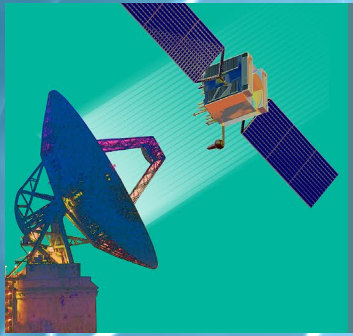


Ground System Architectures Workshop

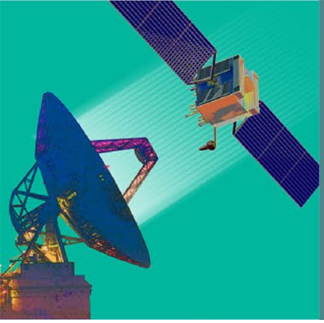
Stronger Together: Improving Interoperability for Users and Operations

February 22–March 2, 2023 | The Aerospace Corporation | El Segundo | California

Working Group C (9:00 AM PT)
Bridging Together Ground and Space Capabilities for Users and Operators

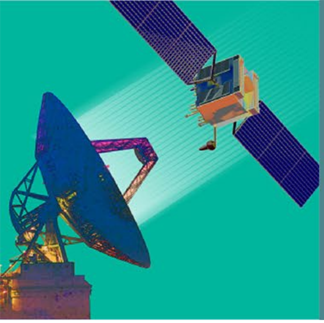
Leads: Mr. Alvin Leung
SSC/BCTI
Dr. Xinyu Wang
The Aerospace Corporation

February 27, 2023



Session Goals

- Develop near-term strategic action plan to bridging the gap bringing together ground and space capabilities for users and operators
- Working group attendees share their past experiences and thoughts through an interactive, guided whiteboarding and breakout session



Rules of Engagement

- This workshop is entirely **UNCLASSIFIED**

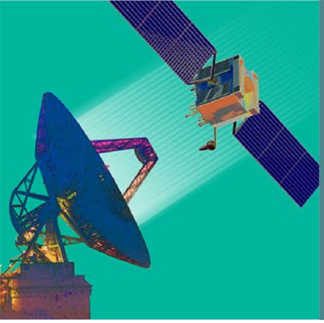
Proprietary

CUI
(Official Sensitive)

Classified

Competition Sensitive

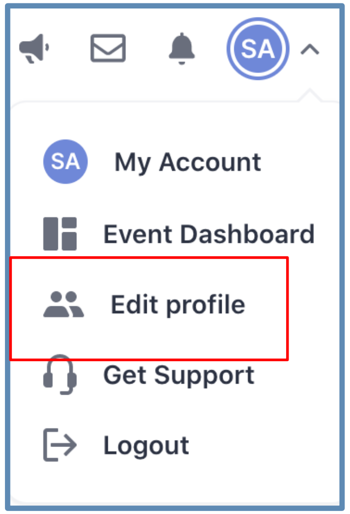
- This workshop will be **recorded** for note-taking purposes



Housekeeping Notes

Reminders:

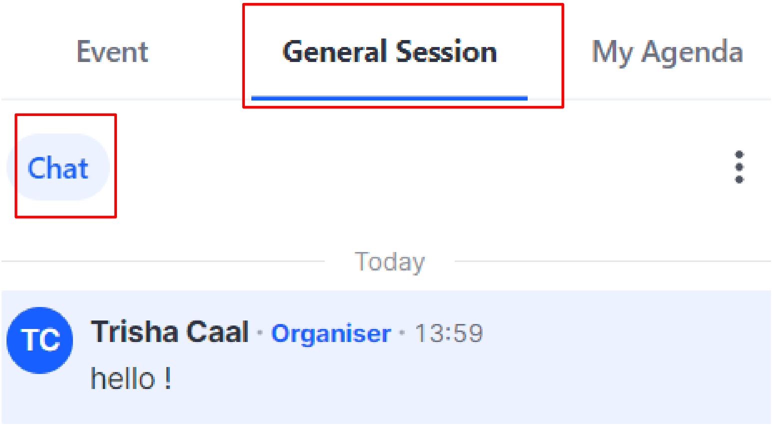
- If you experience any Hopin issues, please click on your account icon at the top right corner of your screen, then select "**Get Support**" to view the FAQs, troubleshooting tips and more.



Attendees are encouraged to use the chat box for questions or comments:

- The host, if time permits, may ask the speaker to answer questions, recap, or provide closing thoughts after their presentation is complete
- The facilitators will help consolidate the questions entered through the chat box and deliver them to the speaker during the live Q&A.
- Questions and comments should be professional, relevant, and related to the subject
- Aerospace retains the right to release all questions from the chat in our public release

Click on the "General Session" tab, then select "Chat" to send questions/comments to all attendees:



About the Speaker

Alvin Leung is the meshONE-T Technical Lead with the United States Space Force's Civilian Service, Space Systems Command, Enterprise Corps, Los Angeles Garrison, Los Angeles AFB CA. Alvin developed architectures for the space launch ranges at the 30th and 45th Space Deltas and for the Satellite Control Network (formerly AFSCN). Previously, Alvin spent over 10 years at Boeing in various engineering and business development roles, designing satellite communications systems and integrating avionics on the International Space Station. Alvin completed his MBA and MS in Systems Engineering from the University of Southern California (USC), and his BS in Electrical Engineering from the University of Texas at Austin. A lifelong aviation and space enthusiast, Alvin is an Eagle Scout and licensed private pilot.

Agenda

- Introductions
- Discussion Topics
  - Interoperability – Network Layer (FNI)
  - Interoperability - Physical Layer (DIFI)
  - Interoperability - Space-Air-Ground Integrated Network (SAGIN)
  - Break
  - On-Demand Resource Provisioning of Space and Ground Networks
  - Cybersecurity – Zero Trust Architecture (ZTA) in Space
  - Cloud Computing - Space-Based vs. Ground-Based
- Recommendations from our Working Group

Introductions

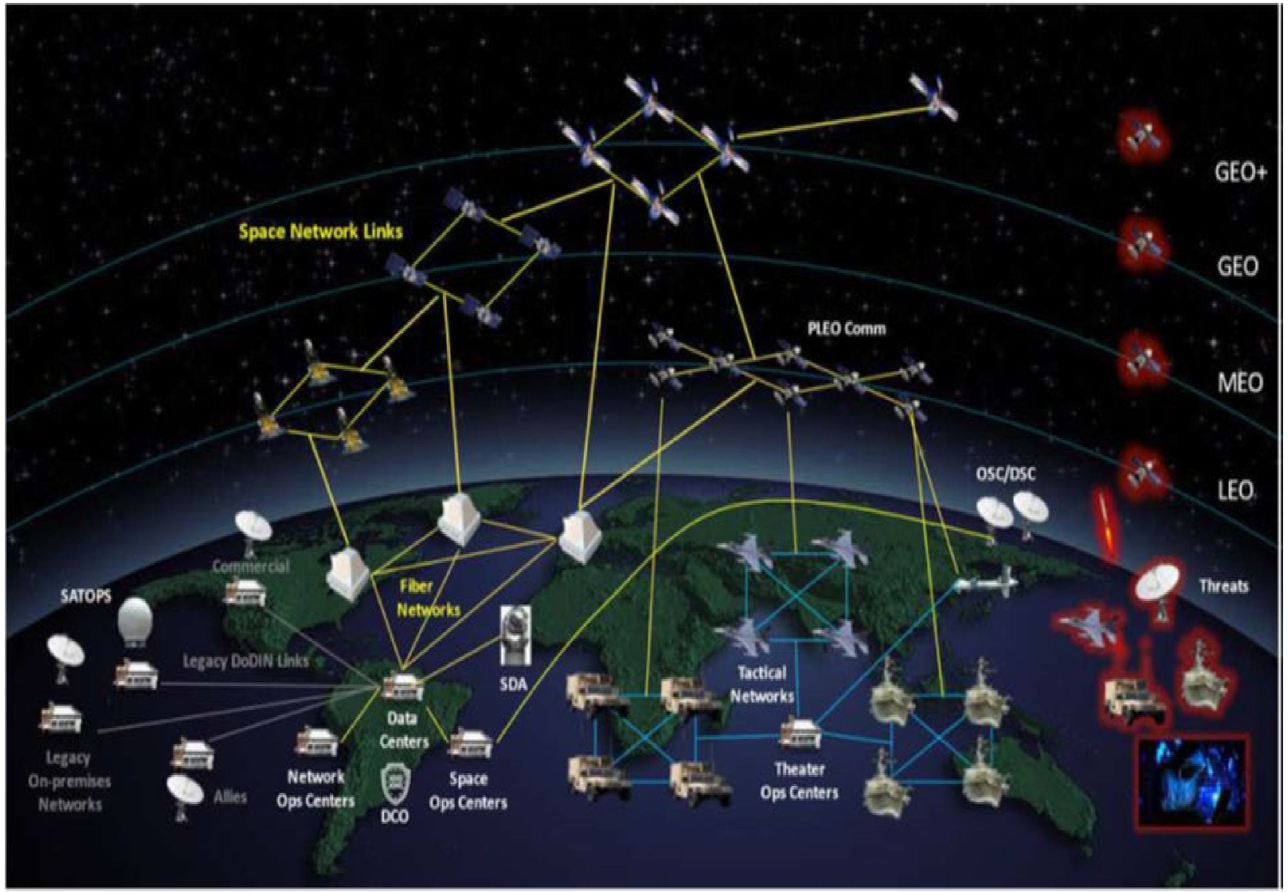
- What is your name?
- What company/organization are you from?
- What is your biggest challenge in bridging space and ground capabilities?
- What are you most interested in learning from today's Working Group?

Agenda

- Introductions
- Discussion Topics
  - Interoperability – Network Layer (FNI)
  - Interoperability - Physical Layer (DIFI)
  - Interoperability - Space-Air-Ground Integrated Network (SAGIN)
  - Break
  - On-Demand Resource Provisioning of Space and Ground Networks
  - Cybersecurity – Zero Trust Architecture (ZTA) in Space
  - Cloud Computing - Space-Based vs. Ground-Based
- Recommendations from our Working Group

Interoperability with FNI - Background

- Problems:
  - The primary challenge in the hybrid SATCOM architecture is to integrate many DoD networks to support warfighter missions. Those networks exist as stovepipes with disparate transmission media, networking architectures, performance, cybersecurity policies, management and control tools
  - The Internet Protocol (IP) convergence becomes insufficient to achieve interoperability in the future military mission networking context
- Goals:
  - Transform the DoD networking capability from fragmented "networks we have" to integrated "networks we want", i.e., one on-demand, global, interoperable, secure, and mission-centric network that supports warfighting



Reference: J. Vanderpoorten, et. al., "Flexible Network Interface (FNI): A Mission-centric Integration Framework for Next Generation DoD SATCOM Networks," IEEE MILCOM, 2021

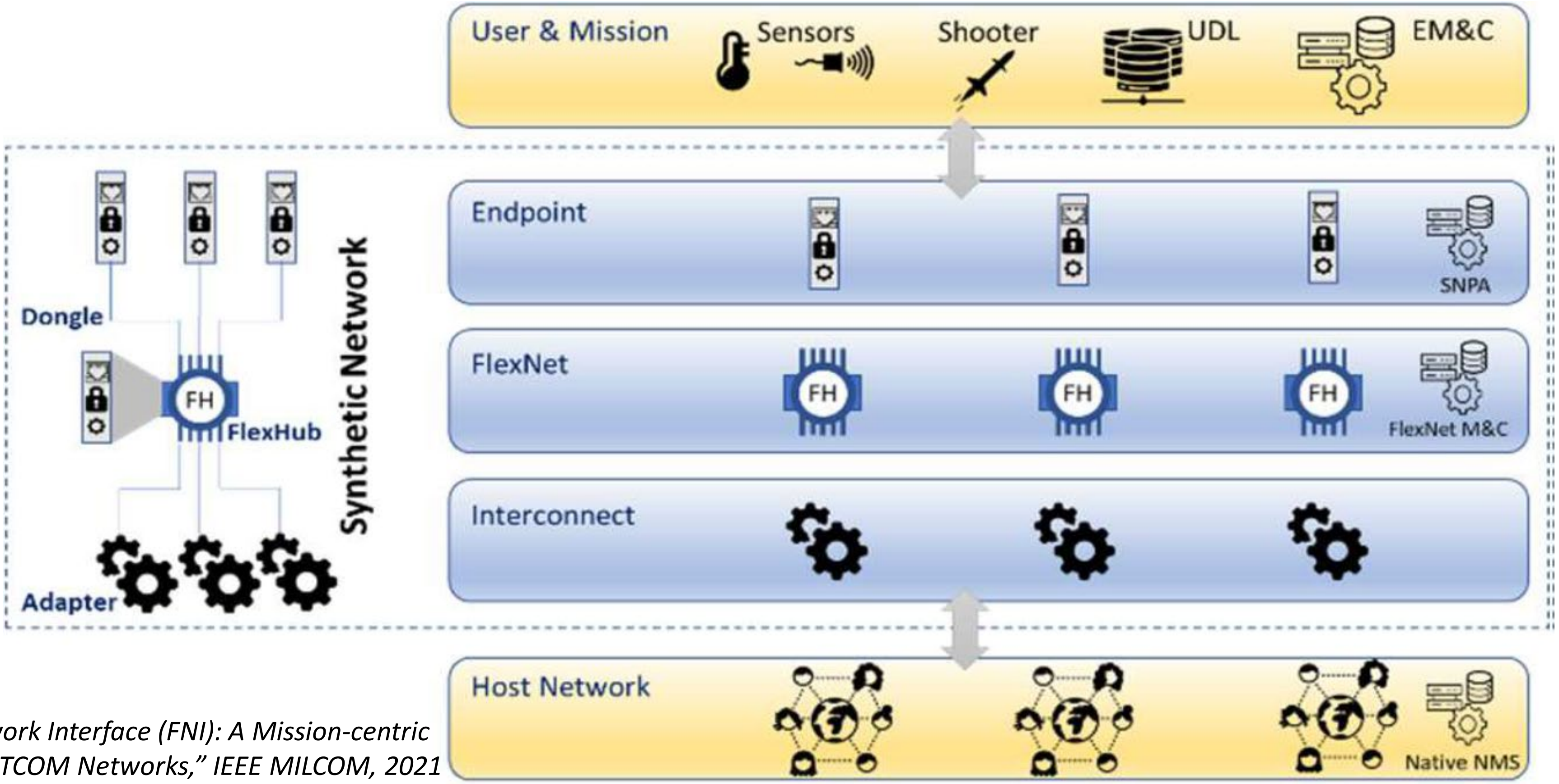
Interoperability with FNI – Solution and Status

- Solution:
  - The Flexible Network Interface (FNI), which is a robust integration framework that deploys enabling technologies to operationalize heterogeneous networks (DoD and commercial) across space, air, ground, and sea
  - FNI enables multiband, multi-waveform, multi-network, controllable and manageable terminals that can access military and commercial SATCOM networks on demand
- Current Status:
  - It is a USSF Space Systems Command (SSC) initiative that has been matured through a series of technology prototyping and demonstration efforts
  - The Flexible Modem Interface (FMI) concept has seen multi-vendor and interoperable implementations and demonstrations

Interoperability with FNI – Architecture

- FNI creates dynamical association of the users in the User & Mission layer with the underlying physical network infrastructure, represented in the Host Network layer
    - The host networks are owned, operated, and managed by different organizations such as Services, COCOMs, and agencies. Those organizations build their own network solutions with narrowly defined requirements, resulting in siloed networks

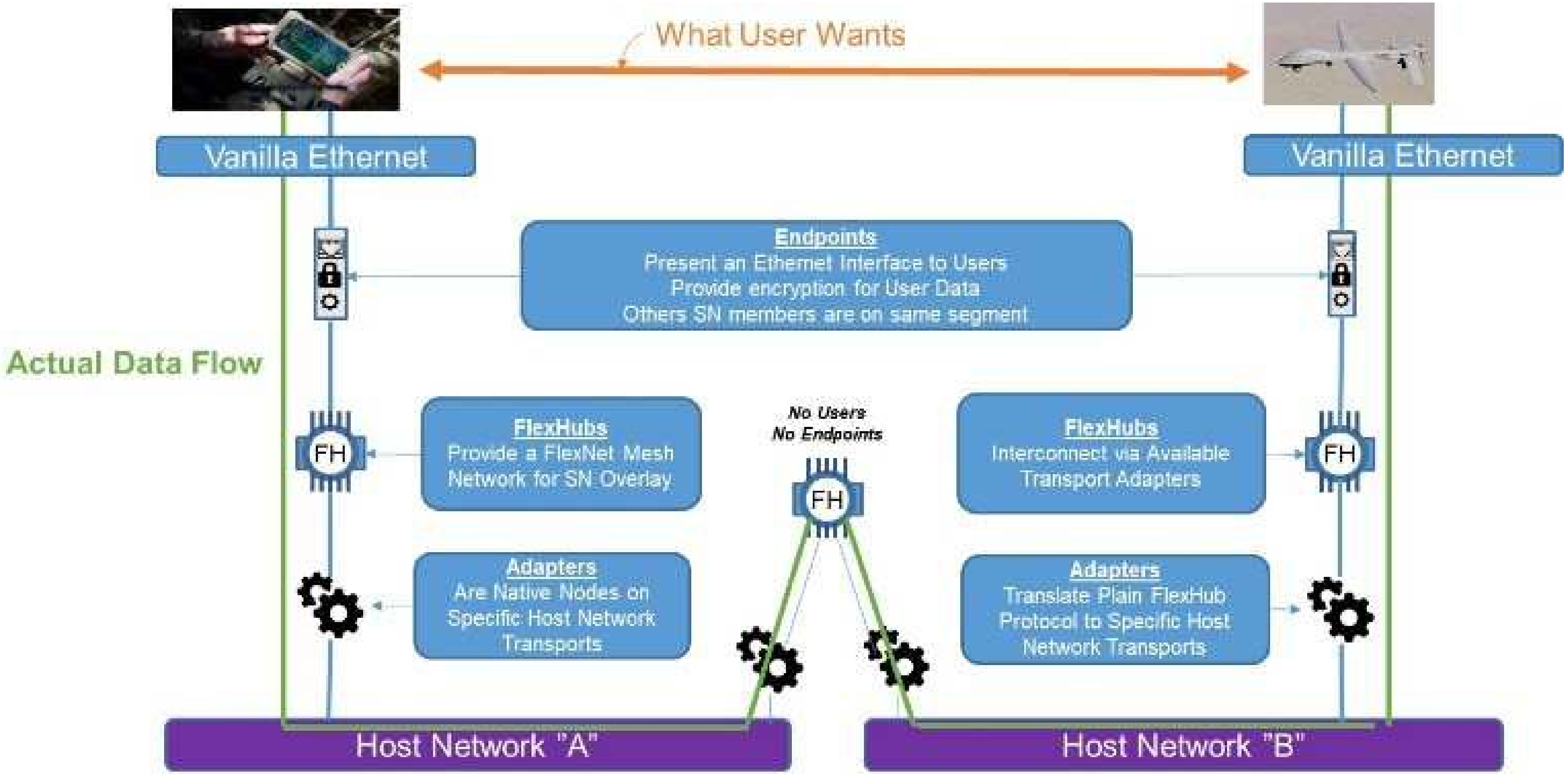
- FNI has 3 layers:
    - ***Endpoint*** Layer presents a common network interface to the users – red L2 Ethernet I/F, and encryption
    - ***FlexNet*** Layer provides a network overlay on top of various underlying host networks that provide transport services
    - ***Interconnect*** Layer presents diverse interfaces with physical host networks



Reference: J. Vanderpoorten, et. al., "Flexible Network Interface (FNI): A Mission-centric Integration Framework for Next Generation DoD SATCOM Networks," IEEE MILCOM, 2021

Interoperability with FNI – Architecture (Cont’d)

- Synthetic Network (Endpoint, FlexNet, InterConnect) provides an secured vanilla Ethernet connection between mission assets



Reference: J. Vanderpoorten, et. al., “Flexible Network Interface (FNI): A Mission-centric Integration Framework for Next Generation DoD SATCOM Networks,” IEEE MILCOM, 2021

Interoperability with FNI - Discussion

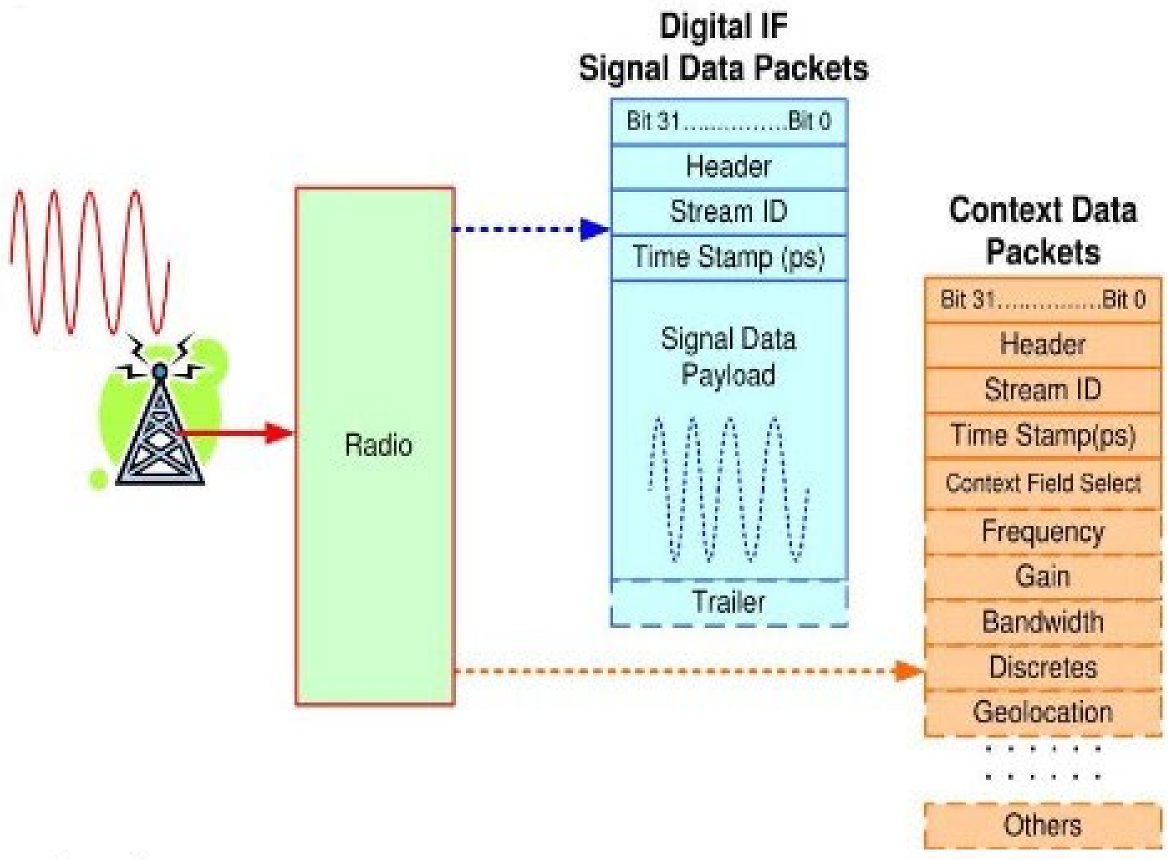
- *There are three relevant technologies: 1) Software-Defined Wide Area Network (SD-WAN) is a solution to integrate multiple underlay networks. 2) Metro Ethernet Forum (MEF) defines External Network-Network Interface (E-NNI) for the interoperable networks, which involves signaling between different service networks. 3) Generic Routing Encapsulation (GRE) over an Internet Protocol Security (IPsec) tunnel is a traditional approach to stitch different underlay networks together. What are the benefits of FNI compared to these three technologies?*
- *How to provision the network resources from the Host Networks for "Users and Missions"? Is there an on-demand bandwidth provisioner or pre-agreed SLAs?*
- *What are the technical challenges to deploy FNI to support DoD missions?*
- *Are there any limitations of "Users and Missions" that could potentially deploy the FNI?*
- *Are there any constraints on the "Host Networks" to be integrated into the FNI framework?*
- *Are there any DoD policies and cybersecurity concerns that prevent the adoption of FNI in the DoD environment?*

Agenda

- Introductions
- Discussion Topics
  - Interoperability – Network Layer (FNI)
  - Interoperability - Physical Layer (DIFI)
  - Interoperability - Space-Air-Ground Integrated Network (SAGIN)
  - Break
  - On-Demand Resource Provisioning of Space and Ground Networks
  - Cybersecurity – Zero Trust Architecture (ZTA) in Space
  - Cloud Computing - Space-Based vs. Ground-Based
- Recommendations from our Working Group

Interoperability with DIFI - Background

- Physical layer - Digital Intermediate Frequency Interoperability (DIFI) Consortium
  - The mission of DIFI is to enable the digital transformation of space, satellite, and related industries by providing a simple, open, interoperable Digital IF/RF standard that replaces the natural interoperability of analog IF signals and helps prevent vendor lock-in
- Goals:
  - Match the interoperability that is native to analog IFs (e.g., L-band)
  - Create an open, simple, interoperable digital IF standard, and encourage its adoption throughput the industry



Reference: Digital Intermediate Frequency Interoperability (DIFI) Consortium Introduction, https://dificonsortium.org/, August 19, 2021

Interoperability with DIFI – Solution and Status

- Solution (ref: https://dificonsortium.org)
  - Define an interoperable standard based on the ANSI standard VITA-49
  - VITA-49 is deployed in 100+ operational digital IF systems today; choice of the US military
  - Specification tailored for satellite industry requirements
- Status (ref: https://dificonsortium.org)
  - Leverage IEEE-ISTO to manage the Consortium and specification
  - IEEE-ISTO Std 4900-2021: Digital IF Interoperability Standard, v1.1 – August 9, 2022. The data plane interface provides the ability to transmit and receive digitized IF data and corresponding metadata over standard IP networks
- Certification (ref: https://dificonsortium.org)
  - Direct connection and cloud connection certifications
  - Excluding testing of the LAN/WAN network

Interoperability with DIFI – Discussions

- *What are the technical challenges in the implementation of the DIFI standards?*
- *What is the current Industry adoption status and the future outlook ? (e.g., space-to-ground in the pLEO)*
- *Given the fast advances in the free space optical communications in the SATCOM field, what’s the impact to the DIFI standard?*

Agenda

- Introductions
- Discussion Topics
  - Interoperability – Network Layer (FNI)
  - Interoperability - Physical Layer (DIFI)
  - Interoperability - Space-Air-Ground Integrated Network (SAGIN)
  - Break
  - On-Demand Resource Provisioning of Space and Ground Networks
  - Cybersecurity – Zero Trust Architecture (ZTA) in Space
  - Cloud Computing - Space-Based vs. Ground-Based
- Recommendations from our Working Group

Interoperability – Space Air Ground Integrated Network (SAGIN)

- SAGIN Background
  - *Current SAGIN networks are stove piped. Most of them do not communicate with each other. The future SAGIN systems are envisioned to enable communications among GEO, MEO, LEO, vLEO, air platforms, and terrestrial networks*
  - *Many researchers in SAGIN, including the 5G/6G standardization*
- Many industry and academia conferences internationally are involved with SAGIN
- For your situational awareness, but due to its international nature, out of scope for this Working Group

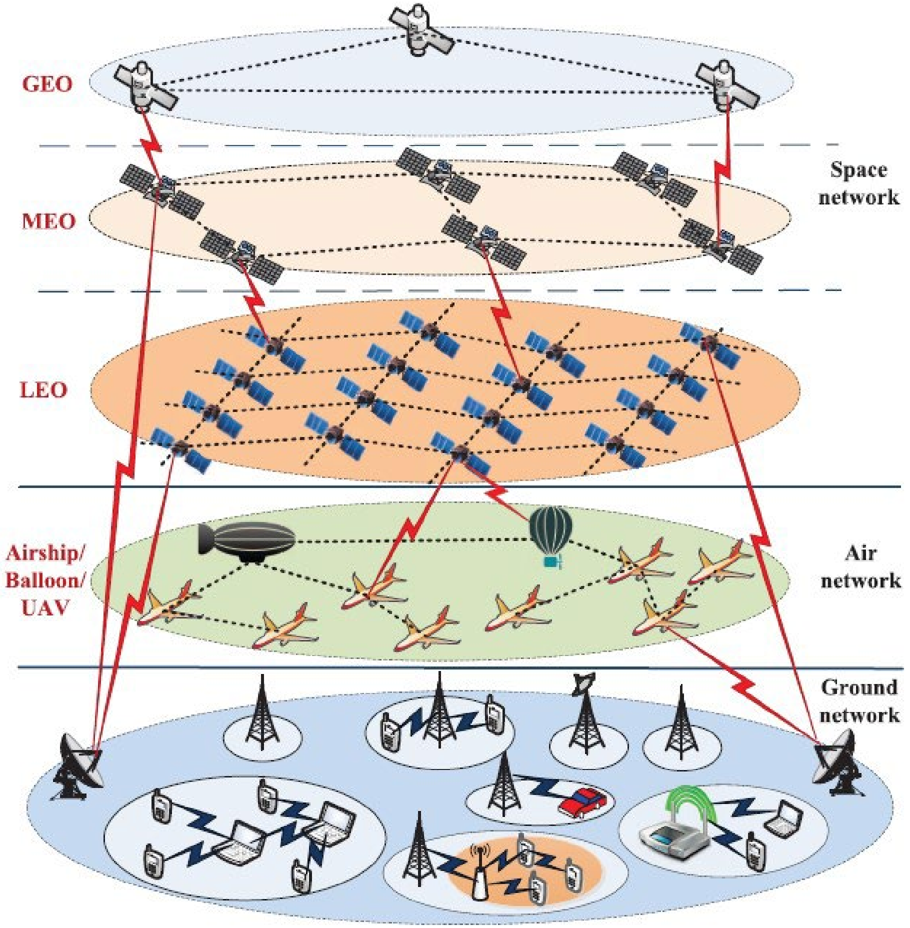


Fig. 1. An architecture for space-air-ground integrated network.

Reference: J. Liu, et. al., "Space-Air-Ground Integrated Network: A Survey," IEEE Communications Surveys & Tutorials, 4th Quarter 2018

Agenda

- Introductions
- Discussion Topics
  - Interoperability – Network Layer (FNI)
  - Interoperability - Physical Layer (DIFI)
  - Interoperability - Space-Air-Ground Integrated Network (SAGIN)
  - Break
  - On-Demand Resource Provisioning of Space and Ground Networks
  - Cybersecurity – Zero Trust Architecture (ZTA) in Space
  - Cloud Computing - Space-Based vs. Ground-Based
- Recommendations from our Working Group

Ground System Architectures Workshop

Stronger Together: Improving Interoperability for Users and Operations

February 22–March 2, 2023 | The Aerospace Corporation | El Segundo | California

Break

Will return at:

Agenda

- Introductions
- Discussion Topics
  - Interoperability – Network Layer (FNI)
  - Interoperability - Physical Layer (DIFI)
  - Interoperability - Space-Air-Ground Integrated Network (SAGIN)
  - Break
  - On-Demand Resource Provisioning of Space and Ground Networks
  - Cybersecurity – Zero Trust Architecture (ZTA) in Space
  - Cloud Computing - Space-Based vs. Ground-Based
- Recommendations from our Working Group

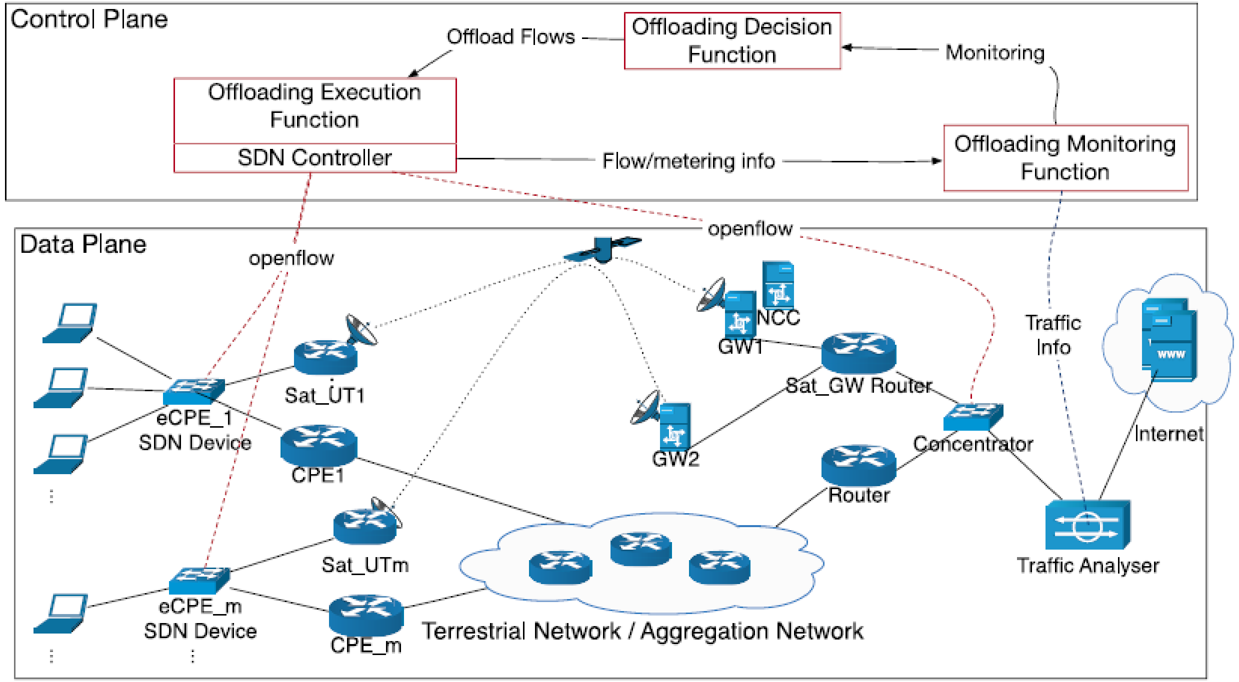
On-Demand Resource Provisioning of Space and Ground Networks

Problems:

- Traditionally, the bandwidth resource provisioning is static. Customers request bandwidth from a service portal, sign the System Service Agreement, and receive the static provisioned resources over a defined time period.

Solutions:

- Dynamic resource provisioning in the time scale of hours or minutes offers many advantages resulting in better resource utilization.



Reference: C. Niephaus and G. Ghinea, "Toward Traffic Offload in Converged Satellite and Terrestrial Networks." IEEE Transactions on Broadcasting, Vol. 65, No. 2, June 2019.

On-Demand Resource Provisioning of Space and Ground Networks

Goals:

- Improve utilization of existing bandwidth resources. Reduce amount of time to provision new resources.

Current Status:

- Researchers are currently looking at methods to offload terrestrial traffic to satellites. Efforts utilizing neural networks and deep learning, as well as dynamic costing models, are being utilized to forecast dynamic allocation of network resources. Researchers have also looked at quality of service (QoS) challenges with the convergence of satellite and terrestrial service provisioning.

On-Demand Resource Provisioning of Space and Ground Networks

- *Discussion:*
  - *What is the framework to implement dynamic resource provisioning?*
  - *What is the state-of-the-art industry practice in dynamic resource provisioning?*

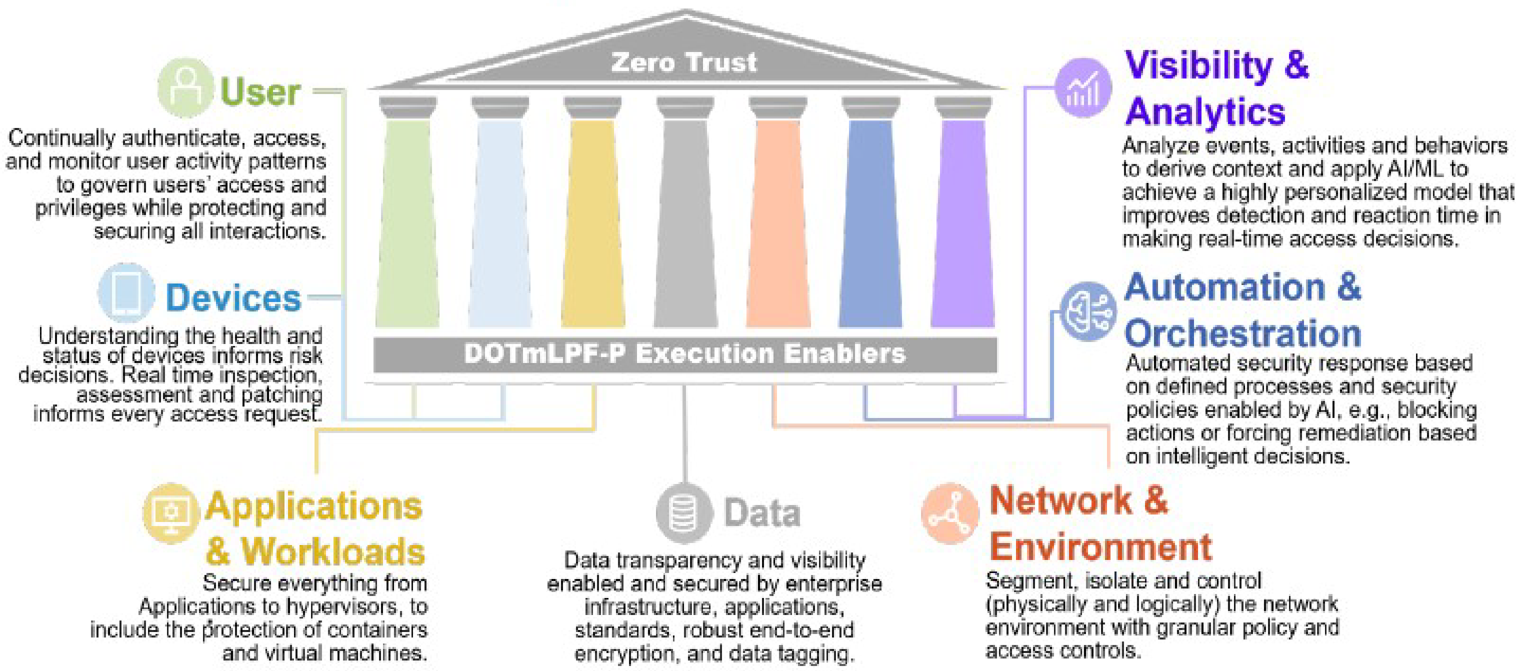
Agenda

- Introductions
- Discussion Topics
  - Interoperability – Network Layer (FNI)
  - Interoperability - Physical Layer (DIFI)
  - Interoperability - Space-Air-Ground Integrated Network (SAGIN)
  - Break
  - On-Demand Resource Provisioning of Space and Ground Networks
  - Cybersecurity – Zero Trust Architecture (ZTA) in Space
  - Cloud Computing- Space-Based vs. Ground-Based
- Recommendations from our Working Group

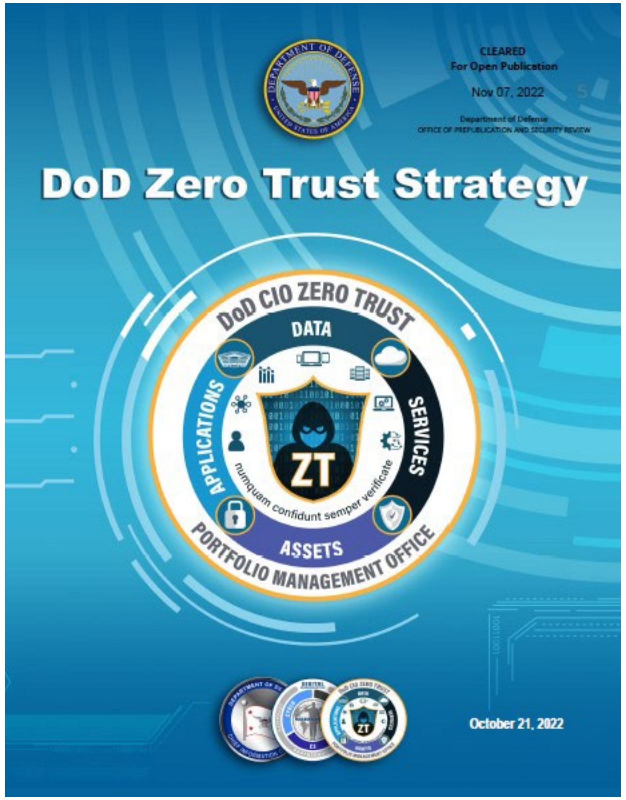
Zero Trust Architecture (ZTA) - Background

- Zero Trust Architecture (ZTA) is a recent DoD mandate. Its application in the enterprise network for the access control and continuous authentication and monitoring are well defined and commercial off-the-shelf solutions are available
- DoD Zero Trust Pillars

Figure 3. DoD Zero Trust Pillars



Reference: DoD Zero Trust Strategy, Oct 21, 2022



Zero Trust Architecture (ZTA) - Capabilities

	Target	Target & Advanced	Advanced
User	**1.1** User Inventory; **1.7** Least Privileged Access	**1.2** Conditional User Access; **1.6** Behavioral, Contextual ID, & Biometrics; **1.3** Multifactor Authentication; **1.8** Continuous Authentication; **1.4** Privileged Access Mgmt.; **1.9** Integrated ICAM Platform; **1.5** Identity Federation and User Credentialing	
Device	**2.5** Partially & Fully Automated Asset, Vulnerability and Patch Mgmt.; **2.6** Unified Endpoint Management (UEM) & Mobile Device Management (MDM)	**2.1** Device Inventory; **2.2** Device Detection and Compliance; **2.3** Device Authorization w/ Real Time Inspection; **2.4** Remote Access; **2.7** Endpoint & Extended Detection & Response (EDR & XDR)	
Application & Workload	**3.1** Application Inventory; **3.3** Software Risk Management	**3.2** Secure Software Development & Integration; **3.4** Resource Authorization & Integration	**3.5** Continuous Monitoring and Ongoing Authorizations
Data	**4.1** Data Catalog Risk Alignment; **4.2** DoD Enterprise Data Governance	**4.3** Data Labeling & Tagging; **4.4** Data Monitoring & Sensing; **4.5** Data Encryption & Rights Management; **4.6** Data Loss Prevention (DLP); **4.7** Data Access Control	
Network & Environment	**5.1** Data Flow Mapping; **5.3** Macro Segmentation	**5.2** Software Defined Networking; **5.4** Micro Segmentation	
Automation & Orchestration	**6.3** Machine Learning; **6.6** API Standardization	**6.1** Policy Decision Point (PDP) & Policy Orchestration; **6.2** Critical Process Automation; **6.5** Security Orchestration, Automation & Response (SOAR); **6.7** Security Operation Center (SOC) & Incident Response (IR)	**6.4** Artificial Intelligence
Visibility & Analytics	**7.1** Log All Traffic; **7.3** Common Security & Risk Analytics; **7.5** Threat Intelligence Integration	**7.2** Security Information and Event Mgmt. (SIEM); **7.4** User & Entity Behavior Analytics (UEBA)	**7.6** Automated Dynamic Policies

Reference: DoD Zero Trust Strategy, Oct 21, 2022

Zero Trust Architecture (ZTA) - Discussion

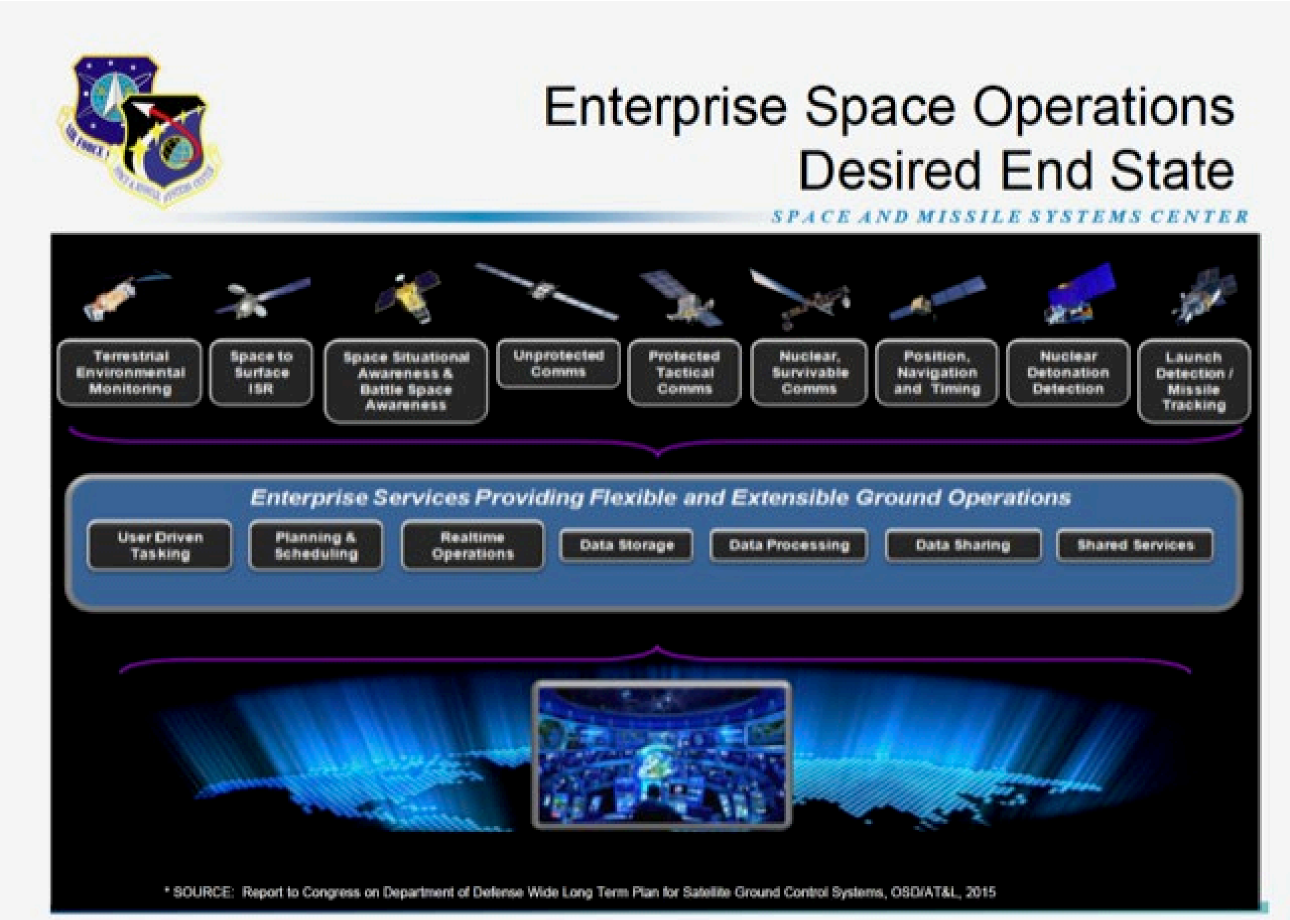
- Zero Trust Architecture (ZTA) is defined for the enterprise terrestrial network, cloud environment and mission network enclaves. The characteristics of the space networking haven not been incorporated
- *Discussion:*
  - *For the space communications, particularly the communications crossing space systems, the threat and attack vectors are different from the terrestrial enterprise network systems. For the space networks, what are the critical ZTA capabilities that should be implemented first?*
  - *For the space communications, how would the ZTA be implemented? What are the technical challenges for the implementation of the ZTA?*

Agenda

- Introductions
- Discussion Topics
  - Interoperability – Network Layer (FNI)
  - Interoperability - Physical Layer (DIFI)
  - Interoperability - Space-Air-Ground Integrated Network (SAGIN)
  - Break
  - On-Demand Resource Provisioning of Space and Ground Networks
  - Cybersecurity – Zero Trust Architecture (ZTA) in Space
  - Cloud Computing - Space-Based vs. Ground-Based
- Recommendations from our Working Group

Cloud Computing – Space-Based vs. Ground-Based

- Problems:
  - Space sensor data is traditionally sent back to ground for processing. This approach utilizes the bountiful ground computing resources. However, it suffers from the longer latency and the availability of the space to ground links.
- Goals:
  - Reduce latency, increase bandwidth, and increase availability of the space to ground links.



References: Enterprise Ground Services (EGS) Overview, SMC/AD, GSAW Presentation 2 Mar 2016
Report to Congress on Department of Defense Wide Long Term Plan for Satellite Ground Control Systems, OSD/AT&L, 2015.

Cloud Computing – Space-Based vs. Ground-Based

- Solutions:
  - Establish space-based cloud computing capability
- Current Status:
  - Ground-based cloud computing systems are being developed to support satellite communications (e.g. Enterprise Ground Services, Unified Data Library)
  - In the commercial sector, SpaceX Starlink, Nippon Telegraph and Telephone (NTT) of Japan are utilizing data centers in space. Also, Amazon Web Services (AWS) provides Ground Station as a Service (GSaaS)
  - meshONE-T provides Data Transport as a Service (DTaaS)

Cloud Computing - Discussions

- *What is the current status of the space-based cloud computing development?*

- *What are the main technical obstacles?*

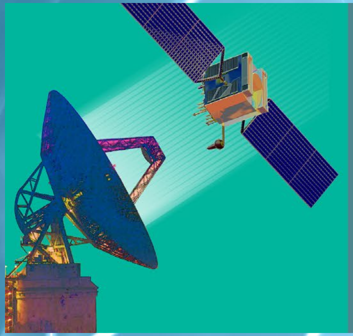
- *What is the state-of-the-art in the hybrid space and ground cloud computing domain? (ground computing resources load-share with the space computing resources)*

Acknowledgements

- Lt Col Louis Aldini, SSC/BCTI
- Mr. Matt Segal, SSC/BCTI
- Dr. Jiayu Chen, Aerospace

References

- "Bluestaq Wins $280 Million Space Force Contract to Expand Data Catalog." *SpaceNews*, March 23, 2021.
- C. Niephaus and G. Ghinea, "Toward Traffic Offload in Converged Satellite and Terrestrial Networks." *IEEE Transactions on Broadcasting, Vol. 65, No. 2*, June 2019.
- C. Niephaus, M. Kretschmer, and G. Ghinea, "QoS Provisioning in Converged Satellite and Terrestrial Networks." *IEEE Communications Surveys & Tutorials, Vol. 18, Issue: 4,* Fourth Quarter 2016.
- D. Bega et. Al., "DeepCog: Optimizing Resource Provisioning in Network Slicing With AI-Based Capacity Forecsting." *IEEE Journal on Selected Areas in Communications, Vol. 38, Issue: 2*, February 2020.
- Digital Intermediate Frequency Interoperability (DIFI) Consortium Introduction, https://dificonsortium.org/, August 19, 2021
- "Enterprise Ground Services (EGS) Overview," SMC/AD, GSAW Presentation 2 Mar 2016
- "DoD Zero Trust Strategy." Version 1.0, October 21, 2022.
- "IOWN: The New Technology that Leads to a Better Future." http://global.ntt/isf/the-own-principles.html
- J. Vanderpoorten et. al., "Flexible Modem Interface Demonstration for Military Terminals," in proceedings of the MILCOM 2019, November 2019.
- J. Vanderpoorten and K. Zhang, "Flexible Modem Interface – Enabling DoD Wideband SATCOM Enterprise," in proceedings of the MILCOM2017, October 2017.
- J. Vanderpoorten et. al., "Flexible Network Interface (FNI): A Mission-centric Integration Framework for Next Generation DoD SATCOM Networks." *MILCOM Track 4 – Architectures, Applications, and System of System Perspectives*, 2021.
- J. Liu et. al., "Space-Air-Ground Integrated Network: A Survey." *IEEE Communication Surveys & Tutorials, Vol. 20, No. 4*, Fourth Quarter 2018.
- "Japan's NTT and SKY Perfect JSAT to Develop Data Center in Space." http://asia.nikkei.com, *Nikkei Asia*. May 19, 2021.
- "MEF Service Operations Specification MEF 54, Ethernet Interconnection Point (EIP): An ENNI Implementation Agreement." March 2016.
- "Report to Congress on Department of Defense Wide Long Term Plan for Satellite Ground Control Systems," OSD/AT&L, 2015.
- "Space Systems Command's Unified Data Library Participates in Army's Project Convergence." *Space Systems Command Media Release*. Nov. 8, 2021.
- "United States Space Force Vision for Satellite Communications (SATCOM)." 23 January 2020.

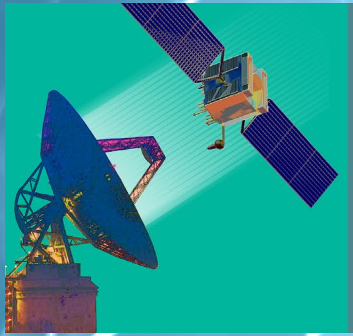


Ground System Architectures Workshop

Stronger Together: Improving Interoperability for Users and Operations

February 22–March 2, 2023 | The Aerospace Corporation | El Segundo | California

Q & A



Ground System Architectures Workshop

Stronger Together: Improving Interoperability for Users and Operations

February 22–March 2, 2023 | The Aerospace Corporation | El Segundo | California

Thank you