasa.gov/agenda.html>



Backup Charts

- **Continuous 20 Hz, 16 bit data (1553-to-IP conversion) ~6 kbps**
 - Aircraft roll, pitch, and yaw rate
 - Aircraft angle of attack
 - Aircraft angle of side slip
 - Atmospheric static pressure
 - Atmospheric dynamic pressure
 - Atmospheric static temperature
 - Aircraft control surface positions
 - Aircraft control commands
 - Aircraft throttle commands
 - Aircraft engine parameters
 - Aircraft control system parameters
 - Aircraft temperature indications
 - Aircraft fuel state
 - Aircraft weapons state
 - Aircraft altitude
 - Aircraft attitude
 - Aircraft heading
 - Aircraft velocity vector
 - Aircraft position information
- **As needed (commanded)**
 - Aircraft manifest data / souls
 - Cockpit voice communications (VOIP 11 kbps)
 - Cockpit / cabin video (full motion MPEG 2: 5-9 Mbps)



Note: enroute updates, and weather information are flowed up to the aircraft

- First generation Cisco 3240 mini-router specs:
 - Two or three 4" x 4" PC-104 compliant cards.
 - 1 router card, up to 2 I/O cards
 - 5 VDC, 10W
 - 1 powered aux (GPS type RX)
 - Commercially available
 - Qualified for space in CY'03
 - Dual 100BaseT Fast Ethernet ports on main router card (one exclusively for the PCI backplane)
 - PCI backplane connects to a maximum of 2 four port 10/100 Ethernet switch or four port serial cards in any combination
 - Maximum of 200 Mbps integrated, duplex throughput (processes a maximum of 50,000 packets/second, 64 byte packets [theoretical])
 - Generic IPSEC encryption
 - Currently flying aboard military transport aircraft





Network Encryption Hardware

- Western DataCom's NSA COMSEC compliant packet encryption devices. Specs:
 - IPE-10M Type 2 IPsec HAIPE.
 - PC104 based
 - 10 Mbps
 - 2 PC-104 plus cards
 - Commercially available Sept. 2002
 - IKE: pre-placed keys
 - Supports the next generation of Type-2 encryption algorithms for 2003 NATO and Coalition partners
 - KIVxx Type 1 IPsec HAIPE
 - 1 Gbps
 - Firefly key management
 - 3 PC-104 plus cards in Type 1 tempest chassis
 - Commercially available August 2005

