Use of Virtual Mission Operations Center Technology to Achieve JPDO's Virtual Tower Vision

William D. Ivancic
216-433-3494
wivancic@grc.nasa.gov
NASA Glenn Research Center
21000 Brookpark Road
Cleveland, OH 44135

Phillip E. Paulsen
216-433-5607
Phillip.E.Paulsen@grc.nasa.gov
NASA Glenn Research Center
21000 Brookpark Road
Cleveland, OH 44135

Abstract—The Joint Program Development Office has proposed that the Next Generation Air Transportation System (NGATS) consolidate control centers. NGATS would be managed from a few strategically located facilities with virtual towers and TRACONS. This consolidation is about combining the delivery locations for these services not about decreasing service. By consolidating these locations, cost savings in the order of $500 million have been projected. Evolving to spaced-based communication, navigation, and surveillance offers the opportunity to reduce or eliminate much of the ground-based infrastructure cost. Dynamically adjusted airspace offers the opportunity to reduce the number of sectors and boundary inconsistencies; eliminate or reduce "handoffs;" and eliminate the distinction between Towers, TRACONS, and Enroute Centers. To realize a consolidation vision for air traffic management there must be investment in networking. One technology that holds great potential is the use of Virtual Mission Operations Centers to provide secure, automated, intelligent management of the NGATS. This paper provides a conceptual framework for incorporating VMOC into the NGATS.

TABLE OF CONTENTS

1. Introduction

The Joint Program Development Office (JPDO) has proposed that the Next Generation Air Transportation System (NGATS) consolidate control centers. NGATS would be managed from a few strategically located facilities with virtual towers and TRACONS. Thus, what JPDO has proposed is basically movement of the current air transportation system from a circuit-base, voice-based, manual control system to a fully network centric system using netcentric operation concepts [1].

FAA is currently working some of these issues for ground-based communication under the System Wide Information Management (SWIM) program. However, SWIM does not currently include mobile operations to the aircraft or support for unmanned aerial vehicles – although that is being considered for the future [2].

The following are some key features that network centric solutions regarding mobile network technology that need to be considered for future communication systems.

- **Interoperability**
  - Is the new network fully interoperable with existing open standards (IETF)?
- **Scalability**
  - Will the technology that works on a single vehicle also work on many?
- **Survivability**
  - Can one still maintain network connectivity, even if a primary data

path fails?

- **Mobility**
  - Can one maintain network contact with something in motion without the need for manual reconfiguration?
- **Transparency**
  - Can one field a mobile network that is truly "set and forget"?
- **Security**
  - Can one securely cross multiple domains (i.e. open, closed, government, etc…)?
- **Use of Shared Infrastructure**
  - Can one take advantage of low cost (open) network infrastructure? (The ability to share network infrastructure enable dramatic cost reductions and system flexibility.)

2. Virtual Mission Operations Center

Requirements

Some of the original Virtual Mission Operations Center (VMOC) concepts beginnings can be traced to NASA's Glenn Research Center. Glenn Research Center worked collaboratively with General Dynamics Advanced Information Systems[1]to demonstrate secure command and control of space assets at NASA Johnson's Inspection 99 and 2000. After receiving feedback form mission and operations specialists at the NASA Johnson Space Center's Mission Control Center, requirements for generic mission operations were developed. These generic requirements are:

- Enable system operators and data users to be remote
- Verify individual users and their authorizations
- Establish a secure user session with the platform
- Perform user and command prioritization and contention control
- Apply mission rules and perform command appropriateness tests
- Relay data directly to the remote user without human intervention
- Provide a knowledge data base and be designed to allow interaction with other, similar systems
- Provide an encrypted gateway for "unsophisticated" user access (remote users of science data)

VMOC Defined

A Virtual Mission Operations Center (VMOC) can be defined as a framework for providing secure, automated command and control, resource management, data mining, machine-to-machine communications and access to an asset or assets by remote users using Internet technologies.

A VMOC may also include the following features: intrusion detection, survivability and redundancy, accounting and data mining. Intrusion detection ensures that malicious users have not gained access to the system. Intrusion detection may also entail deployment of countermeasures to ensure system integrity.

The VMOC may also be designed to ensure survivability and redundancy. There may be a number of VMOCs, geographically separated and networked in such a manner that if one VMOC goes off-line a secondary VMOC can immediately take over. Effectively, this is failover to a geographically-separated hot standby. Such geographically separated systems are directly in line with JPDO's consolidated control center concept.

The VMOC may implement an accounting mechanism in order to keep track of a customer's use of the resources for auditing or billing purposes.

Finally, a VMOC may offer data-mining services. With regards to the NGATs, data mining services directly correspond to the SWIM concept of publish and subscribe. Here data such a aircraft location, passenger lists, destinations, security information, flight plans, weather information, turbulence information,

[1] General Dynamics Advanced Information Systems acquired Veridian Information Solutions, a leading network security vendor for the intelligence community, in August 2003, along with Veridian's Nautilus Horizon software.

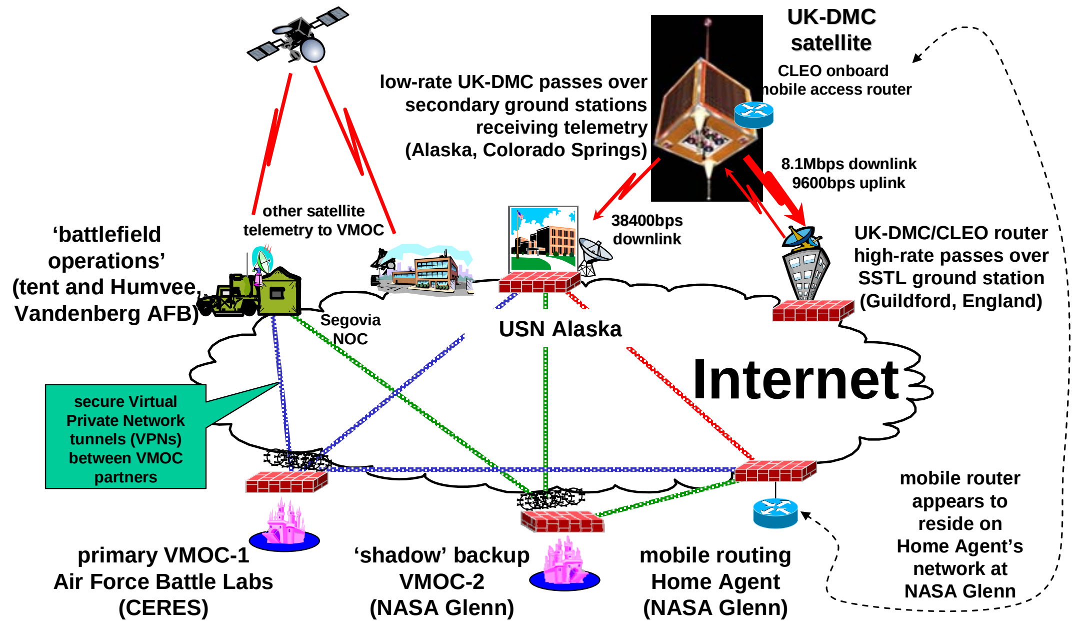

UK-DMC satellite
CLEO onboard
obile access router
low-rate UK-DMC passes over secondary ground stations receiving telemetry (Alaska, Colorado Springs)
8.1Mbps downlink
9600bps uplink
other satellite telemetry to VMOC
38400bps downlink
'battlefield operations' (tent and Humvee, Vandenberg AFB)
UK-DMC/CLEO router high-rate passes over SSTL ground station (Guildford, England)
Segovia NOC
USN Alaska
Internet
secure Virtual Private Network tunnels (VPNs) between VMOC partners
mobile router appears to reside on Home Agent's network at NASA Glenn
primary VMOC-1 Air Force Battle Labs (CERES)
'shadow' backup VMOC-2 (NASA Glenn)
mobile routing Home Agent (NASA Glenn)

Figure 1 - Real World VMOC Deployment

maintenance records, etcetera can be access from virtual storage facilities. Of course, ownership and privacy issues will have to be addressed regarding the access provided by any database service.

3. VMOC Real World Experience

NASA Glenn collaborated with Cisco Systems, General Dynamics, the Air Force, the Army Space and Missile Battle Labs, Surrey Satellite Technology Limited (SSTL), Universal Space Networks (USN), the Office of Secretary of Defense and others to demonstrate space-based netcentric concepts and real-time command and control of a space-based asset. A VMOC base on General Dynamics Nautilus Horizon product provided a framework for the mission partners to define, test, and field an IP-based command and control system capable of supporting secure distributed mission operations of any IP-based platform or sensor. This VMOC provided a path for the rapid development and demonstration of new technologies within the relevant environment [3, 4].

The VMOC tied remote space operators directly to an orbiting spacecraft via the open Internet through a Web environment. The VMOC was implemented as a geographically distributed, dual, hot-standby operations center. The primary VMOC was located at the Center for Research Support (CERES) on Schriever Air Force Base, CO, with the backup VMOC located at NASA's Glenn Research Center (GRC) in Cleveland, Ohio. With the satellite ground stations tied to the Internet, the VMOCs are the control elements that orchestrate the tie between the user and the spacecraft. This VMOC has continued spiral development to enhance system interoperability and responsiveness, enhance situational awareness, facilitate "system of systems" solutions, and support automated machine-to-machine interactions.

This master VMOC used Internet Protocols to acquire satellite data, dynamically task satellite payload, and perform telemetry, tracking and control (TT&C) of on-orbit satellite assets. The VMOC performs a number of functions:

(1) Enables system operators and data users to be remote from ground stations
(2) Verifies individual users and their authorizations
(3) Establishes a secure user session with the platform
(4) Performs user and command prioritization and contention control
(5) Applies mission rules and performs command appropriateness tests
(6) Relays data directly to the remote user without human intervention
(7) Provides a knowledge database and is designed to allow interaction with other, similar systems
(8) Provides an encrypted gateway for "unsophisticated" user access (remote users of science data)

Security Manager

The security management concept is illustrated in figure 2. Access to the VMOC was controlled and monitored for intrusion with a "defense-in-depth" strategy. Autonomous network intrusion detection and countermeasures were conducted using the Automated Security Incident Measurement (ASIM) intrusion detection system and the Common Intrusion Detection Director (CIDD). Both ASIM and CIDD were developed by General Dynamics for the Air Force Information Warfare Center, and they are used routinely by most Department of Defense (DOD) bases to mitigate the network risks associated with hackers (external to the monitored connections) and saboteurs (internal to the monitored connections).

For the June 2004 demonstration, the remote user was authenticated via user name and password. Additional VMOC authentication is planned using technologies such as biometrics and DoD common access cards (CAC). Each user was assigned a priority and ordered by priority in the VMOC's database. Priorities were demonstrated for command and control. A high-priority user's request preempts a lower priority user request. In addition, the database included information to determine what authorizations specific users possessed. For example, one user may be able to request a stored image whereas another may actually be authorized to command the system to take an image.

Redundancy and Survivability

The VMOC is designed for survivability by utilizing multiple mirrored, geographically separated VMOCs. The demonstration used two VMOCs, with the primary VMOC located

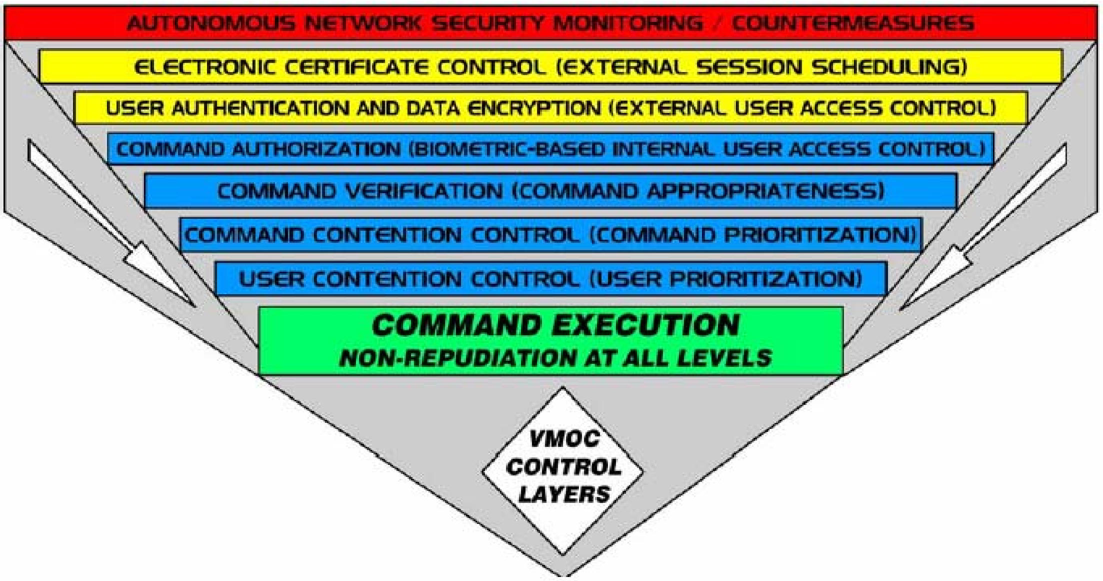

AUTONOMOUS NETWORK SECURITY MONITORING / COUNTERMEASURES
ELECTRONIC CERTIFICATE CONTROL (EXTERNAL SESSION SCHEDULING)
USER AUTHENTICATION AND DATA ENCRYPTION (EXTERNAL USER ACCESS CONTROL)
COMMAND AUTHORIZATION (BIOMETRIC-BASED INTERNAL USER ACCESS CONTROL)
COMMAND VERIFICATION (COMMAND APPROPRIATENESS)
COMMAND CONTENTION CONTROL (COMMAND PRIORITIZATION)
USER CONTENTION CONTROL (USER PRIORITIZATION)
COMMAND EXECUTION
NON-REPUDIATION AT ALL LEVELS
VMOC CONTROL LAYERS

Figure 2 - Security Management Concept

at CERES in Colorado Springs, and the secondary VMOC located at NASA GRC in Cleveland, Ohio. Both VMOCs held mirror images of all hardware and databases. When the primary VMOC was deliberately made to fail, a switch to the secondary at GRC was nearly instantaneous. Furthermore, when the CERES VMOC came back online, the switch back was also indiscernible by the user. Currently, this switch was performed by the redirector, which is a single point of failure. Other techniques are being investigated to perform this dual hot-standby function.

Systems Integrator

The General Dynamics master VMOC is actually an integrator of systems. That is, the master VMOC coordinates the external user requests with space and ground assets available from SSTL—here, the United Kingdom–Disaster Monitoring Constellation (UK-DMC) satellite and images requested via SSTL's mission planning system—and ground assets from USN. Thus, the master VMOC acts both as a resource coordinator and as an interface to various systems that are available.

For aeronautics system, one may have a master VMOC for air traffic management coordination communicating with a VMOC located onboard and controlling an unmanned aerial vehicle (UAV).

Scheduler

The scheduler takes user requests, prioritizes these requests and then looks at the available resources to determine if and when a request can be granted. Data that is used by the scheduler includes available space-based assets, available ground system support, orbital dynamics, and user priority. For our real world demonstration, the General Dynamics' VMOC did not have to determine availability of onboard assets. That was done by the SSTL mission planning system, as the UK–DMC is under SSTL control and the SSTL mission planning system understands the details of the UK–DMC power management and resource availability better than the external VMOC can. However, future implementations may require the master VMOC to also perform resource management and monitor such resources as available power and battery levels.

Scheduling is an iterative process. The VMOC receives a request, then determines what assets may be available to service that request. The VMOC then queries those assets as to their availability. If all assets are available, the VMOC schedules those assets and schedules the request. If the assets are not available, the VMOC will determine if there is another time the request can be scheduled. If so, the VMOC again queries all necessary assets for availability. This process is repeated until a time can be found when all required assets are available or until the VMOC determines that the request cannot be granted. As additional assets are added to the system, the complexity of the scheduling process grows.

For aeronautics, such scheduling can be applied to the gates, tarmac area, arriving and departing flights, rescheduling of traffic due to weather, aircraft maintenance and numerous other applications.

Data Mining

The General Dynamics VMOC was implemented to perform data mining. When the VMOC receives a request for an image, the VMOC will first examine its data base and other image data bases to determine if an existing image will fulfill the user's needs. If so, the stored image will be sent to the user. If an existing image is not available, a new image request will be made. Once the new image is received, it will be sent to the user and stored locally in an image database and will likely also be stored remotely.

4. Life Cycle Development

The VMOC can be deployed throughout the mission life cycle – here the life cycle consists of the air traffic management upgrade, deployment and implementation, and operations life cycles. Figure 3 illustrates the process. The VMOC can be incorporated into the system developers' conceptual design to

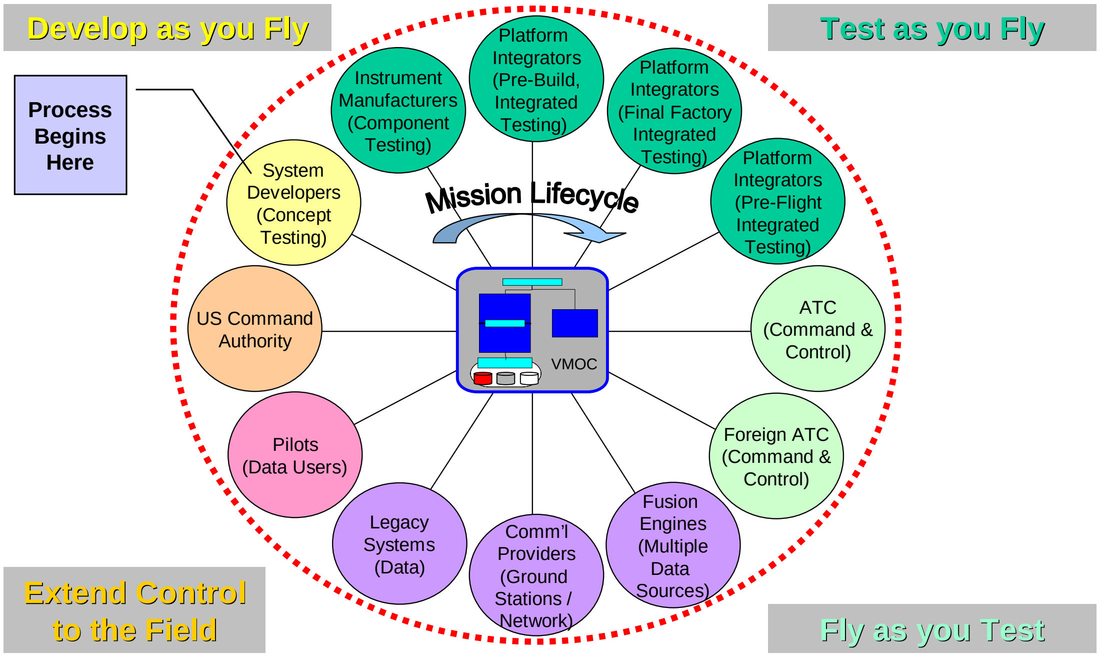

Develop as you Fly
Test as you Fly
Process Begins Here
Mission Lifecycle
Platform Integrators (Pre-Build, Integrated Testing)
Instrument Manufacturers (Component Testing)
Platform Integrators (Final Factory Integrated Testing)
System Developers (Concept Testing)
Platform Integrators (Pre-Flight Integrated Testing)
US Command Authority
VMOC
ATC (Command & Control)
Pilots (Data Users)
Foreign ATC (Command & Control)
Legacy Systems (Data)
Comm'l Providers (Ground Stations / Network)
Fusion Engines (Multiple Data Sources)
Extend Control to the Field
Fly as you Test

Figure 3 - Life Cycle Development

enable concept testing and provide a framework for integrating new technologies, instruments, platforms and system operations concepts. These interrelated systems can use the VMOC as a test integrator prior to deployment in the field. Once system has been tested off-line, they can be brought into operations using the same VMOC.

The VMOC also provides a secure, portal that enable domestic and foreign civil and DoD air traffic control centers to integrate command and control operations. The VMOC can contain the mission rules that enable disparate ATC operations to interoperate.

As a secure portal, the VMOC can provide a common interface for System Wide Information Management (SWIM). Furthermore, it can provide fusion engines whereby data from multiple sources can be integrated to produce knowledge databases. Such databases can include weather, flight plans, cargo, radar data, aircraft tracking and 3D trajectory information, passenger lists, maintenance information, black-box data depositories, and numerous other types of information.

Finally, the VMOC can provide an intelligent interface to enable legacy systems to interoperate with other disparate legacy systems and with future communication systems.

5. Legacy Interoperability Support

The VMOC can provide the secure portal framework and location for housing radio bridging technologies which enable interoperability among a variety of radio systems. Robust radio bridging applications and development suites allow one to connect two way radios, cellular phones, traditional and IP telephones, PCs, PDAs, and other communications devices. These systems are based on open-standard software including voice-over-internet-protocol (VOIP) and provide interoperable group communications to otherwise stand-alone communication systems for international, national, state, and local public safety and defense organizations, as well as for diverse commercial enterprises. Such bridging technology is available from at least two commercial entities today and will

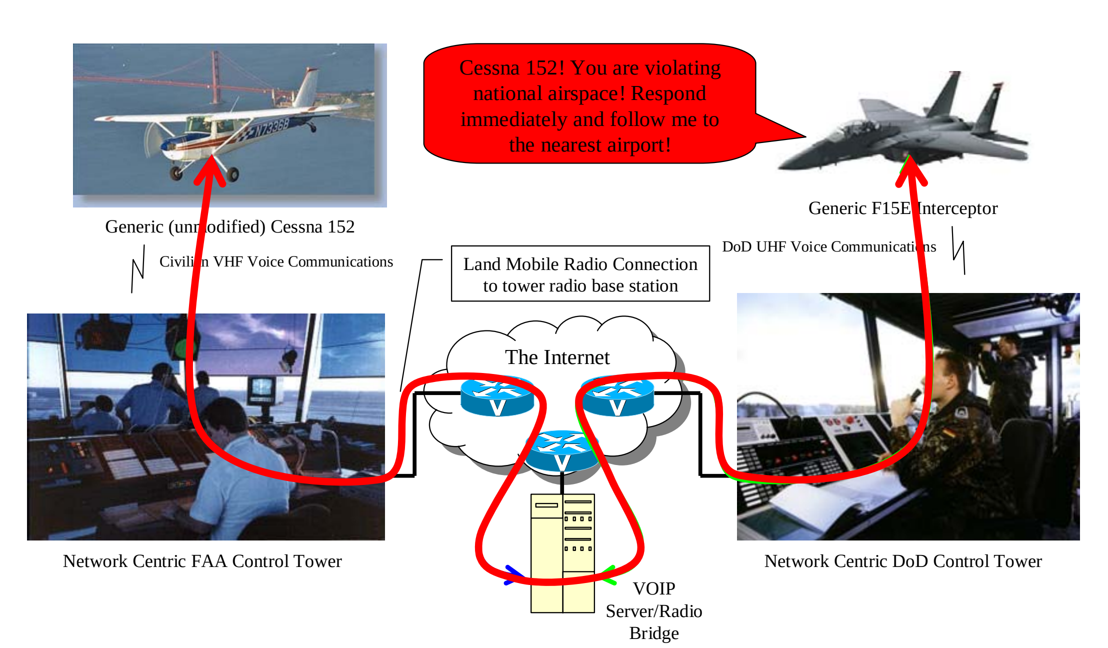

Cessna 152! You are violating national airspace! Respond immediately and follow me to the nearest airport!
Generic (unmodified) Cessna 152
Generic F15E Interceptor
Civilian VHF Voice Communications
Land Mobile Radio Connection to tower radio base station
DoD UHF Voice Communications
The Internet
Network Centric FAA Control Tower
Network Centric DoD Control Tower
VOIP Server/Radio Bridge

Figure 4 – Legacy Radio Interoperability

likely become more prevalent in the future [5, 6]. These systems create massively scalable group communications among all types of communication devices. They are already in use in the military theater. They provide a "virtual" device which can be located anywhere in the world that has Internet connectivity. For "survivability" and redundancy, multiple units can be mirrored and deployed in geographically distributed areas. Furthermore, since the technology is based on Internet Protocols, the radio systems can easily be integrated with encryption systems for secure communications and communications isolation.

Figure 4 provides an example of interoperability between disparate radio systems. In this example, a military aircraft equipped with a UHF analog radio can talk to a civilian aircraft via a bridging application. At each ground radio site, the analog radio signal is tuned into IP packets which are sent to the VOIP server/radio bridge. The server application can forward the packets between radio systems using IP technology. Furthermore, the server can also route these same VOIP packet to other radio systems, and phones. Thus, the DoD, Federal Bureau of Investigation (FBI), Federal Emergency Management Authority (FEMA), Department of Homeland Security (DHS), FAA and other communities of interest can all be brought into the situation if so necessary. In addition, various parties can be listen-only mode while others may be provided push-to-talk capability.

6. Summary

A Virtual Mission Operations Center is a framework for providing secure, automated command and control, resource management, data mining, machine-to-machine communications and access to an asset or assets by remote users using Internet technologies. All of these features are required for the Joint Program Development Office's virtual tower vision. The VMOC concept is currently deployed to provide a secure portal and mission rules for the Cisco Router in Low Earth Orbit (CLEO) and has been selected for use in the Air Force space and missile defense system.

The VMOC provides a framework to define, test, and field an IP-based command and control system capable of supporting secure distributed operations of any IP-based platform or sensor. It also provides a path for the rapid development and demonstration of new technologies within the relevant environment. Incremental integration and demonstration of key technologies, and architectures will lead the way to true transformational communications by facilitate many of the goals of network centric operations.

References

[1] "NGATS ATM Enterprise Architecture Report," Joint Planning and Development Office of Crown Consulting, Inc, June 2005 http://www.crownci.com/NGATS_EA_REPORT.doc as of April 2006 http://www.crownci.com/NEA_Presentation.ppt as of April 2006

[2] "Next Generation Air Transportation System 2005 Progress Report," To The Next Generation Air Transportation System Integrated Plan http://www.jpdo.aero/site_content/pdf/ngats-np_progress-report-2005.pdf as of April 2006

[3] Will Ivancic, Dave Stewart, Dan Shell, Lloyd Wood, Phil Paulsen, Chris Jackson, Dave Hodgson, James Northam, Neville Bean, Eric Miller, Mark Graves, Lance Kurisaki: "Secure, Network-Centric Operations of a Space-Based Asset: Cisco Router in Low-Earth Orbit (CLEO) and Virtual Mission Operations Center (VMOC)," NASA Technical Memorandum TM-2005-213556, May 2005

[4] B. P. Conner, L. Dikeman, V. Osweiler, D. Schoenfelt, S. Groves, P. E. Paulsen, W. Ivancic, J. Walke and E. Miller: "Bringing Space Capabilities to the Warfighter: Virtual Mission Operations Center (VMOC)," paper SSC04-II-7, 18th Annual AIAA/USU Conference on Small Satellites, Logan, Utah, 9-12 August 2004.

[5] Twisted Pair Solutions' Wide Area Voice Environment^{TM} (WAVE^{TM}) http://www.twistpair.com/ as of April 2006

[6] CISCO Land Mobile Radio Gateway, http://www.cisco.com/application/pdf/en/us/guest/products/ps259/c1650/cdccont_0900aecd8034ef85.pdf as of April 2006

Biography

Will Ivancic *is a senior research engineer at NASA's Glenn Research Center working in the networking and advanced communication technology development. Mr. Ivancic's work includes: advanced digital and RF design, communications networks, satellite onboard processing, and system integration and testing, Mr. Ivancic's recent work has concentrated on research and deployment of secure mobile networks for aerospace and DoD networks*

Phillip E. Paulsen *received a B.S. degree in mechanical engineering and a Masters in Business Administration from Cleveland State University. He is a certified NASA Project Manager with over 17 years of experience in the design and development of space flight systems. He served as the Tracking and Data Acquisition Manager (TDAM) for all intermediate and large class NASA ELV missions from 1993 to 1999. Since 1999 Mr. Paulsen has been managing the development of Internet Protocol-compliant network hardware and software for use in space-based platforms.*

Virtual Mission Operations Center for Virtual Towers

2006 Integrated CNS Conference and Workshop

Will Ivancic
NASA Glenn Research Center
wivancic@grc.nasa.gov
216-433-3494
Phil Paulsen
NASA Glenn Research Center
Phillip.E.Paulsen@grc.nasa.gov
216-433-8705

Consolidate Control Centers.

- Virtual Towers is a Joint Program Development Office (JPDO) proposal for the Next Generation Air Transportation System (NGATS)
- Idea: have a few strategically located facilities with virtual towers and TRACONS
- Goal is to combine the delivery locations for ATM services not about decreasing service

This requires Network Centric Operations

Cost Savings

- Projected cost savings in the order of $500 million
- Evolving to spaced-based communication, navigation, and surveillance
  - Reduce or eliminate much of the ground-based infrastructure cost
- Dynamically adjusted airspace
  - Reduce the number of sectors and boundary inconsistencies
  - Eliminate or reduce “handoffs”
  - Eliminate the distinction between Towers, TRACONS, and Enroute Centers.

Network Centric Operations

Key Issues

- **Interoperability**
  - Is the new network fully interoperable with existing open standards (IETF)?
- **Scalability**
  - Will the technology that works on a single vehicle also work on many?
- **Survivability**
  - Can I still maintain network connectivity, even if a primary data path fails?
- **Mobility**
  - Can I maintain network contact with something in motion without the need for manual reconfiguration?
- **Transparency**
  - Can I field a mobile network that is truly “set and forget”?
- **Security**
  - Can I securely cross multiple domains (i.e. open, closed, government, etc...)?
- **Use of Shared Infrastructure**
  - Can I take advantage of low cost (open) network infrastructure?

The FAA’s Goals for the Future NAS

- Modernizing the NAS is based on improving:
  - Safety - such as better weather information in the cockpit and on controller displays
  - Accessibility - such as instrument approaches to many more airports
  - Flexibility - such as allowing users to select and fly desired routes
  - Predictability - such as meeting flight schedules even in adverse weather conditions
  - Capacity - such as increasing aircraft arrival rates to airports
  - Efficiency - such as saving fuel by reducing taxing times to/from the runways
  - Security - such as controlling access to facilities and critical information systems.

Transformational Communications

Lessons Learned

- For the Future NAS to fully succeed the following network issues need to be addressed:
  - Establishment of a **QOS** policy
    - Secure, assured, timely data distribution
    - Bandwidth management
      - Queuing Management
        - Differentiated services
        - Priority queuing
      - High: emergency messages, commands, multimedia
      - Medium: action reports, ISR data
      - Low: status messages, logistics
    - Latency management
    - Jitter management (non-uniform distribution of data packets)
  - Establishment of **Encryption** policy
    - Key management
    - User access management
    - Security infrastructure
    - Policy management
  - Establishment of **Information Assurance** policy
    - Information operations that protect and defend information and information systems
      - Availability, integrity, authentication, confidentiality, auditing, countermeasures, and non-repudiation
    - Methods for promulgating policy across the entire system simultaneously

Virtual Mission Operations

- Virtual Mission Operations is a combination of hardware and software that has been designed to provide secure, virtual, command and control of a sensitive element
- 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 has been implemented as a Service Oriented Architecture

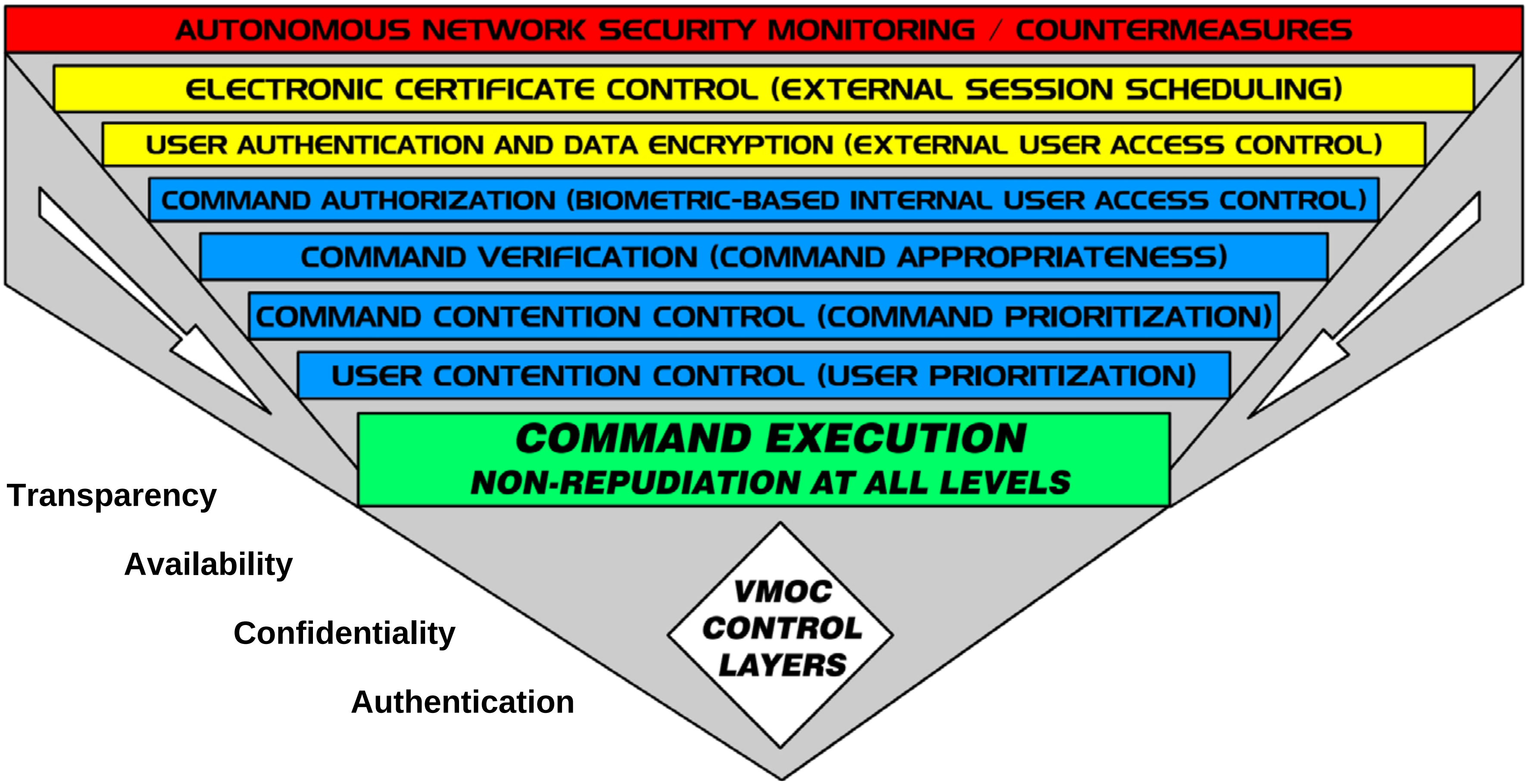
GLENN RESEARCH CENTER
at Lewis Field

VMOC Requirements

- Enable system operators and data users to be remote
- Verify individual users and their authorizations
- Establish a secure user session with the platform
- Perform user and command prioritization and contention control
- Apply mission rules and perform command appropriateness tests
- Relay data directly to the remote user without human intervention
- Provide a knowledge data base and be designed to allow interaction with other, similar systems
- Provide an encrypted gateway for “unsophisticated” user access (remote users of science data)

Virtual Mission Operations

Conceptual Design



AUTONOMOUS NETWORK SECURITY MONITORING / COUNTERMEASURES

ELECTRONIC CERTIFICATE CONTROL (EXTERNAL SESSION SCHEDULING)

USER AUTHENTICATION AND DATA ENCRYPTION (EXTERNAL USER ACCESS CONTROL)

COMMAND AUTHORIZATION (BIOMETRIC-BASED INTERNAL USER ACCESS CONTROL)

COMMAND VERIFICATION (COMMAND APPROPRIATENESS)

COMMAND CONTENTION CONTROL (COMMAND PRIORITIZATION)

USER CONTENTION CONTROL (USER PRIORITIZATION)

COMMAND EXECUTION

NON-REPUDIATION AT ALL LEVELS

VMOC CONTROL LAYERS

Transparency

Availability

Confidentiality

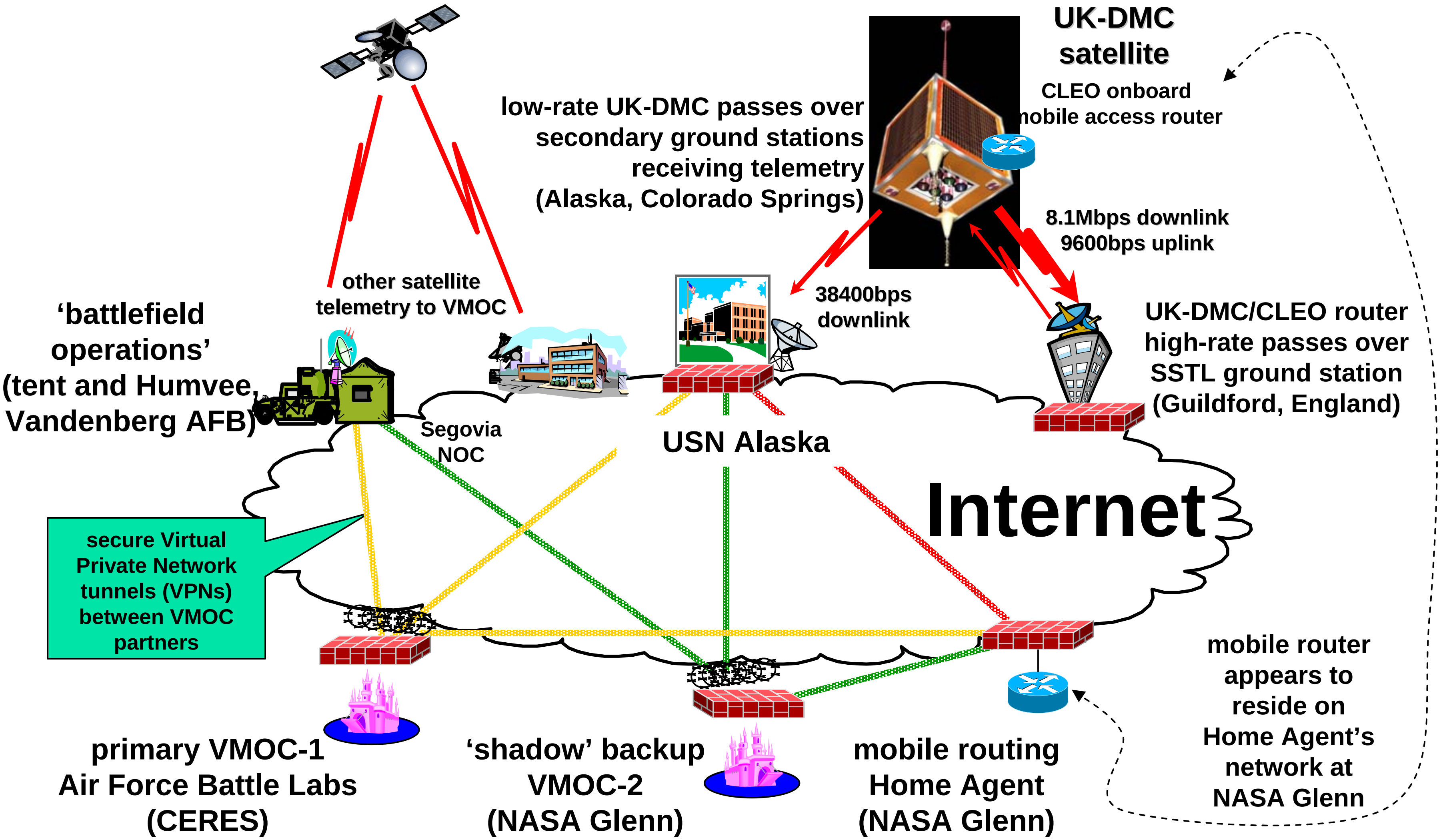
Authentication

The Right Person, Time, and Command

Virtual Mission Operations

- 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 Checks
  - Command Appropriateness
- Command Prioritization and Queuing
- Command Archive
  - User Non-Repudiation

CLEO/VMOC Network



UK-DMC satellite

CLEO onboard mobile access router

low-rate UK-DMC passes over secondary ground stations receiving telemetry (Alaska, Colorado Springs)

8.1Mbps downlink 9600bps uplink

38400bps downlink

other satellite telemetry to VMOC

'battlefield operations' (tent and Humvee, Vandenberg AFB)

UK-DMC/CLEO router high-rate passes over SSTL ground station (Guildford, England)

Segovia NOC

USN Alaska

Internet

secure Virtual Private Network tunnels (VPNs) between VMOC partners

mobile router appears to reside on Home Agent's network at NASA Glenn

primary VMOC-1 Air Force Battle Labs (CERES)

'shadow' backup VMOC-2 (NASA Glenn)

mobile routing Home Agent (NASA Glenn)

Virtual Mission Operations

Field (Cockpit and ATC) User Interface

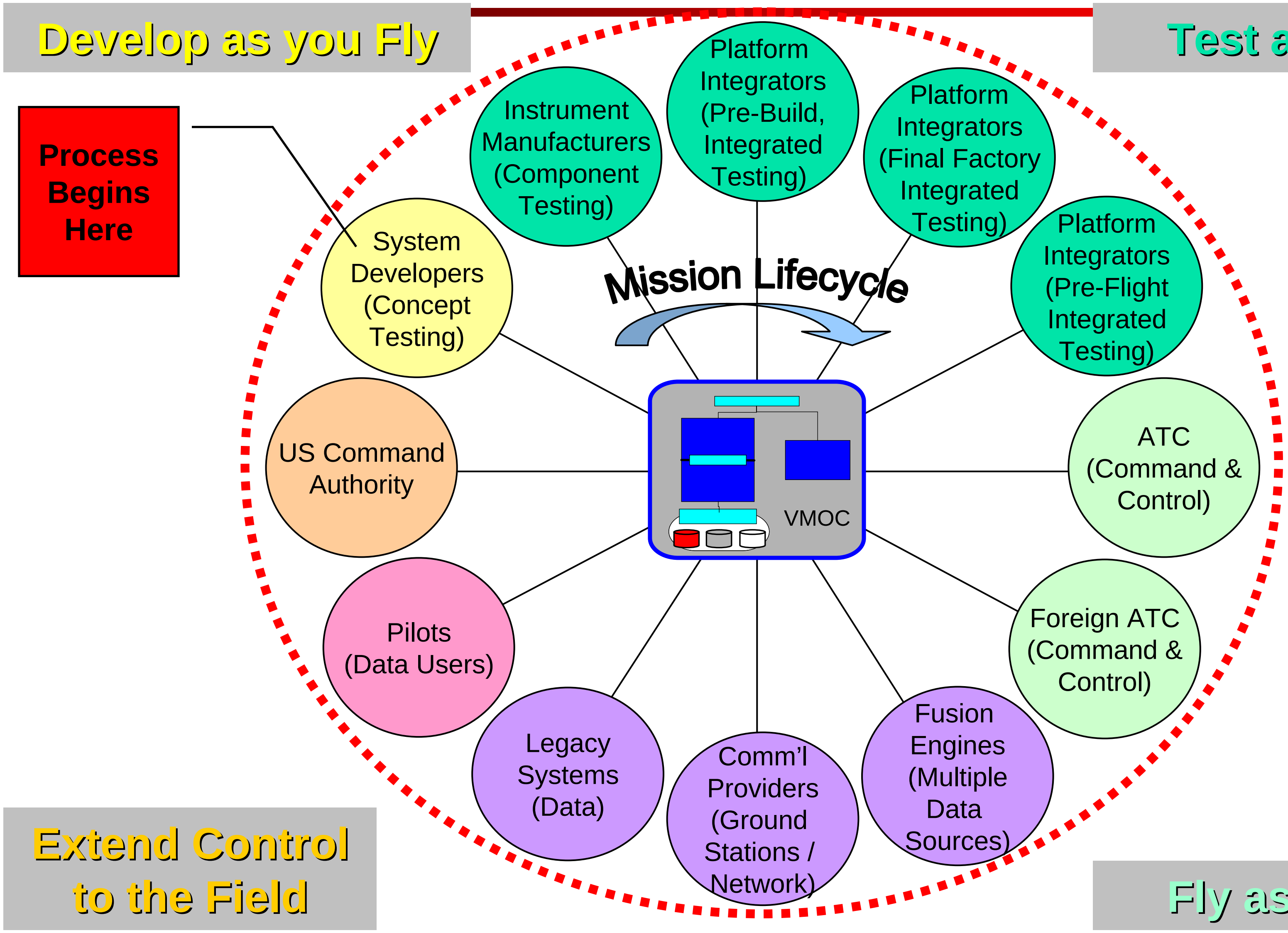
- JAVA-based (utilizes a generic web browser for access)
  - Truly “virtual”, nothing to steal or compromise post-session
  - Survivable system includes multiple, mirrored command elements
- Cockpit user provided with local terrain / weather / traffic keyed to GPS location
- ATC user input defines area 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)
- System responds to cockpit and ATC requests with: standard data sets, meta data, data file sizes, data latency, estimated time to download, alternative data sources, additional related data. Users can always:
  - Request additional data products
  - Request the generation of new data

Virtual Mission Operations

Support Across the Entire Mission Lifecycle

Develop as you Fly

Test as you Fly


Process Begins Here
System Developers (Concept Testing)
Instrument Manufacturers (Component Testing)
Platform Integrators (Pre-Build, Integrated Testing)
Platform Integrators (Final Factory Integrated Testing)
Platform Integrators (Pre-Flight Integrated Testing)
Mission Lifecycle
US Command Authority
VMOC
ATC (Command & Control)
Pilots (Data Users)
Foreign ATC (Command & Control)
Legacy Systems (Data)
Comm'l Providers (Ground Stations / Network)
Fusion Engines (Multiple Data Sources)

Extend Control to the Field

Fly as you Test

Virtual Mission Operations

Integrated Operations

- FAA operations following transformation will not be limited to the direct command and control of aircraft
  - The FAA routinely offers a variety of data products (like weather information and routing updates) to authorized users
  - The VMOC, as currently envisioned, will offer three primary interfaces:
    - A **User Interface** to provide a standards-driven, common user interface
    - A **Mission Interface** to enable policy-based tasking / prioritization and a machine-to-machine interface (eliminating requirements for a man-in-the-loop)
    - A **Policy Interface** to enable authorized organizations to establish system / platform policies
  - VMOC is modular and has been designed to allow rapid adaptation to change and flexible response to dynamic mission requirements

Virtual Mission Operations

User Interface

- Provides standard web-based interface for end users (pilots, ATC, etc…)
  - User requests and priorities based on system policies promulgated by Policy Interface
- Allows “unsophisticated” users to request information from sophisticated systems without the need for extensive training
  - Utilizes generic web interface (a browser such as IE or Netscape)
  - Compartmentalizes data products on a need-to-know basis
  - Checks product centers for info that meets request
  - Promulgates information to user in motion when available
  - Can request tasking through other mission interfaces if user’s needs can not be not met with existing data (i.e weather updates from the National Weather Service)
  - Fuses information from multiple sources (if required)

Virtual Mission Operations

Mission Interface

- Logically located at operations and product centers, physically embedded within remote assets
- Autonomously racks and stacks user requests based on policy driven from Policy Interface
  - Authenticates users
  - Integrates user requests
  - Provides authorized information requested
  - Integrates tasking
- Enables machine-to-machine interface
  - Enables autonomous UAV operations in the NAS

Note: This interface has not been developed yet

Virtual Mission Operations

Policy Interface

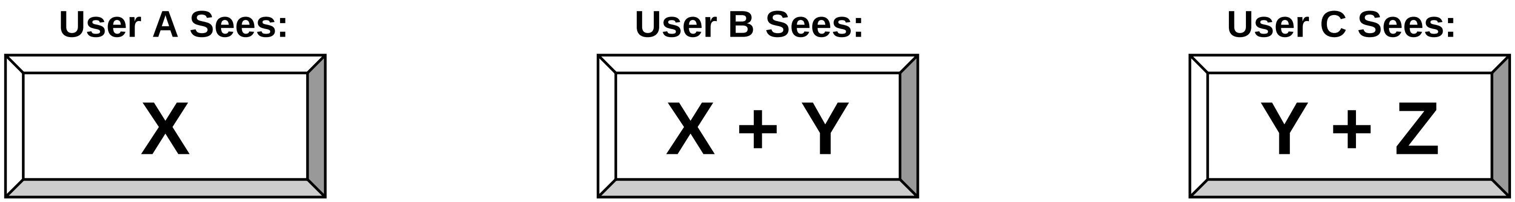
- Most platforms will require policy-driven management
- The VMOC will “rack and stack” policy requests from multiple communities of interest:
  - FAA, USAF, USCG, NORAD, FBI, Intel Community, etc.
  - Policy parameters will include such things as bandwidth allocations, quality of service, type of service, duration of service, prioritization of users, authorization of users
- Will use predictive modeling and simulation to respond to and manage requests
- Will adjust to the real-time situation
- Will autonomously promulgate policies to all assets and mission interfaces

Note: This interface has not been developed yet

Virtual Mission Operations

GD’s Trusted Network Environment (TNE)

- TNE technologies enable compartmentalized access to secure data from a wide variety of assets and locations using generic devices in physically secure locations
  - TNE security capabilities meet or exceed NSA’s strict standards for processing the nation's most sensitive classified secrets
- TNE is a scalable suite of Multi-Level Security (MLS) applications, servers, databases, gateways, and services that ensure fully audited, controlled access to all information and services across an IT enterprise, in full compliance with DCID 6/3
- Trusted technologies label and segregate both data files and applications - users only “see” what their individual security profiles allow, with no knowledge of any other data files, applications or users on the enterprise



Future NAS: Policies to be Revisited?

- Requirement to use dedicated links for high priority traffic
- Use of shared infrastructure for high priority traffic
- Requirement to use link layer (versus IP layer) security
- Handover methodology (frequency versus IP addresses)

Legacy Interoperability Support

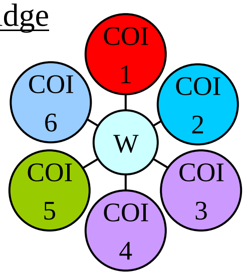
Integrating Disparate Radio
Systems

Legacy Interoperability Support

VOIP Radio Bridge

- A VOIP Radio Bridge treats a cell phone like a virtual radio (# sign = “push to talk”)
  - Unlike existing cell phone services, multiple cell phone users can individually call the VOIP Radio Bridge to get connected together (not limited to just one or two users)
- A VOIP Radio Bridge also accommodates inputs from a wide variety of systems
  - Allowing connectivity between existing radio systems, wired phones, and cell phones
  - Radio systems can be accommodated via the ACU1000 or through generic network devices (routers) offering “Land Mobile Radio” (LMR) service
    - Note: RF is still line of sight. Each individual system (base station and antenna) will still need to be co-located and connected locally to either an ACU1000 or a LMR enabled router during the actual event
- A VOIP Radio Bridge allows system managers to create “Communities of Interest” (COI) to segregate users by common mission or theme. For example:
  - COI #1 would be the Air Traffic Contoller
  - COI #2 would be DHS
  - COI #3 would be DoD
  - COI #4 would be FBI
  - COI #5 would DoT/FAA
  - COI #6 would local first responders

<u>VOIP Radio Bridge Approach</u>

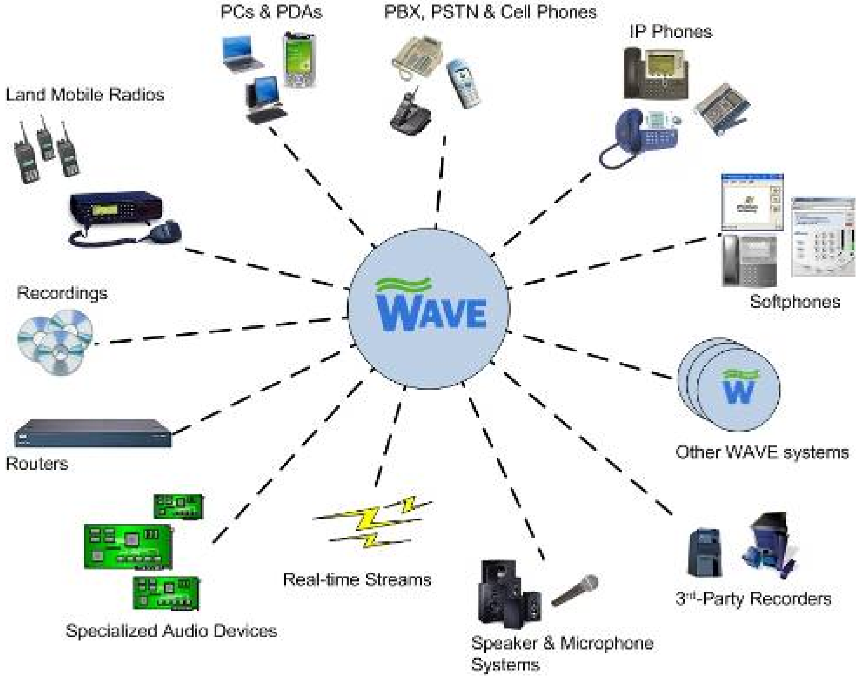


Legacy Interoperability Support

Managing VOIP Service in Real Time

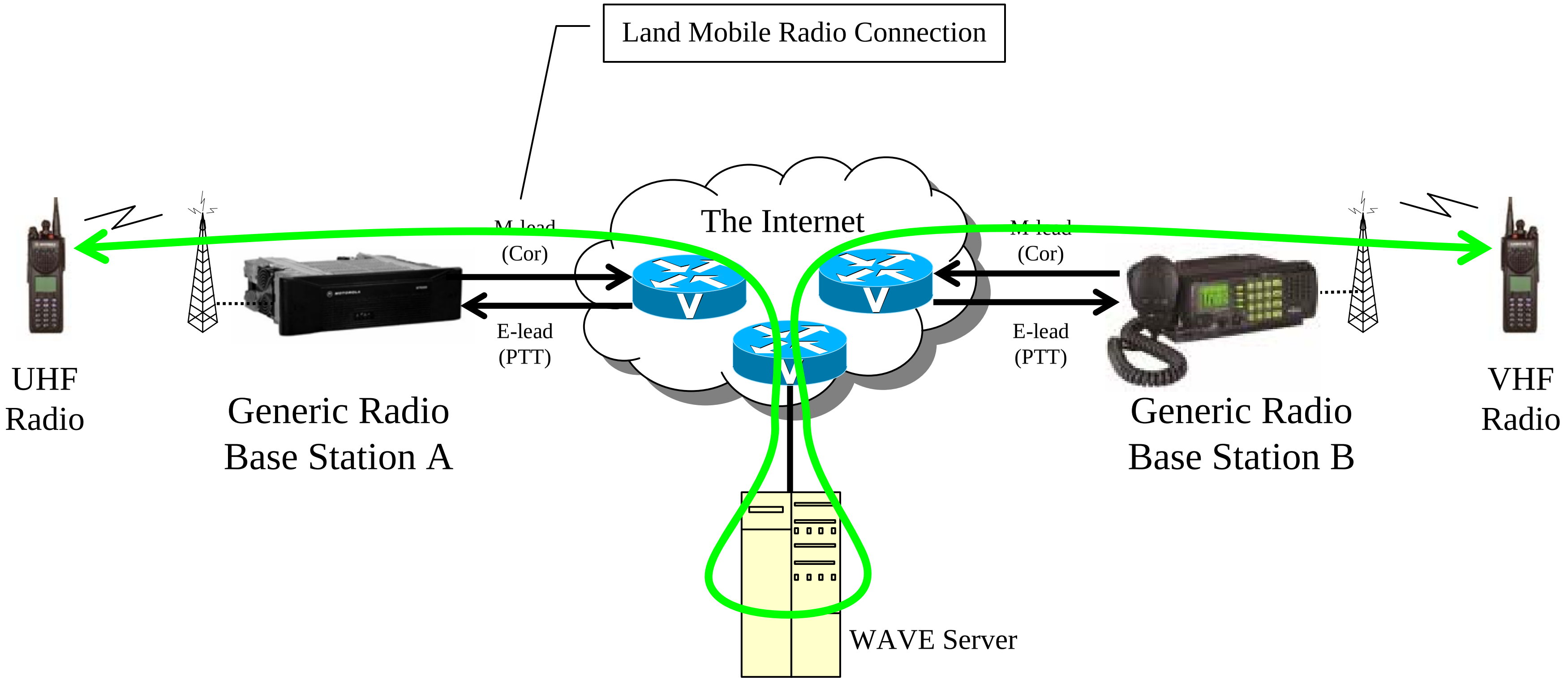
- A WAVE server is a VoIP-based **W**ide **A**rea **V**oice **E**nvironment software solution that creates massively scalable group communications among all types of communication devices
  - Already in use in theater providing SOF ground communications support
  - As a “virtual” device it can be located anywhere that has Internet connectivity
  - For “survivability”, multiple units can be mirrored and deployed in geographically distributed areas
  - Can easily be integrated with encryption svstems for secure communications & communications isolation

If it’s voice, it can easily be routed and managed by using a Wave server



Legacy Interoperability Support

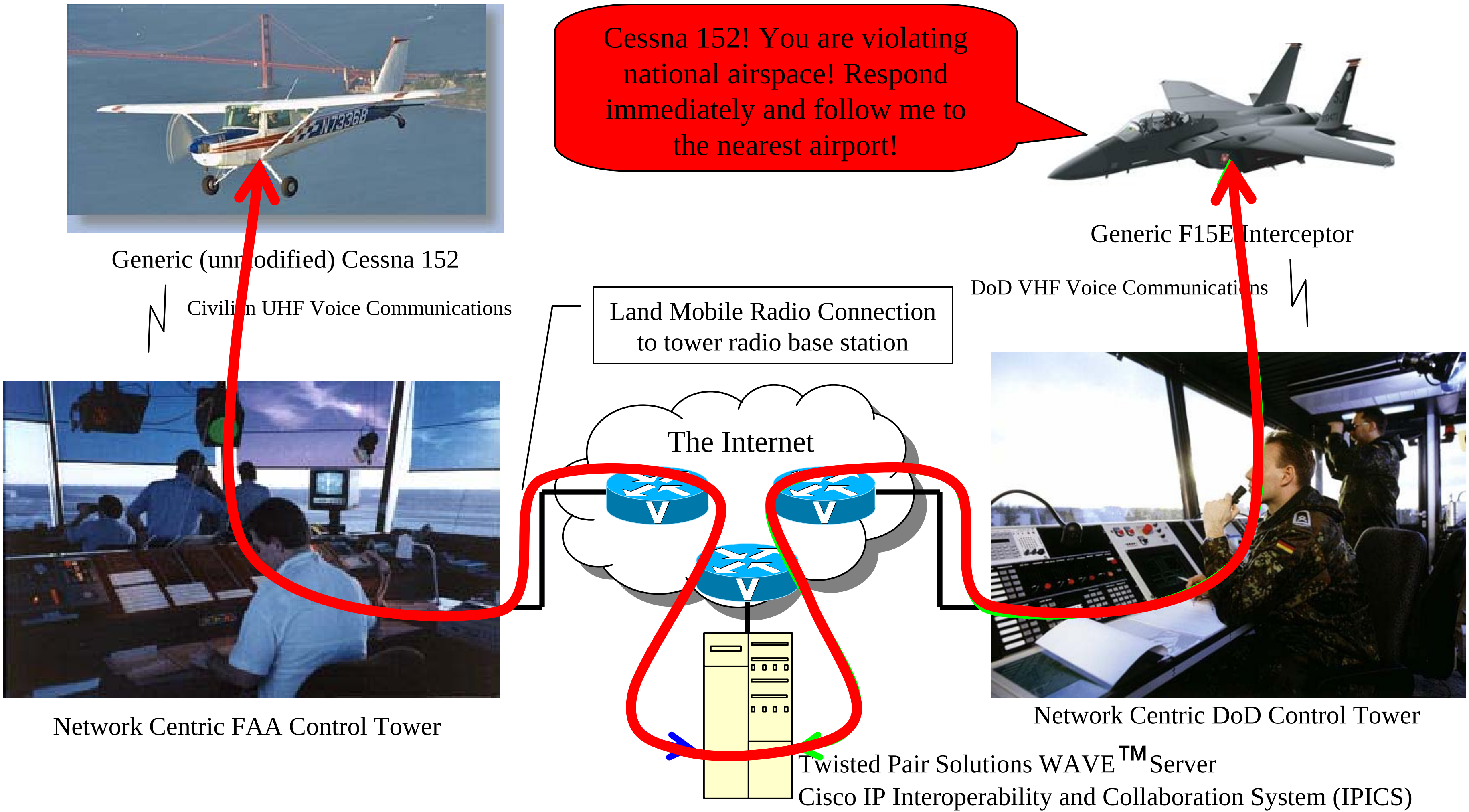
Tying Together Disparate Radio Systems Virtually



- Cisco's Land Mobile Radio (LMR) allows any radio to be connected to the Internet using VOIP technology
- The WAVE server allows the two disparate radio systems to be connected together "virtually"

Legacy Interoperability Support

Emergency Communications Over Disparate Radios



Cessna 152! You are violating national airspace! Respond immediately and follow me to the nearest airport!
Generic (unmodified) Cessna 152
Civilian UHF Voice Communications
Land Mobile Radio Connection to tower radio base station
Generic F15E Interceptor
DoD VHF Voice Communications
The Internet
V
V
V
Network Centric FAA Control Tower
Network Centric DoD Control Tower
Twisted Pair Solutions WAVE™ Server
Cisco IP Interoperability and Collaboration System (IPICS)

The VOIP Radio Bridge can be used to tie together disparate radio systems for emergency communications

Where Do You Go From Here?

- A strategic plan must be formulated which takes into account everything that has been learned:
  - The Future NAS will be packet-based
  - The security solution cannot be decoupled from the network solution
  - 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)
  - Generic data (voice, video, email) will commingle with data from secure systems

NASA GRC is well ahead of all others with regards to a comprehensive, secure, scalable, survivable, mission operations system

Where Do You Go From Here?

- 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

NASA GRC is well ahead of all others with regards to a comprehensive, secure, scalable, survivable, mission operations system