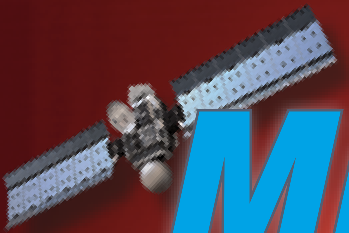


SATCOM for Net-Centric Warfare

MilsatMagazine

SEPTEMBER 2018

iDirect Government: TRANSEC
Kratos Defense
Government Satellite Report
Horizon Technologies
Adcole Maryland Aerospace
The Aerospace Corporation
Norsat International
Globecomm
Dispatches

CYBER WARFARE

PUBLISHING OPERATIONS

Silvano Payne, Publisher + Executive Writer
Hartley G. Lesser, Editorial Director
Pattie Lesser, Executive Editor
Jill Durfee, Sales Director + Associate Editor
Simon Payne, Development Director
Donald McGee, Production Manager
Dan Makinster, Technical Advisor
Sean Payne, Industry Writer

SENIOR CONTRIBUTORS

Richard Dutchik, Dutchik Communications
Chris Forrester, Broadgate Publications
Karl Fuchs, iDirect Government Services
Dr. Bob Gough, Goonhilly Earth Station
Rebecca M. Cowen-Hirsch, Inmarsat
Giles Peeters, Track24 Defence
Paul Scardino, Globecomm
Koen Willems, Newtec

AUTHORS

Mehdi Ardavan
John Beckner
Barbara M. Braun
Terri Moon Cronk
Darko Filipi
Karl Fuchs
Peter Hoene
Jordan Kepler
Roly Rigual
Paul Scardino
Ryan Schradin
Sr. M/Sgt. Jennifer Shirar
Lewis Siempelkamp
Elena M. Sims

FEATURES

DISPATCHES

The future of the Space Force

Deputy Defense Secretary Patrick M. Shanahan walks with Air Force Lt. Gen. John F. Thompson, commander of the Space and Missile Systems Center; Air Force Brig. Gen. Philip Garrant, SMC vice commander; and Joy White, SMC, during a visit to Los Angeles AFB in August.

Space is a contested environment, and the United States must deploy new tools, new capabilities and the right leadership to ensure dominance in that environment , Deputy Defense Secretary Patrick M. Shanahan said recently.

The deputy secretary spoke August 27 to airmen, civilians and contractors at Los Angeles Air Force Base's Space and Missile Systems Center in El Segundo, California. The SMC, a subordinate unit of Air Force Space Command, is the center of technical excellence for developing, acquiring, fielding and sustaining military space systems.

"*We've got a president who says space is no longer a sanctuary*," he added. "*We need to defend our economy. We need to put in place the authorities and the capabilities [in space] to protect our way of life — period. The first law of transformation is, do no harm. Our missions are too important. That doesn't mean we don't take calculated risks or we don't move quickly,*" he said. "*But, from the Pentagon's standpoint we're not going to do harm, and that's why I wanted to come out here and spend some time with you,*" the deputy secretary added.

During the course of the next year, a lot of changes will take place in terms of technology, roles and responsibilities, he said.

"*If we don't choose the right technical solution, we lose. This... is about physics. It's about capability. And when you pick the wrong product, no matter how talented the team or how many resources there are, you lose,*" Shanahan said. “*This is about development and programmatics. Acquisition is a huge enabler, but getting the product right is, in my mind, the most important thing we can do,*” he added.

It’s also vital to put a plan in place that achieves performance, the deputy secretary said. “We have to have clear goals. Without clear goals, the team can’t practice what I call ‘selectful neglect.’ We have -- in large organizations like this -- competing priorities, and if the goals aren’t clear, then it just creates too much confusion.”

Having the right leaders in place also is critical, he said. “*There are so many great people that work in the Department of Defense, so we have the talent. We just need to put them into the right roles The hidden secret sauce is engagement of the team. When the team is engaged, they reward you with discretionary effort. And when you have that kind of environment, it is really fun and energizing to come to work.*”

As for innovation, he noted, “*You find the really great leaders, because they’ll put the project or the program ahead of their own careers, and that’s the kind of culture we want at the end of the day — [the] people who are mission-oriented, first and foremost.*”

Organizations should be centered around the capability DoD wants to deploy and the resources it needs to deploy them, the deputy secretary noted.

“*If you want to know what I think about the Space Force [it’s this]: How do we deliver warfighting capability more quickly?*” Shanahan said.

Other key priorities, he said, are how to give the Missile Defense Agency more capability to do “*birth-to-death tracking*” of ballistic missiles and other cold objects in space, and how to operate in a GPS-denied environment.

“*If we’re really serious about being combat credible, forward-deployed, you’re going to have to operate in GPS-denied environments. We have to get after that capability. We’re standing on the air hose with technology that can be readily deployed. We can go faster.*”

Command and control at the DoD level will set the foundation to do what’s important, Shanahan said.

“*And whether we say it is the legacy of the SMC or the department, but you know the capability emerging to do persistent surveillance of the globe, the amount of data that we’ll be able to collect and parse that in the decision tools to aid the war fighter, that’ll create a time constant that is going to be, you know, unbeatable,*” he added.

DoD will create the environment and infrastructure to provide data to the warfighter, Shanahan said.

www.afspc.af.mil/

Story by Terri Moon Cronk, DoD News

DISPATCHES

GPS III arrives at the Cape for launch

The U.S. Air Force's Space and Missile Systems Center (SMC) Global Positioning Systems (GPS) Directorate achieved a major program milestone on August. 21, successfully delivering the first GPS III satellite to Cape Canaveral Air Force Station, Florida to begin launch processing.

"*The shipment of the first GPS III satellite to the launch processing facility is a hallmark achievement for the program*," said Lt. Gen. John F. Thompson, SMC commander and Air Force program executive officer for Space. "*The modernization of GPS has been an outstanding collaborative effort and this brings us another step closer to launch.*"

The satellite, dubbed "*Vespucci*" in honor of Amerigo Vespucci, the Italian explorer for whom the Americas were named, was transported in a custom container from the Lockheed Martin factory facility in Waterton, Colorado to the Space Coast Regional Airport in Titusville, Florida, by a C-17 Globemaster III originating from Joint Base Lewis-McChord, Washington.

THE GPS III satellite.
Photo is courtesy of Lockheed Martin.

The delivery of Satellite Vehicle 01 (SV01) starts the clock for final testing and checkout of the space vehicle prior to launch. The satellite will be processed at the Astrotech Space Operations Florida facility. A government and contractor team will ensure the integrity of the satellite after shipment by performing a Mission Readiness Test to verify the health and safety of the vehicle, as well as communication compatibility with the ground operations center. The team will then prepare for propellant loading and encapsulate the satellite in its protective fairing. At the completion of these activities, the satellite will be headed for a first of its kind horizontal integration with the SpaceX Falcon 9 launch vehicle.

"*While the launch of the last GPS IIF satellite marked the end of an era, the upcoming GPS III launch will be the start of a brand new one*," said Col. Steven Whitney, director of the GPS Directorate. *"It is the first of our new GPS III satellites, first to integrate with a SpaceX rocket, first to interact with elements of GPS' Next Generation Operational Control System (OCX) Block 0, and first to have spacecraft acquisition and on-orbit checkout from Lockheed Martin facilities.*"

The modernized GPS III SV01 is slated to launch in December and will augment the current constellation of 31 operational GPS satellites.

ADVERTISER INDEX

Advantech Wireless	7
AvL Technologies	5
Comtech EF Data	3
CPI Satcom Products	13
EM Solutions, Inc. (EMS)	21
HISDESAT	19
iDirect Government	1 + 4
Int'l Astronautical Federation	29
Newtec CY	9
SMi Group: Global MilSatCom, London	41
SSPI Halll of Fame Benefit Dinner (DC)	33
Satnews Digital Editions	37
Satellite Innovation	50

*MilsatMagazine is published 11 times a year by Satnews Publishers, 800 Siesta Way, Sonoma, CA — 95476 — USA.
Phone: (707) 939-9306 — Fax: (707) 939-9235*

*We reserve the right to edit all submitted materials to meet publication content guidelines, as well as for grammar and spelling errors, or to move articles to an alternative issue to accommodate publication space requirements, or remove content due to space restrictions. Submission of content does not constitute acceptance of said material by Satnews Publishers. Edited materials may, or may not, be returned to author and/or company for review prior to publication — article review PDFs must be returned with corrections within 72 hours of receipt by the author. The views expressed in Satnews Publishers' various print, online and PDF publications do not necessarily reflect the views or opinions of Satnews Publishers. All rights reserved. All included imagery is courtesy of, and copyright to, the respective companies and/or named individuals. **© 2018 Satnews Publishers***

AvL TECHNOLOGIES

avltech.com

Visit AvL at
OilComm in Houston, TX
Satellite Innovation Symposium
in Mountain View, CA

ENABLING COMMUNICATIONS IN ANY SITUATION

AvL'S FAMILY OF INTEGRATED TERMINALS (FIT)

- Ultra lightweight - meets IATA requirements for carry-on or checked baggage
- One person set-up in less than 10 minutes
- Carbon fiber reflectors - sizes range from 45cm to 1.35M
- All-in-one positioner system & switchable manual or motorized operation
- Quick change tri-band feed and RF kits
- AvL AAQ computer-assisted pointing and acquisition
- Beacon receiver, ODU/modem integration and BUC/LNB integration
- Watch the video at avltech.com/media

U.S. Strategic Command authorizes expanded, operation use of MUOS for the U.S. Navy

Marines from the 1st Marine Division test out the Mobile User Objective System at a Field User Evaluation in Camp Pendleton, California. MUOS is a satellite communication system that uses commercial cell phone technology on the battlefield. Marine Corps Systems Command will begin fielding MUOS in the fourth quarter of 2018.

Photo is courtesy of the U.S. Marine Corps — Eddie Young

The U.S. Navy has announced that U.S. Strategic Command has approved the service's next-generation, narrowband satellite communication system for expanded operational use, this according to a news report in the AFCEA's online Signal Magazine infopage.

The news article, written by *George I. Seffers*, the publication's Technology Editor, reveals that this authorization paves the way for U.S. Navy and U.S. Marine Corps "early-adopter" commands to use the system on deployment as early as this fall, primarily in the Pacific theater, according to the written announcement.

An Atlas V launch vehicle carrying the U.S. Navy's fifth and final Mobile User Objective System (MUOS) communications satellite lifts off from Space Complex 41, Cape Canaveral Air Force Station, Florida.

Photo is courtesy of the U.S. Navy.

The Navy's on orbit, five-satellite constellation — the Mobile User Objective System (MUOS) — began providing legacy satellite communications shortly after the system's first satellite launch in 2012.

Each MUOS satellite has dual capability. The legacy satellite communications payload was designed to maintain legacy narrowband communications for the Defense Department while the advanced MUOS capability came online.

The full-suite MUOS payload, known as Wideband Code Division Multiple Access (WCDMA) waveform, adapts commercial cellular technology to allow warfighters to communicate beyond-line-of-sight, more securely and reliably than before, and with 10 times the capacity compared to the legacy capability, the announcement states.

On June 24, 2016, the U.S. Navy's fifth Mobile User Objective System (MUOS) satellite launched at 10:30 a.m. EDT from Space Launch Complex 41 aboard a United Launch Alliance Atlas 5 rocket in the 551 launch vehicle configuration.

With the MUOS constellation on orbit, the ground and network management system operational, and the WCDMA waveform available for end-user radios, operators today with MUOS WCDMA radios are connecting beyond line-of-sight around the globe, transmitting simultaneous voice, video and mission data on an Internet Protocol-based system that connects to military networks. MUOS-enabled radio population continues to be the limiting factor for greater MUOS WCDMA use.

The system could be declared fully operational following Multi-Service Test and Evaluation next summer.

The U.S. said it would be the first service to widely deploy MUOS, largely due to its investment in MUOS-portable radios over the past six years.

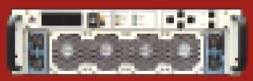
The USMC is slated to begin initial MUOS fielding in the fourth quarter of 2018, followed by initial operational capability in the first quarter of 2019.

ADVANTECH
WIRELESS

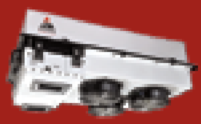
Second Generation GaN based SSPAs/BUCs in C, X, Ku and Ka-Band

250W C-Band
2nd Generation GaN SSPA/BUC

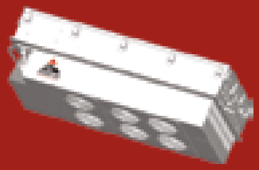
400W C-Band
2nd Generation GaN SSPA/BUC



300W-400W C-Band Rackmount
2nd Generation GaN SSPA/BUC



400W Ku-Band
2nd Generation GaN SSPA/BUC



1,250W Ku-Band
2nd Generation GaN SSPA/BUC

These GaN based units provide an impressive 60% increase in Linear Transmit Power, without any increase in size or weight.

www.advantechwireless.com

DISA helps to ensure the U.S. Coast Guard is 'always ready' on their 228th birthday + Joint Regional Stacks

The U.S. Coast Guard (USCG) will celebrated their 228th birthday on August. 4.

This unique, uniformed service operates under the Department of Homeland Security during peacetime and can be transferred to the Department of the Navy by the U.S. President at any time, or by Congress during times of war.

Although the Coast Guard is not a Department of Defense (DoD) agency, it does rely on DISA-provided services and capabilities to accomplish its many missions at home and abroad, including protecting shipping and trade, search and rescue, installing and maintaining aids to navigation, combating drug smugglers, and marine environmental protection.

"*The U.S. Coast Guard is a Defense Information Systems Network, or DISN, subscriber*," said Scott Steinmeyer, a representative from DISA's Mission Partner Engagement Office. "*That means they have access to terrestrial and satellite infrastructure services supporting voice, video, and data transmission, including the Non-secure Internet Protocol Router Network (NIPRNet) and Secure Internet Protocol Router Network (SIPRNet), and cybersecurity services.*"

Coast Guard Commander, Harold "Lars" McCarter, director of the Network Operations and Security Center at Coast Guard Cyber Command, said the force uses DISN services across all operational mission areas, just like the Army, Marine Corps, Navy, and Air Force.

He specifically named a number DISA-provided security services the Coast Guard uses.

"*Operationally, we leverage Joint Regional Security Stacks (*editor's note: additional information regarding Regional Security Stacks is provided at the close of this news story...*) in addition to those tools provided by DISA for the DOD enterprise, whether it's the Assured Compliance Assessment Solution, Host Based Security System, and the Windows 10 Secure Host Base Line*," said McCarter. "*As a DISN subscriber, we also get the shared benefit of Tier 1 security services at the DOD Information Network (DODIN) boundaries.*"

The Coast Guard also uses Defense Collaboration Services (DCS), DISA's real-time collaboration tool suite, in classified and unclassified environments, and Defense Enterprise Email on the SIPRNet, McCarter said.

Although the Coast Guard has been performing missions alongside the other services during every war since the nation was founded, a large portion of their communication today is done with people outside of the DOD.

"*Unlike many of DISA's mission partners, the Coast Guard interfaces significantly with a range of civilian customers*," said McCarter. "*Web services, such as Homeport, which operates within the DODIN, allow the Coast Guard to provide services to the civilian sector.*

"*Homeport is basically our interface with all our port owners and operators, who are, for the most part, civilian," said McCarter. "It's challenging because we have to make those systems work in a way where the civilian users can access the systems, while still meeting stringent DOD security requirements.*"

McCarter said the Coast Guard can operate on the DODIN with confidence, knowing DISA is diligent about defending the network and ensuring high availability of services.

Another example he gave was DISA's aid to the Coast Guard's mission of facilitating the secure arrival and departure of cargo in and out of the country. When ships need to come in to port, they have to send passenger manifests and cargo manifests to the Coast Guard.

"*All personnel and cargo communications are vetted on our systems residing on the DODIN*," said McCarter. "*External '.com' emails and other forms of communications coming from the internet must traverse the DODIN gateways to reach us within the '.mil' environment.*"

In a video posted by DefenseNews.com, retired Admiral Charles Michel, former Vice Commandant of the Coast Guard, explained the unique nature of the Coast Guard's information technology infrastructure.

"*We operate on the DODIN but we're also a law enforcement agency, a member of the Department of Homeland Security, and a member of the intelligence community*," he said.

DISA understands the Coast Guard's unique role in the defense of our nation, and stands ready to assist, said Ted Lewis, deputy chief of the agency's Mission Partner Engagement Office.

"*Our goal is to allow the Coast Guard to focus on their core missions — protecting life, property, the environment, and our nation's economy — while we, DISA, focus on providing, sustaining, and securing their information technology and communications infrastructure.*"

"*The Coast Guard motto is Semper Paratus, or 'always ready*,'" said Lewis. "*And DISA is always ready to support our port partners.*"

What are Joint Regional Stacks?

DISA stipulates that Joint Regional Security Stacks provide increased network visibility, shared data, and a stronger defense.

The importance and complexities of enabling seamless data sharing through the Joint Regional Security Stack (JRSS) platform was the subject of discussion among expand experts from DISA and Joint Forces Headquarters -

PEACEKEEPING
GOVERNMENT
HUMANITARIAN
ISR
BORDER SECURITY
EDUCATIONAL
school
NAVAL
VOTE
AISR
HEALTHCARE

Department of Defense Information Network (JFHQ- DODIN) during an earlier Armed Forces Communications and Electronics Association's Defensive Cyber Operations Symposium in Baltimore, Maryland.

The JRSS platform is a DoD-wide initiative to enable military services, combatant commands, and defense agencies to see more network activity, defend networks more efficiently, and share information seamlessly within their own organizations and with DoD mission partners.

"*JRSS will deliver to the greater DOD community the ability to act uniformly with predictable outcomes through a centralized, standardized, and modernized infrastructure*," said Army Colonel Greg Griffin, JRSS Program Manager.

The typical unclassified "stack" is comprised of 20 equipment racks that manage and defend traffic flows; perform firewall functions, intrusion detection and prevention, enterprise management, and virtual routing and forwarding; and enable the ingest of large sets of data, and provide the platforms to process that data and the mechanisms to help cyber operators analyze the data.

Fourteen unclassified Joint Regional Security Stacks are currently operational, and 20 will protect the DOD unclassified network by the end of fiscal year 2019: 11 are in the continental United States, two in Europe, two in the U.S. Central Command area of responsibility (AOR), and five in the U.S. Pacific Command AOR. The classified set of networks will require 25 stacks.

Griffin said in the not-too-distant-future, a JRSS platform fielded with standardized suites of equipment, complete with defined syntaxes and procedures, will enable the military services, combatant commands, and agencies to share tips and cues from within a common platform without having to recreate or reformat data for different devices.

DISA assembled a JRSS Defensive Cyber Operations working group to build toward that future. The group is made up of members from various JRSS stakeholder organizations charged with defining the tactics, techniques and procedures that govern JRSS best practices, to include information sharing between organizations.

"*The big thing for us is accessibility for everybody... not keeping (data) stove-piped... which is what we have now*," said Army Colonel Darlene Straub, Chief of DISA's Defensive Cyber Operations (DCO) Division and chair of the JRSS DCO working group.

"*One of the things we've come to agreement on recently is we want to make sure we use the JRSS as a data source, not only having the data available on our site within the Joint Management System (JMS), but also being able to share it*," Straub said. "*How can we use that data to become more powerful and more [knowledgeable] about what's on the network?*"

Straub's team works closely with the DISA Global Operations Command (DISA Global), which is responsible for operating and maintaining JRSS.

The DISA Global commander, Army Colonel Lisa Whittaker, also emphasized the value of looking across organizational boundaries to understand network operations.

"I'm looking forward to JRSS stabilization, followed by data consolidation, so that we can start looking at the analytics to more rapidly identify nefarious behavior and counter it," she said.

According to the 2015 DoD Cyber Strategy, building an architecture that transcends individual branches will enable a robust network defense and shift focus from protecting service-specific networks and systems to securing the DoD enterprise in a unified manner.

"*As JRSS matures, and we better understand the ability to share that information, one of the key constructs of this is that we know what 'right' looks like and what 'good' looks like so we can better share the tactics, techniques, and procedures (TTPs) and indicators of compromise that cause fault points, regardless of where they are*," said Air Force Colonel Jordan Cochran, Future Operations Division chief for JFHQ-DODIN. *"I think we ought to do that at speed. We obviously want to get ahead of reacting to an adversary's maneuvers, to be more proactive, so that we're less concerned about the big data problem and more concerned about mission assurance for all the components to be able to do mission essential tasks and functions*."

As DISA works to procure and deliver the remaining systems and define TTPs for leveraging the capability, JFHQ DODIN is defining procedures for a JRSS Operational Board (JOB) it stood up less than two months ago. JOB's role is to provide consistency, guidance and direction for establishing a sound foundational basis across JRSS mission partners, Cochran said. This promises to be very useful as the DCO working group and DISA Global offer up best practices based on input from across the military services and from lessons learned from day-to-day operations.

"*Right now in DCO, there are pockets of excellence throughout DOD, what JRSS is going to be able to do is bring all that together*," Straub said. "*We're going to be able to share our threats, and it is not going have to be through the IT community or through some stove-piped channel or through a memo or an email. It's actually going be through the data source. And we're going to be faster, more flexible, more agile in being able to thwart our enemies and what they are trying to do within our networks. For me, from a DCO perspective, I'm ready to get there because I think it's going to help immensely*."

www.uscg.mil//

www.disa.mil/

SOSi to provide MILSATCOM support for U.S. Army

PEO EIS
Wideband Enterprise Satellite Systems
WESS

www.sosi.com/

www.eis.army.mil/programs/wess

SOS International LLC (SOSi), a mid-tier government services integrator working principally in the defense and intelligence market sectors, is the sole awardee of a $55 million contract.

This award is to provide technical support to the Wideband Enterprise Satellite Systems (WESS) managed by the U.S. Army's Program Executive Office — Enterprise Information Systems (PEO-EIS).

SOSi will support Product Manager WESS Data Communications Network customers worldwide in providing secure and non-secure voice, data and video services and all phases of SATCOM management, engineering, installation, integration, operation, maintenance, and lifecycle support.

Julian Setian, SOSi President and CEO, said that this award demonstrates the synergies the company anticipated from their recent acquisition of STG.

He added that by serving the SATCOM needs of the nation's military under this contract, SOSi is effectively expanding the company's global footprint in support of U.S. Army, U.S. Air Force, and Joint operations, leveraging the firm's decades of experience in managing complex network operations and security.

Oregon Airmen train to support wildland firefighters

Oregon National Guardsmen, including airmen from the 173rd Fighter Wing, train to use emergency fire shelters in Warrenton, Ore., July 10, 2018. Photo is courtesy of the Oregon Air National Guard.

Fifty-seven airmen from the Oregon Air National Guard's 173rd Fighter Wing based at Kingsley Field in Klamath Falls, Oregon, spent two weeks in Warrenton, Oregon, learning to assist wildland firefighters.

This was the first time National Guardsmen were trained before to being tasked to support firefighting efforts in Oregon.

"***In the past, we did not train beforehand, and this caused about a two-week delay in having Oregon National Guard resources ready to deploy***," said U.S. Air Force Chief Master Sergeant James Dean, Chief of the 173rd Mission Support Group. "*Now we are trained and ready to deploy*"

U.S. Air Force Colonel Jeff Smith, commander of the 173rd Fighter Wing added, "*We should cut the response time [by] more than 50 percent, enabling our manpower surge to augment the [Oregon Department of Forestry] and other partners sooner, hopefully minimizing impacts of fire damage.*"

Last year, nearly 100 airmen from Kingsley Field were part of the more than 600 Oregon National Guard soldiers and airmen called to support firefighting efforts across the state. It is anticipated that there may be a similar call this year due to extremely dry conditions across Oregon.

"*As one of the Oregon National Guard's state missions -- to protect our state from natural disasters -- wildland firefighting has become one of the biggest issues for many of the north western states,*" Dean said. "*We have some of the best and brightest on our team, and they come from all ranks, ethnicities and backgrounds; the ability to work together as one team in such a short amount of time in such a hazardous and dangerous environment is truly amazing to see and to be a part of these efforts.*"

National Guard units are tasked with supporting the state and federal governments. Smith said this can be a tricky balancing act at times.

"*We are sworn to support the nation and the state in times of need, and sometimes we have to do both*," he said.

He pointed out that, last year, the 173rd Fighter Wing accomplished just this, supporting all three of its major mission sets simultaneously — deploying in support of global operations, training F-15C Eagle pilots and fighting wildfires in Oregon.

Smith says this was accomplished by being able to call up Drill Status Guardsmen to support these missions. "*Without them, we could not tackle so many tasks at once.*"

Smith noted that this is the wing's mission as well as personal.

"*We live here; we're raising our kids here. Because we're rooted in the community, we're also vested in it. By training to support wildfire fighting efforts, we prepare to defend and preserve the beautiful landscape we're so lucky to have in Oregon.*"

www.173fw.ang.af.mil/

Story by
U.S. Air Force Senior Master Sergeant. Jennifer Shirar
173rd Fighter Wing

Paradigm's SWARM + the R.A.F.

Paradigm's ultra-portable, high throughput SWARM terminal, operating on the Inmarsat Global Xpress network, delivers seamless connectivity for RAF100 Flypast.

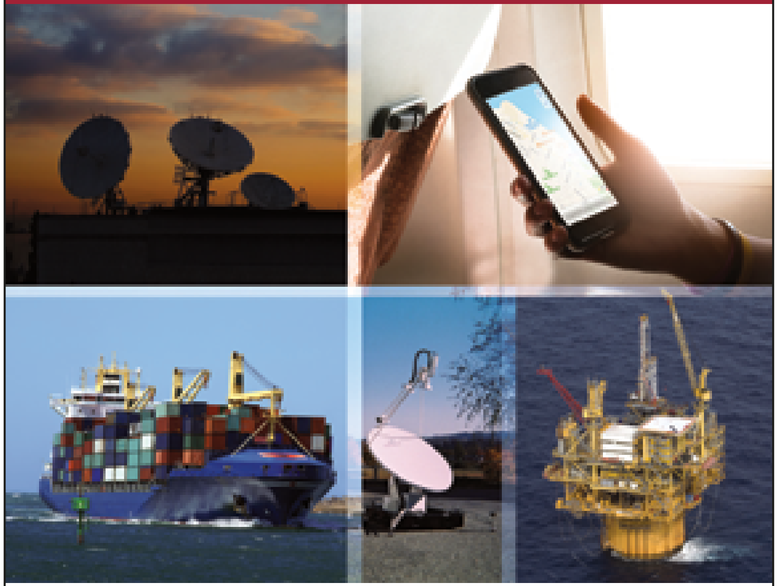
This high-profile event was staged in July by the RAF to celebrate their 100th Birthday and involved 100 aircraft from the past 100 years flying over Buckingham Palace and the skies of London. The small, but powerful, SWARM terminal from Paradigm ensured that the media feed could rely on constant communications throughout the day in the face of high demand from the public on the terrestrial 4G network.

Following the event, Squadron Leader Gordon Henderson remarked on the "*outstanding level of service from the lightweight and easily operated SWARM terminal. By providing the Air Command Media team with access to Inmarsat's Global Xpress connectivity, they were able to continue uploading videos from the parade even as the 4G network in London begun to struggle.*"

The SWARM is small and light enough to be carried in a backpack and really easy to setup and deploy. Even a non-skilled user can set it up and be on the air in less than four minutes.

Later this year, Inmarsat and the SWARM terminal will also provide SATCOM support for the RAF100 Himalayan Venture 18 (HV18)

paracomm.co.uk/



INNOVATION: IDIRECT GOVERNMENT

What Is TRANSEC?

By Karl Fuchs, Senior Vice President, Technology, and Roly Rigual, Senior Director of Systems Engineering

iDirect Government™ (iDirectGov) recognizes the critical need to protect the flow of communications to wherever the military and government agencies may operate. Wherever this may be, threat actors readily stand by to monitor, exploit or intercept communications for malicious intent.

To mitigate this threat, iDirectGov has been providing Transmission Security (TRANSEC) capabilities since the initial release of the Evolution software. With the release of 4.2, iDirectGov has further enhanced their TRANSEC capabilities by extending protection to cover both one-way and two-way networks.

In combatant situations, where even a small "spike" in traffic can be a critical piece of intelligence, the need to mask any communications activity becomes apparent. The National Security Agency (NSA) has outlined the following vulnerabilities inherent in an IP-based TDMA transmission that must be addressed in order to provide true TRANSEC:

Channel Activity
The ability to secure transmission energy to conceal traffic volumes.

Control Channel Information
Disguise traffic volumes to secure traffic source and destination.

Hub and Remote Unit Validation
Ensure remote terminals connected to the network are authorized users.

What is TRANSEC?
TRANSEC prevents an adversary from exploiting information available in a communications channel without necessarily having defeated encryption.

TRANSEC requires all network control channels and Management & Control (M&C) data to be encrypted, and that any and all traffic engineering information be obfuscated from an adversary.

For example, TRANSEC requires a communications channel to appear completely full to an adversary even if little or no actual data is flowing. This is contrasted with communications security (COMSEC); the actual communication (e.g. voice, video or data stream) is encrypted, but certain header information is sent in the clear.

While the encryption is virtually impenetrable, the information in the IP header including the source address, destination address and, most importantly, the Type of Service (ToS) field are in the clear. With the IP header of an encrypted packet in the clear, an adversary can determine how much of the traffic stream is voice, video or data. More significantly, an adversary could determine when high-priority flash-override traffic has been initiated and from which location.

In a traditional SCPC (single channel per carrier) satellite network topology, achieving TRANSEC compliance is relatively straight forward. For SCPC connections, a bulk encryptor is employed to encrypt any data and control information traversing the network.

The IP header of the packet would be encrypted by the bulk encryptor prior to being transmitted to the satellite. In addition, since an SCPC link is static, always on and no control information needs to be exchanged between the SCPC modems, all of the TRANSEC requirements are met.

In a TDMA network, TRANSEC compliance is more difficult. A TDMA network dynamically allocates bandwidth to remotes; therefore, there must be some type of control information transmitted to each device in the network. This control data containing traffic engineering information, as well as information available from an encrypted IP packet header, can be exploited by an adversary.

For example, anomalous traffic volume to a specific remote can indicate new activity in that area while varying ratios of voice-to-data traffic can denote the distribution of intelligence (data) compared to lower priority voice traffic.

iDirectGov has implemented the following solutions in response to the security vulnerabilities of a TDMA Very Small Aperture Terminal (VSAT) network.

Masking Channel Activity

CHALLENGE

The first vulnerability that exists in a TDMA network is the availability of traffic engineering information. In an SCPC network, the link is static with no variation in transmission characteristics based on end user communications. An adversary looking at a satellite transponder with a spectrum analyzer will see a constant RF signal.

This is contrasted with a TDMA network. A TDMA in-route carrier energizes and de-energizes as traffic flows and stops. The on-and-off nature of a TDMA in-route is the natural extension of the ability to allocate satellite transponder space to remotes that have transient demands.

While this characteristic makes TDMA networks much more bandwidth efficient, it allows an adversary to determine peak periods of activity, identify unusual or unexpected activity spikes, and identify locations of remotes that have remained quiet for a period of time and suddenly experience increased traffic volumes.

The obvious risk in having this information in the hands of an adversary is the potential to extrapolate timing, location and scale of a strategic activity.

SOLUTION

iDirectGov has implemented free slot allocation in its TDMA bandwidth distribution algorithm. With free slot allocation, an adversary snooping for satellite transponder energies will see a constant "wall of data" regardless of traffic profiles.

As the name implies, free slot allocation keeps the in-routes active regardless of actual traffic flows. Free slot allocation preserves the efficiencies of a TDMA system while obfuscating actual traffic volumes, negating the risk of using transmission activity as an intelligence gathering mechanism.

Obfuscating Acquisition Activity

CHALLENGE

The rate at which remotes acquire into a network can provide critical information to an adversary about troop activities. All TDMA networks provide a dedicated channel for remote acquisition activity. If adversaries monitor the activity in this channel, they will be alerted to troop movements by a flurry of acquisition activity.

SOLUTION

iDirectGov exceeds TRANSEC requirements by addressing acquisition activity vulnerability. The iDirectGov acquisition algorithm inserts dummy bursts from remotes already in the network and intentionally skips acquisition bursts at times of high activity, ensuring an adversary sees only a random distribution of acquisition activity.

The iDirectGov acquisition algorithm goes a step further by randomly varying the dummy burst's frequency, timing and power. This randomization makes sure an adversary cannot distinguish between a dummy burst and actual acquisition activity.

Control Channel Information

CHALLENGE

A great deal of traffic volume and priority information can be gleaned by examining the in-band or out-of-band control information within an encrypted Time Division Multiple Access (TDMA) network. As previously discussed, the IP header of a packet contains source, destination and priority information.

In order for a TDMA network to provide the quality of service (QoS) needed to support real-time traffic, data quantities and prioritization information must be gathered. This information could be more useful to an adversary than channel activity data because it is specific enough to delineate between general communications like email and web traffic, versus tactical communications like voice and video.

SOLUTION

The only solution for this vulnerability is to completely encrypt all Layer 2 information as well as any control information disseminated to the remotes. The encryption methodology must be secure enough to thwart an adversary long enough that the data becomes old and unusable.

iDirectGov has implemented Federal Information Processing Standard (FIPS) 140-2 certified 256-bit keyed Advanced Encryption Standard (AES) for all Layer 2 and control information. The encryption of the Layer 2 frames has a side benefit of re-encrypting the data payload. Therefore, the transmitted IP header itself is AES-encrypted.

Additionally, the iDirectGov TRANSEC TDMA slot is a fixed size, again to obfuscate any traffic characteristics. This Layer 2 encryption solution solves all existing control channel vulnerabilities. The iDirectGov Layer 2 encryption method goes a step beyond to feature over-the-air (OTA) key updates and a unique Layer 2 frame format, including an Initialization Vector that ensures randomization of repetitive data streams.

The net result is that adversaries are precluded from detecting any repetitive pattern, which can aid in deciphering encryption algorithms.

Hub and Remote Authentication

CHALLENGE

Another vulnerability of a TDMA VSAT system is the concept of Hub and Remote validation. In traditional SCPC architectures, a link remains active for very long periods of time when it is established. Because these connections are fixed, and there is a significant level of coordination between personnel commissioning the SCPC, a high degree of confidence exists that an adversary is not trying to assume the identity of a trusted entity.

In TDMA networks, remotes are routinely coming into and dropping out of the network. This is especially true of networks with mobile or itinerate terminals where terminals are located in moving vehicles, aircraft or maritime vessels. This type of dynamic environment gives an adversary a greater opportunity to obtain a VSAT remote through licit or illicit channels, spoof the device ID and insert a rogue remote into a secure network.

Equally feasible is an adversary acquiring a VSAT hub terminal and coaxing a blue force remote into the adversary's network.

SOLUTION

To mitigate this risk, iDirectGov has implemented X.509 digital certificates on TRANSEC remotes. An X.509 certificate utilizes RSA public key cryptosystem. With this cryptosystem, two related keys are generated: one private key and one public key.

The functionality of these keys is so that anything encrypted with the public key can only be decrypted with the private key, and anything encrypted with the private key can only be decrypted with the public key. In the iDirectGov system, X.509 certificates can be generated via the NMS server.

Certificates are placed on all TRANSEC line cards and Protocol Processors as well as on the remotes. The hub system keeps the public keys of each remote configured to operate on the hub, and the remotes have the public keys of each hub device.

During network acquisition, the remote encrypts its X.509 certificate with its private key, and the hub verifies by decrypting the certificate with the remote's public key and vice versa. This process ensures a remote is not only authorized to operate in the network, but that the hub is a trusted entity.

Operational Implementation

CHALLENGE

Implementing security and ensuring all security policies are followed can be a burden to the soldier in the field. Implementing TRANSEC and performing key management is no exception. Challenges one would face in operating a TRANSEC network include creation, distribution and revocation of X.509 certificates; ACQ and Data Channel key generation, distribution and management; and zeroizing modems.

A robust TRANSEC network also requires the use of at least two network-wide keys: The ACC Key for acquisition, and the DCC Key for the data channel. A long-lived, user-generated passphrase is used to protect the keys during initial commissioning. The use of front panel displays to enter the passphrase and external key fill mechanisms places an undue burden on the warfighter and introduces security vulnerabilities.

SOLUTION

iDirectGov has implemented a FIPS-approved software method of key generation and automatic, OTA key distribution protocol. Generated passphrase is used in Security Level 3, in addition to the requirements of Level 2, are required to be able to detect and respond to attempts at physical access or modification. Not only does the software-based key generation and key distribution mechanism make TRANSEC operation simpler and more convenient for the warfighter, it makes the system much more secure by removing a human from key distribution.

Another advantage of automatic key generation and distribution is that it seamlessly enables a global communications-on-the-move (COTM) TRANSEC network. By automatically generating and distributing new acquisition passphrases, a single, dynamic passphrase can be used across global networks.

Additional Security Measures

FIPS 140-2

The FIPS 140-2 is a U.S. government security standard for accrediting cryptographic modules. The standard is published by the National Institute of Standards and Technology (NIST).

FIPS 140-2 provides stringent third-party assurance of security claims on any product containing cryptography that may be used by a government agency. FIPS 140-2 establishes the Cryptographic Module Validation Program (CMVP) as a joint effort between NIST and Canada's Communications Security Establishment (CSE).

FIPS 140-2 specifies four levels of security when it comes to the design and implementation of cryptographic modules. As described by NIST, the following is a high-level overview of these security levels:

Security Level 1 is the basic level of security. No specific physical security features are required, and only one approved security function algorithm is required.

Security Level 2 requires tamper-evident coatings or seals that must be broken to gain access to the cryptographic keys and critical security parameters.

Security Level 3, in addition to the requirements of Level 2, physical security mechanisms are required to be able to detect and respond to attempts at physical access of modification of the cryptographic module.

Security Level 4 requires a complete envelope of protection around the cryptographic module with the ability to detect and respond to all unauthorized attempts at access.

In addition to the hardware requirements described above, FIPS validation applies to the cryptographic solution as a whole, including the operating system and software.

Enhancing TRANSEC and Security with the 9-Series and DLCs

With the release of iDirectGov's new 9-Series Satellite Routers and Defense Line Cards, the company has expanded the firm's existing FIPS 140-2 certification from Level 2 to Level 3 from our previous line of products.

As part of the effort, iDirectGov developed a TRANSEC module designed to meet the stringent FIPS 140-2 Level 3 requirements as defined by NIST. Through hardware and software development, the embedded, and yet independent, TRANSEC module on the 9-Series and DLCs operates through a separate and trusted path from all other interfaces on the product.

The module also features a strong physical security measure for tamper prevention and the capability to zeroize the security keys or critical security parameters (CSPs) stored on the module itself. If required, the revocation or zeroization of the keys can be accomplished either OTA by the hub operator or locally on the remote by authorized personnel.

One-Way Networks

iDirectGov has further enhanced their TRANSEC capabilities by securing one-way broadcast transmissions

Based on their encapsulation method, LEGS, the iDirectGov platform, can provide the same level of security for one-way networks to that of two-way networks as described earlier. The 900 and 9350, with dual-demodulator support, are capable of dual-domain TRANSEC; the ability to establish two independent chains of trust (sets of X.509s) between two different CAs.

An example use case of this feature would be one demodulator on a two-way TRANSEC network while the second demodulator receives a separate one-way TRANSEC-secured broadcast. Elliptical Curve Cryptography (ECC) is used for key generation along with X.509 certificates for authentication in each security domain.

Founded in 2007, iDirectGov has provided the U.S. Department of Defense (DoD) and other government agencies with hubs and satellite routers deployed worldwide. The proven Evolution platform has shown, to both hub and field operators, the performance and efficiency gains that iDirectGov brings into the realm of satellite communications. The platform is capable of transporting high data rates in either direction using DVB-S2, TDMA and SCPC. iDirectGov's line of satellite routers and hub line cards are designed and have been tested to operate using the NSA compliant TRANSEC and access Wideband Global SATCOM (WGS) satellites.*

** Certification pending.*

Fuchs joined iDirect Government in 2004 as the director of sales engineering, just as the satellite-based IP communications company was expanding its VSAT market presence into the federal government and international Internet Protocol (IP) networking world. With more than 20 years of experience in technology and with the federal government, Fuchs leads iDirect Government's team of federal systems engineers and serves as chief architect for new product integration.

Active in the satellite industry for more than 15 years, Fuchs has contributed editorial to numerous industry publications and he is a Senior Contributor to MilsatMagazine.

Roly Rigual serves as the Senior Director of Systems Engineering at iDirectGov.

Kratos Defense & Security completes second phase of U.S.A.F. satellite ground services study

Kratos Defense & Security Solutions has demonstrated successful performance on the second phase of a pathfinder study for migrating the Command and Control System – Consolidated (CCS-C) ground system to the Enterprise Ground Services (EGS) architecture.

CCS-C currently operates a fleet of more than 20 Military Satellite Communications (MILSATCOM) satellites from four different spacecraft families.

In phase 2, Kratos demonstrated:

(1) Data source independent automation over the EGS message bus using Kratos' TAO-DSI

(2) Web based support schedule creation and execution, also over the EGS message bus

(3) Elastic Telemetry and Commanding Server (TCS)

(4) Cloud deployment, and

(5) automated deployment concepts.

These capabilities were demonstrated on the local Kratos Enterprise Ground Services (KEGS) lab and on a secure commercially available cloud based platform. Following the demonstration, the program office approved starting Phase 3.

Enterprise Ground Services (EGS) is an enabling technology for the U.S. Air Force's Space Enterprise Vision (SEV).

EGS enables a sustainable, resilient space architecture that can respond to threats and protect space-based assets. Two other SEV components focus on enhanced satellite communications and satellite manufacture. Kratos is actively involved in supporting the satellite ground and satellite communications enhancement initiatives.

Fully implemented, EGS will result in a common service-based ground architecture for all U.S. Air Force spacecraft that will enable Air Force Space Command (AFSPC) to fight and win a war that extends into space.

AFSPC is implementing EGS with prototyping activities to mature the concepts, technologies, EGS standards, and transition paths for legacy and future ground systems.

The Kratos study for MILSATCOM is a 27 month effort that consists of four phases and is an essential step in the evolution of CCS-C to exploit the benefits of EGS.

Phase I concluded last June with a successful demonstration. The final study phase will be completed in December, 2018.

Kratos products used in the study so far include EPOCH IPS Telemetry and Command Server; TAO-DSI, a platform enabling communication with external data sources; Webic, an advanced GUI; and Catapult, a schedule display and activity launch platform.

Larry Lind, Vice President, Kratos Federal Solutions Group explained that the biggest driver behind the development of EGS is an increasingly ominous threat environment and the speed with which those threats occur.

Lind added that the transition from stovepiped ground systems to horizontally integrated architectures will optimize resources across space missions, enabling greater resiliency. Kratos' involvement with EGS goes beyond the CCS-C/EGS interoperability study as they are actively involved in defining and redefining the standards that will make EGS a reality.

www.kratosdefense.com/

www.afspc.af.mil/

Viasat gains NSA authorization for their BATS-D device

Viasat's BATS-D AN/PRC-161 Handheld Link 16 radio.

Viasat Inc. (NASDAQ: VSAT) has introduced their Battlefield Awareness and Targeting System – Dismounted (BATS-D) device, known to the United States Department of Defense as the AN/PRC-161 — this product is now authorized by the National Security Agency (NSA) for immediate use by Five Eyes (FVEY) partners and coalition forces, worldwide.

The Viasat BATS-D radio bridges a critical gap between air and ground forces by providing real-time fused air/ground situational awareness to coordinate and direct forces instantaneously via machine-to-machine interface.

The terminal offers warfighters at the tactical edge secure, reliable access to integrated air and ground data for improved situational awareness capabilities and enhanced close air support communications. Empowered with better communications, warfighters can more rapidly engage enemy targets and reduce the risk of fratricide incidents.

The patented AN/PRC-161 BATS-D handheld radio is ideal for bringing full Link 16 network access to FVEY Special Operations and Expeditionary Forces. Security innovations in the AN/PRC-161 BATS-D handheld Link 16 radio, including Type 1 encryption, allow for seamless interoperability with other Link 16 radios such as the Multi-functional Information Distribution System Low Volume Terminal (MIDS-LVT), MIDS Joint Tactical Radio System (MIDS JTRS) and KOR-24A Small Tactical Terminal (STT).

Ken Peterman, President, Government Systems, Viasat, said that Viasat's AN/PRC-161 BATS-D is the world's first and only handheld Link 16 radio and is designed to solve the military's urgent need for a small, secure Link 16 device capable of being employed by a dismounted operator that can seamlessly interoperate between air and ground forces. With NSA authorization, Viasat can speed the time to market.

www.viasat.com

COBRA
X/Ka Triband Maritime terminal enables both WGS and Inmarsat GX Operation.
Patent pending for Flat Panel Antennas for mobility.
Interested in our Flat Panel Antenna development? Contact us for more information
sales@emsolutions.com.au | www.emsolutions.com.au
Another First from
EM SOLUTIONS

INNOVATION: KRATOS DEFENSE

New Government and IC program alternatives

By Jordan Klepper

For a number of years, small satellites have been seen as a way to provide low cost solutions for technical demonstrations. Only recently, have smallsats been viewed as mission-ready for government and IC programs. The commercial world has been quicker to adopt these new platforms than government and IC.

Now, however, the advent of virtualized ground system environments that feature plug-and-play design for simplified setup, automation tools for lights-out operation and complete situational awareness have opened new alternatives for government and IC programs.

While virtualized environments allow IC programs to stand up new ground stations quickly and efficiently there is still some resistance to migrating legacy systems for a number of reasons — time and effort to prepare and complete a successful migration being chief among them. New programs, with no legacy systems to migrate, have been quicker to embrace virtualized environments.

What Does it Mean to be Virtual?
Webster defines virtual as "being on or simulated on a computer or computer network."

For the purposes of this article, virtual is further defined as a system or piece of equipment requiring only Commercial-Off-The-Shelf (COTS) hardware in standard configurations to run. Applying this definition to ground equipment, a virtual ground system or piece of ground equipment can run on a standard server or in a cloud instance with no special or system specific configuration of the underlying hardware.

A Virtual Architecture

Before discussing virtual architectures, a quick synopsis of existing ground architectures is insightful. A traditional satellite control ground system requires basic elements to perform three general functions: Command and Control (C2), Baseband, and Radio Frequency (RF).

> *Legacy Architectures*
> The architecture shown in *Figure 1* below is generally common and known to be reliable among many satellite programs that are operational today.
>
> In a traditional architecture, antenna systems tend to be more expensive and inflexible than the other pieces of ground equipment. In order to mitigate the need for every satellite program to build its own antenna farm, shared antenna systems, such as the Air Force Satellite Control Network (AFSCN), were created to provide a common, distributed antenna system through which multiple Department of Defense (DoD) programs could interface for antenna uplink and downlink services.

Shared antenna systems also exist in the commercial market as well with companies such as Kongsberg Satellite Services AS (KSAT), Swedish Space Corporation (SSC) and Atlas providing services to commercial entities as well as some national programs.

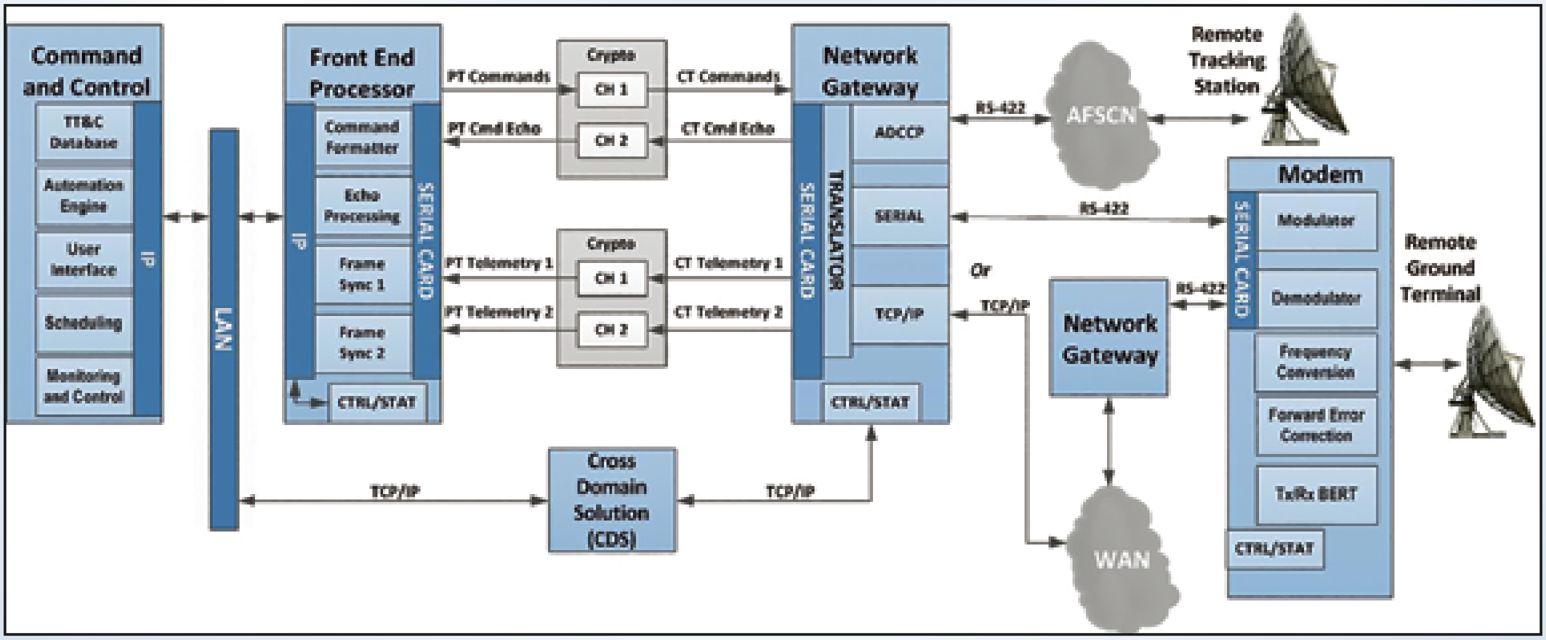


Figure 1: Typical Traditional Ground System Architecture[1]

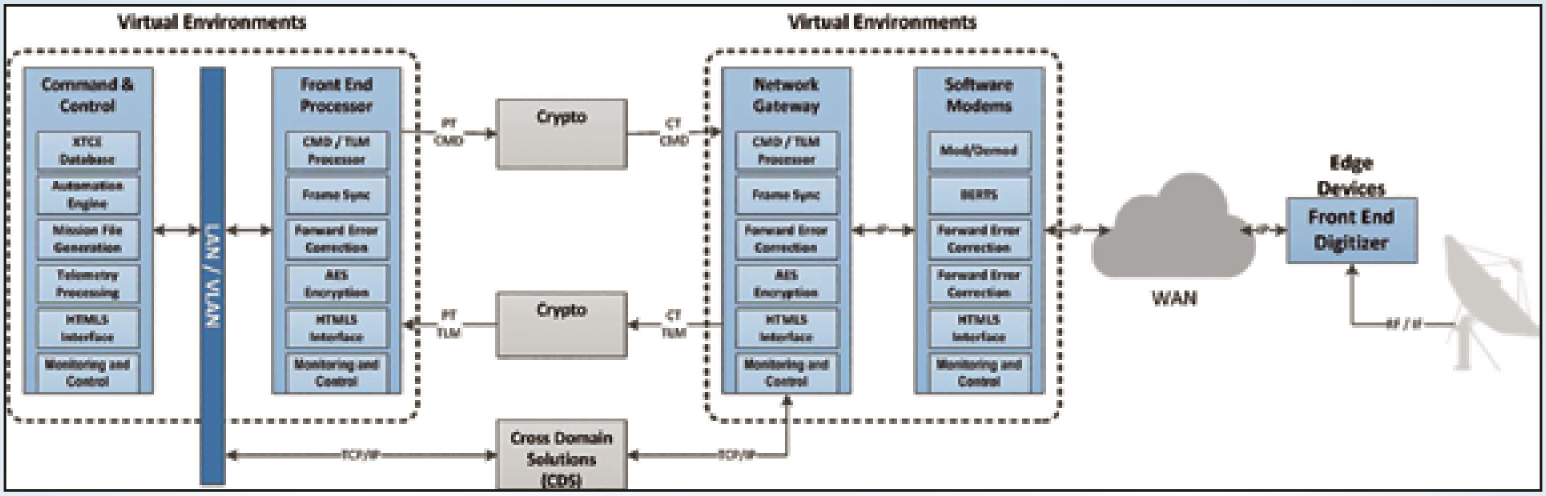


Figure 2. Virtual Architecture.

While shared antenna systems reduce the antenna expense, mission specific hardware or systems may still be required to be co-located at the antenna site. Such co-location increases hardware investments and expands datacenter floor space. Using edge devices, virtual architectures, and even architectures augmented with virtual solutions can result in a reduction in overall operating costs.

Virtual Architectures

Virtual architectures look very similar to the "traditional ground system architecture", yet there are some major differences:

- *Hardware platforms*
- *Data interfaces between components*
- *Configuration flexibility*
- *Cyber security considerations*
- *Reduction in integration labor*

In traditional architecture, the edge device or digitizing front end and modem are in the same hardware package. In a virtual architecture (*see Figure 2 above*), the edge device is a hardware piece that could be co-located at the antenna site.

Now separated from the digitizing front end, the virtual environment could host the modem (software). This lends itself to unique architectures such as distributed ground sites with consolidated processing through RF transport.

Serial communications, as shown in *Figure 1* on the previous page, are common in traditional ground systems. Virtual environments by their nature do not support serial interfaces. However, by using serial to IP converters, items such as legacy serial cryptographic devices can be used in a virtual environment. This is one example of how a current architecture can be augmented with virtual solutions.

There are a number of pros and cons to a virtual architecture and not all differences are listed here. When it comes to small satellites, many of the benefits discussed later drive a small satellite program to a virtual architecture.

A Virtual Ground System: quantum®

For this article, smallsats are defined as "*a small satellite being nominally 500 kilograms.*"

Smallsats require ground systems that match the rapid rate of innovation and reduction in cost that COTS products give them on the spacecraft side. As traditional architectures are unable to rapidly meet the ever-changing needs of small satellites, a virtual ground system environment is the perfect solution for small satellite users.

quantum is the Kratos smallsat virtualized product family that is intended to solve small satellite ground system requirements. The quantum system consists of narrowband and wideband offerings. The system has been designed to support missions through various stages; *i.e.*, development, integration, launch and operations.

Multi-mission and re-use were major development requirements for the quantum system. By ensuring the developed ground system could be used for the current missions, but also for the next several missions, the quantum system is a virtualized solution meeting the majority of users needs. While many users can use a COTS ground system out of the box, provided the system has enough configurability, there will always be those users who need something special.

A virtual environment provides the flexibility for ground system developers to create custom patches to standard baselines allowing them to adapt quickly and efficiently to special customer requests.

While the majority of the quantum ground system is virtualized, there are pieces, which for different reasons, consist of hardware units. These hardware pieces are further discussed in their respective sections.

Narrowband Systems

The quantum narrowband system, in its typical configuration, consists of a digitizing front end or edge device (SpectralNet® Lite), a quantumRadio, quantumFEP (quantum Front-End Processor), and quantumCMD (quantum Command). The quantum system is fundamentally designed to support virtual environments.

The edge device or SpectralNet Lite brings a tunable range of RF frequencies, from IF up to S-band, into the digital domain. For small satellites, this is huge as they only need a single device located at the antenna and can potentially remove block converters from their budget.

The SpectralNet Lite supports the Vita-49 interface to transfer the digitized data into the digital domain, *i.e.*, to a software modem. By embracing open standards, the SpectralNet Lite could theoretically interface with any software modem (supporting the open standard) and as such is a modem agnostic edge device.

The software modem or quantumRadio provides a wide range of modulation and forward error correction schemes. Currently, supporting up to 10 MHz of bandwidth, the quantumRadio is designed to handle narrowband commanding and telemetry links but can also be used for narrowband payload links. This flexibility makes it ideal for supporting a small satellite program.

The front-end processor or quantumFEP handles all of the baseband processing. Supporting a range of data protocols, the quantumFEP also provides encryption services at many different levels. Management of AES keys, their storage, and over the air rekeying (OTAR) are functional capabilities baselined into the quantumFEP.

quantumCMD provides central data management of all core command, telemetry and ground Monitor and Control (M&C) needs common to small satellite missions. (***See Figure 3*** below.)

Wideband System

The quantum wideband system, in its typical configuration, consists of quantumMR (quantum Mission Receiver) and quantumDRA (quantum Digital Recording Application).

quantumMR is a COTS hardware solution tailored specifically to meet data rates of small satellite payload downlinks. The quantumMR can support two independent receive channels, each capable of processing up to 600 Msps, making it a power house in the smallsat receiver market. While the quantumMR is a hardware solution, it was developed with a virtual architecture in mind. By embracing standards such as Vita-49 and CCSDS, quantumMR is highly compatible with a virtual environment. The quantumDRA is a virtual recording application that also provides some high level processing.

Edge Devices

Edge devices will continue to play an important role in virtual architectures. Somewhere in the system, the RF signals have to get into the digital domain. Edge devices perform the function of analog to digital (A/D) and digital to analog (D/A) conversion.

The quantum edge device (SpectralNet Lite) supports an open standard on its data interfaces. This is a key feature that must be supported by edge devices wishing to exist in a virtual environment. By open supporting standards, these devices (along with the antenna system) begin to look like nodes on a network and can be used by just about any software modem anywhere to take a pass.

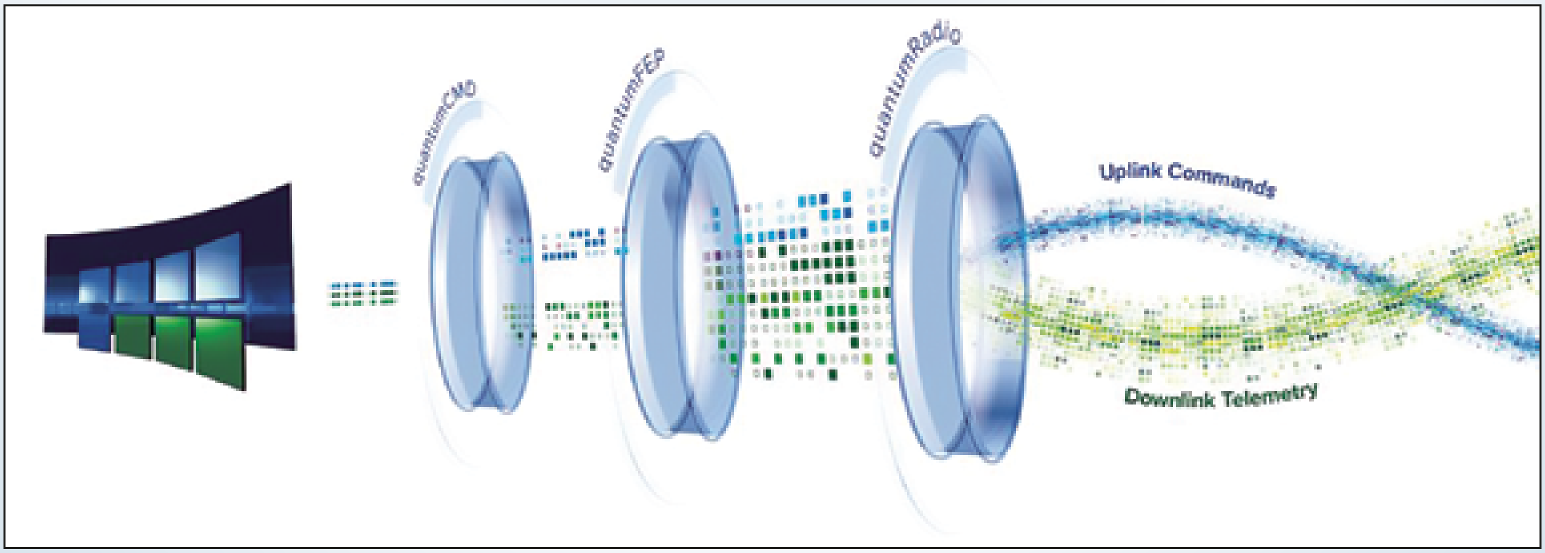


Figure 3. Narrowband Virtual System

Benefits of Virtual Ground Systems

While there are the obvious benefits to virtual ground systems, like total cost of ownership, benefits such as configuration management in a multi-mission environment may not be as obvious.

Multi-Mission

A virtual architecture lends itself well to a multi-mission environment where multiple assets are trying to use the same ground system. Configuration management of ground systems for the multi-missions becomes very important.

The quantum applications allow for application level configuration management. Additionally, VMs have tools (*i.e.*, snapshot and templates) that provide the ability to control configurations at the system level.

Virtual environments allow for ground network service providers to onboard customers quickly and cost effectively. End customers can develop against an instance of the virtual solution and then pass along system configuration files to the network provider. Issues such as different hardware configurations and incompatible pin outs on serial lines that plague hardware solutions do not have any impact on virtual solutions. Additionally, multiple network providers or ground networks can all share the same configuration or even the same instance of the solution (contained in either a virtual machine or container).

Several quantum users today have end customers who use their own instances of quantum that deliver configurations of quantum they have tested. These end customers are able to refine their configurations through various stages of the program, including development, integration and test, through launch and on orbit testing.

Cost

Virtual solutions allow ground systems to scale exponentially with minimal hardware investments compared to hardware solutions. Additionally, cloud computing introduces architectures that reduce the initial capital costs of ground equipment to near zero and missions or programs run entirely on operating budgets. With all that being said, software solutions are not free. Lots of time and effort goes into ensuring virtual products work consistently and that they perform to the same level as the hardware solutions before them.

Delivery

System delivery tends to be the next major pain point. With many hardware based ground systems, typical delivery time frames of three to six months (sometime longer) are not uncommon, whereas quantumRadio has an advertised lead time of less than 30 days.

The ability to deliver virtual ground solutions allows for the rapid deployment of ground sites. Programs that would have taken several years can be deployed in several months. Additionally, new capabilities can be delivered either as updates or as patches to existing systems.

Redundancy and Resiliency

Virtual systems are able to leverage the work going on in other software based environments, one of which is redundancy. With virtual machines (VMs), whole systems can have fail-over capabilities with systems monitoring each other and even fail-over between COTS servers. Kratos has government users who have deployed these architectures to increase the resiliency of their systems today.

Virtual Considerations

Crypto

While many aspects of the small satellite ground architecture have been virtualized, there are a number of things that are much more difficult to virtualize (i.e., serial interfaces). Cryptographic devices used to encrypt commanding data and decrypt telemetry data, especially in the government and IC programs, are hardware systems that are tightly controlled. Virtual systems have the ability to interface with these devices and programs requiring their use.

Many commercial customers today use commercially available AES encryption and decryption to secure their links. quantum supports commercial AES and can support secure links in cloud-based architectures. Small satellites, especially in government programs, have been seen as a way to demonstrate technology. These “tech demos” often have little to no security on the link. quantum offers a way to provide an additional layer of security to these demonstrations.

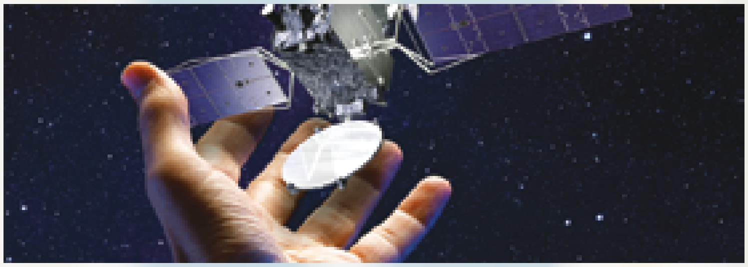
Virtual environments allow for the deployment of new ground stations quickly and efficiently. Virtual solutions can also be used to augment existing traditional systems, as well.

www.kratosdefense.com/

Author Jordan Klepper of Kratos Defense may be contacted at jordan.klepper@kratosdefense.com

MILSATCOM's shifting role

By Ryan Schradin, Executive Editor, GSR, and MilsatMagazine Sr. Contributor



Every now and again, we come to a crossroads in our lives where we're forced to sit down, take a look in the mirror and reflect deeply on our past, present and future. These introspective moments are rare, but they can be revealing — showing us things that we've been doing incorrectly, identifying paths that should be taken and highlighting areas of improvement.

If these moments are rare for people, they're probably rarer for large institutions and organizations. However, the Department of Defense (DoD) recently found itself pausing and taking a deep look within, and analyzing its own approach to satellite requirements and infrastructure.

How did the DoD get to this point? Much of it had to do with timing. The military found itself rapidly approaching the end of the WGS satellite initiative, and the end-of-life of some of the satellites launched early in the life of that program — some of which launched more than a decade ago.

Simultaneously, the military saw massive advancements in the satellite industry — many of which have been discussed extensively on the Government Satellite Report (GSR). New satellite technologies, including the rise of HTS and satellite constellations in new orbits — including LEO and MEO — created new possibilities for the military. These low latency, high bandwidth satellites could offer fiber-like bandwidth to practically anywhere on the planet, and they could do so today — if only the military had access to them.

At a crossroads — having to decide what to do in the wake of the WGS program and wanting to rapidly leverage the advanced technologies entering the marketplace — the DoD did some serious introspective soul searching in regards to its satellite infrastructure. The result? A desire to rely less on purpose-built satellites — launched, owned and operated by the military — and a shift towards working more closely with industry partners to fill satellite communications requirements.

USG to benefit from MEO fleet in 2021

By Peter Hoene, President and CEO, SES-GS

At the annual SMI MilSatCom Conference in 2017, Army Major General Pete Gallagher, former CENTCOM/J6, shared a vignette about U.S. forces fighting ISIS in the CENTCOM Area of Responsibility.

He stated that CENTCOM forces, operating on the ground, were capturing ISIS strongholds that contained "*treasure troves*" of battlefield intelligence, but there was no way to rapidly get that information to exploitation centers and then take advantage of it. He then said, an industry partner came to CENTCOM with a very high throughput and low-latency solution that could get this information to the right people in minutes, not days and weeks like before. He went on to say that this made a big difference for CENTCOM and their planning efforts across the region.

This is just one example of how SES Government Solutions is providing Medium Earth Orbit (MEO) satellite connectivity and solutions for military operations around the world. SES has since added four more satellites to its O3b MEO constellation (now 16 total) and plans an additional four in 2019 (20 total). SES GS, as the only MEO commercial owner/operator, currently provides over five Gigabits per second of MEO High Throughput Satellite (HTS) capability to 21 different U.S. Government sites worldwide.

In April of 2018, SES GS signed a single-award Blanket Purchase Agreement (BPA) with the U.S. Department of Defense (DoD) for MEO low-latency HTS services with a ceiling of $516,700,000 over a five-year period of performance. This BPA allows USG customers to rapidly procure O3b MEO services. There has never been a better time for the U.S. Government to take advantage of high-performance MEO services as well as this new BPA contract vehicle.

MEO missions in the future

In 2021, SES-GS will be able to meet the growing U.S. Government demand for higher throughput and low latency with our next-generation fleet of seven O3b mPOWER satellites.

This shift was reflected in the wideband Analysis of Alternatives (AoA) conducted by the U.S. Air Force. And it's also been reflected in some of the recent reporting making its way into the space and satellite trades. Here are a few examples:

AoA validates expanding commercial role in MILSATCOM architecture

GSR recently dispatched *Warren Ferster* — the former Editor-in-Chief of Space News — to the MilSatCom USA conference organized by SMi Group of London. What Warren heard at that annual conference was very much in line with what was discussed above: The DoD should continue to use a mix of military and commercially owned satellites to serve its wideband communications needs, even as the agency requires increasingly higher levels of protection against jamming and other threats that have emerged in recent years.

Chief among the reasons for this decision to embrace an increasing amount of COMSATCOM services was a requirement to better protect satellites. A hybrid architecture that combines MILSATCOM and COMSATCOM with the ability to switch rapidly between them would best position the military to overcome attempts to deny satellite communications through jamming and other means.

However, there's also the desire to more rapidly take advantage of satellite innovations, which can be utilized sooner and more effectively by partnering with commercial providers — many of which have already built and launched these advanced satellites already.

Just because the desire to increase the use of COMSATCOM services is becoming increasingly pervasive in the government, that doesn't mean there aren't challenges…

To predict the future of military satellite communications, 'Follow the terminals'

The recently-released SATCOM AoA may have determined that it would be advantageous for the military to more broadly and rapidly embrace its commercial partners, but that doesn't mean they're quite ready to do so yet. The satellites, themselves, are really only one part in this equation. There are also the terminals and terrestrial networks that are required to make the whole thing work.

Unfortunately for the military, that side of the equation could be seriously lacking. According to this article in Space News, the military is bullish about embracing commercial SATCOM, but the technology of their terminals lags behind the advanced technologies in commercial satellites. That means the two — quite simply — can't talk to each other.

That's a problem, and a problem that won't be resolved quickly. As Space News noted, "*Because of the cost and the complexity of upgrading military equipment, it could take decades to update or replace all 17,000 wideband SATCOM terminals currently in the Defense Department's inventory.*"

With O3b mPOWER, the company's goal is to offer managed services and solutions that are designed and optimized for the U.S. Government. This fleet will provide an aggregate global bandwidth of more than 420 GHz that is 100 percent fully configurable in terms of power, frequency, and beam flexibility. U.S. Government users will have access to the first global multi-terabit system capable of delivering "*virtual fiber*" anywhere.

O3b mPOWER's secure, flexible and ubiquitous (±50° latitude) connectivity is ideal for today's high-tech military and its network-centric operations, with multiple layers of active and inherent security, and its flexibility to provide data in real time.

The O3b mPOWER system complements SES's existing O3b MEO fleet to connect exponentially more people around the world. The new super-powered satellites will be built by Boeing, SES's first O3b mPOWER technology partner. Existing terminals in the field will also be compatible with the new and current MEO fleets. As part of the O3b mPOWER system, SES and other partners will also develop new Customer Edge Terminals on the ground — converging storage, computing, and routing with software intelligence and specialized antennas.

Government-level encryption mPower

The next-generation O3b mPOWER satellite fleet has multiple layers of security and jam resistance. These include NSA-approved uplink and downlink encryption (CNSSP-12 compliant); inherent jam resistance due to the orbital satellite mechanics, narrow beams and dynamic beam forming capabilities.

The SES-GS satellite platforms are also fully redundant. Since O3b mPOWER satellites are functioning in MEO orbit and are not stationary, they are less susceptible to jamming and interference. We have been a trusted and secure provider of SATCOM for many years. By the time O3b mPOWER launches, we will be operating over 20 MEO satellites for more than seven years.

Beam-forming flexibility

The system will enable government users to securely and autonomously manage beam capacity and location to support secure operations. The U.S. Government will be able to shape, moderate, route shift and switch over 4,000 beams per satellite.

Users in the field will be able to deliver multiple terabits of throughput globally and can scale to tens of terabits. Intelligent beamforming enables the ability to tailor and deliver bandwidth worldwide. With O3b mPOWER, SES GS can land a beam precisely where the customer needs it.

The company also has the ability to land 5GHz of bandwidth into any single spot, or as little as 15 MHz allowing us to serve both high and low-density locations and not limiting us

Regardless, it's only a matter of time before this gets ironed out. In fact, the government's desire to partner with the satellite industry is even creating global alliances with both parties working in partnership to solve some complex problems.

These articles are republished, courtesy of The Government Satellite Report (GSR) and Executive Editor Ryan Schradin*.*

Ryan Schradin is a communications expert and journalist with more than a decade of experience and has edited and contributed to multiple, popular, online trade publications that are focused on government technology, satellite, unified communications and network infrastructure. His work includes editing and writing for the GovSat Report, The Modern Network, Public Sector View, and Cloud Sprawl.

His work for the Government Satellite Report includes editing content, establishing editorial direction, contributing articles about satellite news and trends, and conducting written and podcast interviews. Ryan also contributes to the publication's industry events and conference coverage, providing in-depth reporting from leading satellite shows.

The Government Satellite Report is sponsored by...
SES Government Solutions
www.ses-gs.com

to one or the other. With this system, the U.S. Government can expect a seamless end-to-end service supporting U.S. Government missions on air, land and sea.

Ubiquitous connectivity

Government users can take advantage of O3b mPOWER's global coverage (+/-50 degrees latitude). At launch, there will be more than 30,000 formed beams system-wide providing unrivaled coverage for nearly 400 million km² of the Earth's surface. Together, the low-latency networks will facilitate the massive shift from local storage to cloud-based, network-centric operations, meeting the requirement for an "on-demand" experience virtually anywhere in the world. O3b mPOWER is a system of technology and service partners to innovate, grow and create the most compelling, cost-effective end-to-end experience for our customers.

With the natural disaggregation of the MEO constellation, customizable beam offerings and global presence we see significant potential with government customers. SES GS stands as the only provider of current and next-generation MEO capability to the U.S. Government. While this capability is relatively new, proven, and it powerful. I truly believe that it will change the landscape of connectivity for U.S. forces in the years ahead.

Brigadier General Peter F. Hoene, USAF (Retired) was named President and CEO of SES Government Solutions on January 19, 2015. In his previous role, he served as the Corporate Vice President for Development for SES Government Solutions, headquartered in Reston, VA. As Corporate Vice President for Development, he worked with United States warfighters and other government users to help determine their requirements and offer communications support, hosted payload opportunities, and network solutions. He then communicated those requirements to the SES parent organization to take advantage of existing on-orbit SES fleet capacity, or to influence future satellite designs.

Pete retired from the U.S. Air Force in 2010 as Brigadier General, following 30 years of service. He is a graduate of the U.S. Air Force Academy, as well as a distinguished graduate of both the Air Command and Staff College and the National War College. He holds two masters degrees and served in a wide variety of Space, Command and Control, and research, development, acquisition, test, staff and command assignments.

In his last active duty position, Hoene served as the Defense Information Systems Agency (DISA) Program Executive Officer for Command and Control, where he managed a portfolio of Joint and Coalition Command and Control and Information Sharing programs. Prior to his DISA assignment, he was Commander, 350th Electronic Systems Wing (C2&ISR Wing), Electronic Systems Center, Hanscom Air Force Base, Massachusetts, where he managed a portfolio of 49 command and control (C2), ISR, Space and Cyber programs valued at more than $9 billion.

DISA awards Viasat with connectivity services contract

The United States Defense Information Systems Agency (DISA) has officially awarded global communications company, Viasat Inc. (NASDAQ: VSAT), an eight-year, firm-fixed price contract to provide U.S. Government Senior Leader and VIP aircraft with in-flight broadband and connectivity services.

The base year award value is $55.6 million. The period of performance for the base year award is Sept. 1, 2018, through Aug. 31, 2019. The base year and seven 12-month option periods have a total cumulative value of $559.8 million.

Over the past two and a half years, Viasat has provided in-flight broadband and connectivity services to senior leader aircraft under the AMSS IIa contract, demonstrating the company's satellite communication (SATCOM) capabilities.

Building on the initial contract phase, and leveraging Viasat's continuous improvement, continuous development model, this new contract enables Viasat to provide even more advanced broadband connectivity service options with expanded coverage and increased data rates, as well as enhanced security, resiliency and flexibility.

Viasat's HAN uses cutting-edge hybrid terminal technology to enable automatic and rapid in-flight network switching across Ku- and Ka-band satellite networks as well as multiple orbital regimes for optimized global roaming connectivity. In addition, the HAN leverages Viasat's latest innovations in layered resilience to mitigate against congestion, intentional and unintentional interference sources and rapidly evolving cyber threats in highly contested environments. The HAN is unique to Viasat, and according to the cmpany, not offered by any other service provider today.

The Viasat in-flight internet service has been recognized industry-wide for delivering fast, high-quality, reliable in-flight internet service. As noted by Viasat, the service enables an elite connectivity experience with the ability to use the in-flight broadband connection to stream full-motion high-definition video for en-route Command and Control (C2) missions; to maintain two-way communications through HD video conference calling or voice over internet protocol calls; and to access real-time intelligence and other location-based, live-sensor data for critical decision-making and more.

www.viasat.com

INNOVATION: HORIZON

NewSpace: The next frontier for ISR

By John Beckner, Founder and Owner, Horizon Technologies

On the Libyan coastline in the dark of night, a bedraggled group of African refugees file down a rocky pathway to the water's edge — they look with trepidation at their flimsy craft bobbing a few meters offshore.

The smugglers who organize these voyages hand the refugee "*leader*" (usually the one who can speak some English) a Thuraya SatPhone and tell him to call the pre-programmed number, which is the Italian Coast Guard Alert Center "*as soon as they get out of sight of land.*"

On a nightly basis, ISR aircraft on NATO or FRONTEX missions pick up these frantic, garbled, calls to the Italian Coast Guard and due, to their SIGINT system, are able to pinpoint the location of the handset and coordinate the nearest NATO naval unit to affect a rescue. Regularly, thousands of refugees are saved monthly. However, for those unlucky enough to embark on their journey when there are no air assets in the area, they run a high risk of drowning.

In the very near future, sensors on a constellation of Spire cubesats will allow FRONTEX/EMSA/NATO to have a 24/7 real-time picture of every ship in the Mediterranean, due to the smallsats' AIS and RF transmissions. Any SatPhone call at sea will be immediately correlated with known ship locations, and any uncorrelated phone call/handset location will immediately trigger an alert.

Starting in 2019, refugees in the Med will no longer have to "*hope*" a NATO aircraft is in the air that night watching over them; they will be protected by Lemur smallsats launched by Spire Global, a world leader in Earth Observation (EO) via cubesat.

Today, Spire's more than 50 Lemurs are already providing AIS, micro weather and ADS-B aircraft tracking data to governments around the world. By early 2019, the Lemurs will also have powerful ISR functionality: SatPhone geolocation as well as ESM capabilities (to include radar geolocation and fingerprinting) that will transform space-based AIS correlation.

The term NewSpace is defined as "*an entrepreneurial movement and philosophy encompassing the globally emerging, private, commercial, spaceflight and satellite industry.*" NewSpace is attracting billions of dollars in venture capital investment. Last year, private investors poured $3.9 billion into commercial space companies, a record amount. Experts note that venture capital is flowing into the sector and finding success: More than 120 firms made investments in NewSpace last year, topping a peak of 89 that occurred in 2016.

Artistic rendition of a Spire Lemur smallsat on orbit. Image is courtesy of Spire Global.

While many NewSpace applications are entirely commercial, there are some players such as Spire who are dramatically changing the availability of "*commercial*" ISR data for governments. As the "*NewSpace world*" and associated technologies are moving much faster than the traditional aerospace business cycle, companies that include the likes of Airbus, Lockheed Martin, Leonardo, Boeing, and Raytheon, are all investing in NewSpace startups which have ISR-related products and services and potential value to the government/intelligence customer community.

Under the moniker "*Earth Observation*," these NewSpace companies plan to offer smallsat services which have direct applications in the military ISR world — and these companies have ambitious goals in this market niche. Just as Google Earth suddenly made public a plethora of previously secret military facilities around the world, data from cubesats will have a similar effect. Unlike the larger SIGINT/ELINT intelligence satellites operated by the world's major powers (which are essentially obsolete from the moment they leave the factory), smallsats "*de-orbit*" every two years and are continually replaced with the latest technology.

Small countries who can't afford ISR aircraft, even when leased, will suddenly have access to a steady stream of ISR data. ISR Aircraft and UAVs won't be replaced, but they can be cued and their usage exponentially optimized.

In addition to Spire mentioned above, no discussion of ISR and NewSpace would be complete without a reference to the company Planet. With that firm's last launch of 88 cubesats, the company now has 144 smallsats orbiting the Earth. Planet previously said it would require 100 to 150 of these small spacecraft to be able to photograph the world's entire surface daily and their constellation is now squarely within that target range.

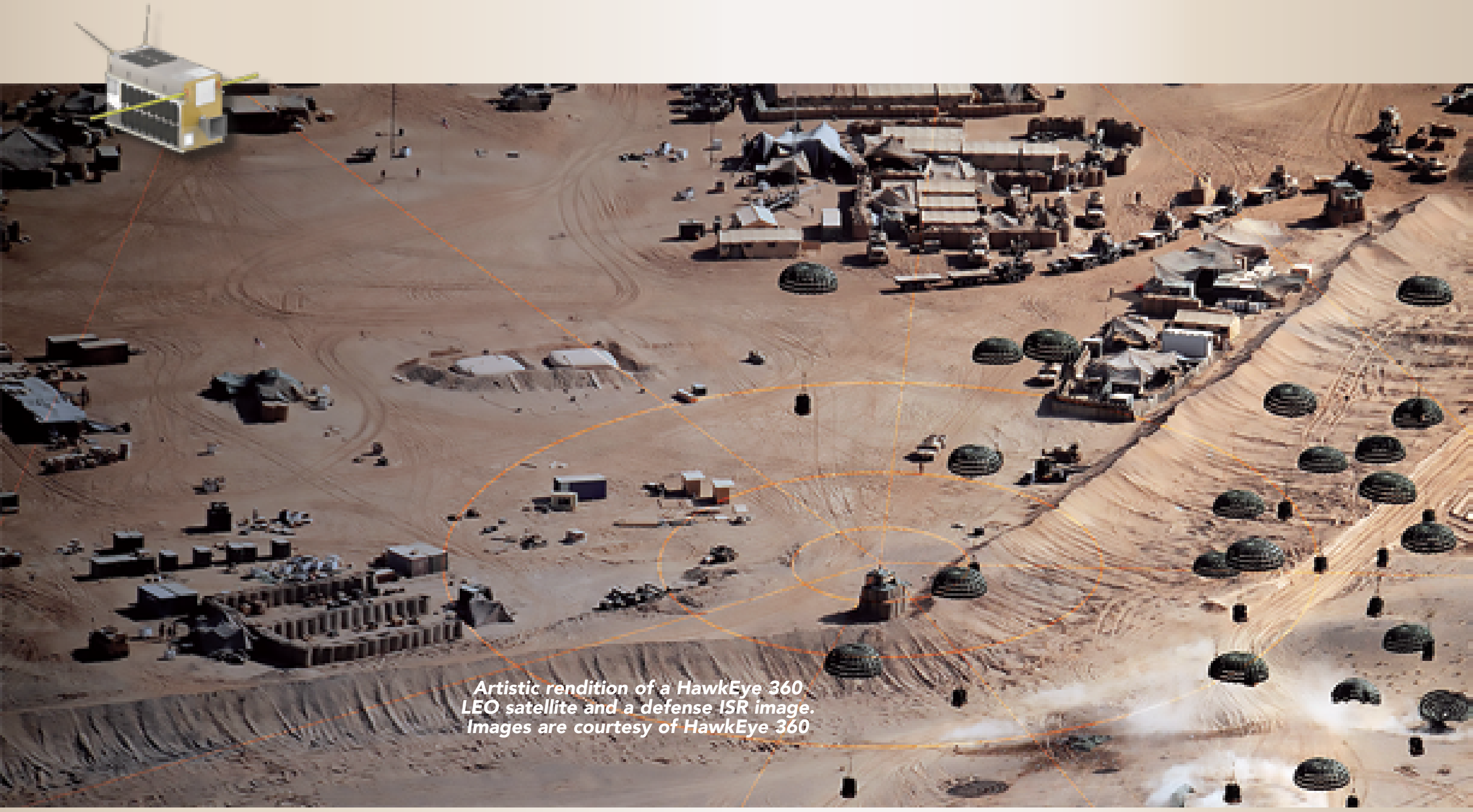
These satellites aren't used to take up-close images, such as of a license plate or a person's face. Instead, they gather wider scale images and pass over the same location at the same time each day, continually comparing the results. Customers, including governments who purchase this data from Planet, use artificial intelligence (AI) to find relationships with data relevant to their particular interest. Planet's imagery acts as a "*time machine*" to go back and look for activity, detected by other means, on a particular place which happened previously in time.

The Washington-based startup Hawkeye360 has attracted major investment from VC funds and U.S. defense primes to offer "*a space-based civil global intelligence network that will use radio frequency (RF) technology to help monitor signals on land and sea and assist with emergencies.*" Their "*product*" is essentially civil SIGINT collection.

They have yet to launch their first group of three (for RF triangulation), somewhat larger, LEO satellites. However, their complex concept, in spite of the high cost, is garnering interest from the U.S. Government and others due to the satellites ' clear ISR value.

The small Finnish startup IceEye has garnered $19 million in VC funding with the laudable goal of using small Synthetic

Planet's Dove smallsats and an ISR defense image capture.
Images are courtesy of Planet.



Artistic rendition of a HawkEye 360 LEO satellite and a defense ISR image. Images are courtesy of HawkEye 360

Aperture Radar (SAR) to monitor the world's ice mass. IceEye's SAR imagery certainly has ISR radar imaging applications, and according to IceEye, the U.S. DoD has already agreed to purchase their imaging data via their DIUx program— and that's before that company's first launch.

In a similar vein, DARPA has realized that they can no longer rely on the big U.S. primes to lead the way in technology — the agency must harness the fast-growing technology of private industry. DARPA recently launched the Blackjack program which asks for "*innovative proposals for low cost, mass reproducible space payloads and satellite buses*."

NewSpace will have a tremendous effect on the military/government ISR world, and much quicker than is generally appreciated. In the maritime arena, illegal fishing, transshipments and smuggling will, essentially, be shut down once enough satellite/sensors are deployed. Any ship with AIS turned off to avoid detection will have to go completely "*dark*." They won't be able to navigate or communicate (in any manner); that's a very dangerous situation for any mariner, especially at night. The situation will be analogous to the early 1940's when German U-boats found it impossible to meet up with U-boat tankers as their communications betrayed them. On land, the effects will be no different. Today's overriding European/NATO security threat is the Russian Army. For those countries that border Russia, real-time ISR data from space (RF emissions and communications) will be an invaluable commodity.

Today, smaller countries simply don't have the means of getting time-critical Russian Electronic Order Of Battle (EOOB) data in their region. They are forced to depend on the U.S. and other NATO assets, such as Rivet Joint, Air Seeker, AGS, and so on. Soon, they will be able to have their own unique ISR data stream — they will be able to make their own, national security decisions based on real-time unfiltered intelligence data.

In sum, NewSpace is not just some commercial Venture Capital "buzzword." NewSpace will have a major role to play in intelligence gathering, and ISR in particular. Countries will no longer have to operate manned and unmanned terrestrial ISR systems to obtain and gather the data that is of importance to them. They can simply purchase the data which is critical to their needs. Smallsat-based ISR will become a service which countries buy, thereby obviating the need for the expensive procurement of terrestrial aircraft vehicles, crews, and support.

As with the first use of aerial balloon observation at the battle of Fleurus in 1794, NewSpace ISR is innovative and transformational and will provide countries with an entirely new source of real-time intelligence information.

www.horizontechnologies.eu/

John Beckner is the founder and owner of Horizon Technologies (www.horizontechnologies.eu) which is a UK startup that, within five years, has become a leader in airborne SIGINT, and ISR.

SAVE THE DATE

SPACE AND SATELLITE PROFESSIONALS
HALL OF FAME
INTERNATIONAL

See the Class of 2019 get inducted!

May 17, 2019
Washington, DC
satellitehalloffame.com

The 2019 Hall of Fame Celebration will be held on May 7th, 2019, breaking with years of winter tradition. Mark your calendar and watch for news of the event as it takes shape!

SSPI
SPACE & SATELLITE PROFESSIONALS INTERNATIONAL

2018 Inductees: Otto Hoernig Jr., Gwynne Shotwell and Terry Hart

INNOVATION — ADCOLE MARYLAND AEROSPACE

It's a small satellite world...

By Darko Filipi, Director of Business Development

Big space had small beginnings — Sputnik, the world's first man-made satellite, was 58 cm (23 inches) in diameter and would fit into the trunk of a family sedan. The first successful U.S. satellite, Explorer I, weighed only 14 kg. (30.66 lb.) and was 203 cm. (80 inches) long by 15.9 cm. (6.25 inches) in diameter and could easily be hoisted aloft by four people — without a crane!

Explorer-1 model being held aloft by the spacecraft's creators.

From those modest beginnings, spacecraft have grown ever larger, heavier, more sophisticated, and significantly more costly. The highly complex satellites produced by today's prime, space-faring nations are routinely the size of a city bus.

The development cycles that lead to these modern behemoths are attributable to ever-increasing technology demands and shrinking risk postures. The cost of building and launching current, state-of-the-art satellites demands that these technological marvels become ever more reliable and long-lived to justify the cost of placing them into orbit.

As this vicious cycle has played out, current generations of U.S. Government spacecraft increasingly include aggregated payloads that meet the demands of multiple users within a single spacecraft.

Unfortunately, as this approach has led to increasingly larger, more sophisticated, and more expensive space assets, the U.S. finds its technological lead in space challenged, not only by traditional rivals, but also by emerging space powers. The historically evolved approach to spacecraft development is not aligned with internet-age technology advances, and the U.S. space enterprise has found that the space environment is increasingly congested, contested, and competitive.

With all of the incredible sophistication built into recent prime space assets, these monolithic and aggregated satellites have such long development cycles that by the time they are deployed, their capabilities may be outdated in light of emerging needs, threats, and insight.

The great irony is that part of the solution to these troubling trends is to go back in time — to smaller, less complex spacecraft — to get to the future. As it happens, while major government and commercial developers have been focused on ever larger and more expensive satellites, innovative forces have been at work on the fringes of the space industry to meet these unfolding challenges head-on — with ever smaller and less expensive satellites.

Cubesats (built and launched in "units" of 10x10x10 cm.) emerged originally as educational projects for university students. Some of these smallsats, being inexpensive to deploy as "rideshare" payloads, have proven to be extremely well suited as testbeds of transformative technologies. These technologies can then be rapidly scaled or further developed based upon lessons learned — inexpensively — from on orbit operations.

With this boot-strap approach, some of the newest and latest space technology is now in the hands of widely varied and non-traditional users. The payload builders and spacecraft bus technology manufacturers benefit from this approach.

These emerging space industry pioneers can rapidly improve their products over short cycle times, including capabilities such as advanced electric propulsion, increasing computer capacity, or laser-based intersatellite communication - all while improving product reliability and driving down costs from operational and manufacturing experience.

Cubesats are quickly growing in capability — and size. Whereas early units were a single 1U cube, these prototypical and educational models were quickly augmented by the addition of 3U cubesats and are now being followed up with 6U and 12U cubesats. The success of these smallsats has also further increased the U.S. Government appetite for other smallsat classes, including 180+ kg. satellites being launched on EELV Secondary Payload Adapter (ESPA) launch opportunities.

These smallsats will never replace the exquisite behemoths that are the backbone of the nation's current space enterprise; however, augmenting current assets with a wide range of smaller spacecraft may be exactly the tool needed to increase resiliency in today's contested space environment.

While the current crop of large platforms routinely achieve capabilities that are well beyond anything a single smallsat will ever be able to deliver, it is possible that clusters of smallsats flying in controlled formations will someday deliver capabilities that single monolithic satellites simply cannot achieve.

Large constellations of inexpensive smallsats also provide other unique advantages — for example, the ability to gather large, spatially and temporally diverse data sets due to frequent revisit times. Another attractive feature of smallsats is the ability to achieve rapid operational deployment (and replenishment), especially if built in advance and stored on the ground to be quickly pulled from a magazine and responsively launched to replace damaged or lost operational units — either partially or completely. With advancements in launch capability, replacement smallsats could be rapidly deployed when and where they are needed to provide responsive intelligence, surveillance, and reconnaissance — or other capabilities.

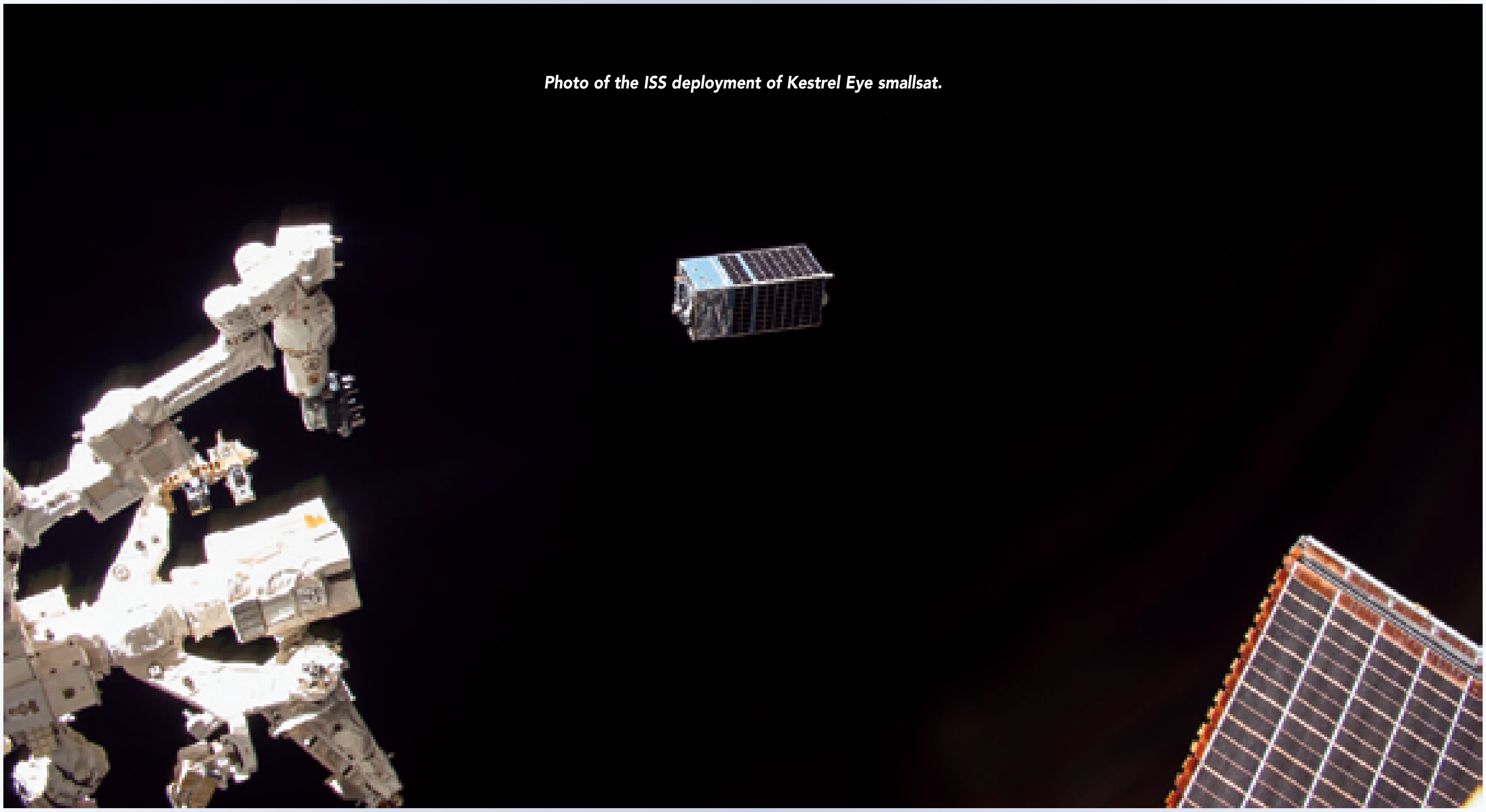
The scientific community has also quickly realized benefits on par with the military utility of smallsats. An entire generation of scientists and engineers is emerging that have not only built a satellite with their own hands, but have witnessed those satellites launched and they have then received their own data from the orbital operations of these satellites — an incredibly valuable education hitherto unavailable to aspiring space explorers.

Furthermore, maturing Principal Investigators have begun to rely on publications from previous smallsat projects to secure funding for new projects. As the trend of satellites becoming larger and more expensive has begun to reverse, access to smallsats is increasing the number of investigators with credentials to lead such missions — a virtuous cycle that is creating the next cadre of Principal Investigators to enhance and eventually replace the existing cohort of space scientists.

Perhaps even more surprisingly, commercial ventures have rapidly embraced the smallsat revolution to provide services that were previously only available to governments from space-faring nations.

In the past, when a government organization needed data, they would develop a mission concept, finance the design and manufacture of the space assets, and obtain the data

Photo of the ISS deployment of Kestrel Eye smallsat.



they needed — putting such ventures out of the reach of disadvantaged users.

With commercial providers (sometimes funded by Venture Capital), the data or information is the product — a product that can be shared with many customers, within and outside of space-faring governments, reducing overall mission cost and releasing hardware providers to do what they know best. To maximize the utility of the aforementioned benefits of smallsats for government users, procurement approaches and mindsets need to realign with the evolving space enterprise. NASA and the U.S. Air Force have successfully used Other Transactional Authorities (OTAs) to develop and set the stage for acquisition of capabilities that would have otherwise never materialized.

A highly successful example is NASA's International Space Station (ISS) resupply program, known as Cargo Resupply Services. This development program was known as Commercial Orbital Transportation Services (COTS). Within a period of less than five years, NASA's COTS program resulted in two companies that deployed two dissimilar end-to-end systems — including two new launch facilities (at the Wallops Flight Facility and Kennedy Space Center); two new launch vehicles (Antares and Falcon 9); and two new space vehicles capable of autonomous travel to the space station without the need for onboard human pilots (Cygnus and Dragon).

If the Department of Defense and other U.S. Government agencies can harness the creativity and efficiency of today's commercial space industry using similarly flexible procurement strategies, the future for small satellite space could be breathtaking. (ed note: see NASA Critical Knowledge captured from the COTS procurement and execution, ***www.nasa.gov/content/cots-critical-knowledge-0***)

Such procurement approaches could match the innovative potential of small satellites, unleashing a wave of space exploration. Correctly and carefully applied regulations, domestic and international, can help foster the burgeoning smallsat industry.

There will be many challenges. Congestion is a common concern in the industry due to both physical conjunctions and radio frequency allocations. Some challenges can be ameliorated with technology, such as improved space situational awareness (reducing conjunction false positives) or laser-based communication, but the cooperation of existing operators in established orbits with new entrants seeking access to space is essential for the success of the industry.

Companies, such as Adcole Maryland Aerospace (AMA), have been on the front line for this new generation of smallsats. AMA built the first self-contained attitude control system for CubeSats and recently delivered the Kestrel Eye tactical imaging satellite to the US Army Space and Missile Defense Command. The experience of such companies has vastly improved and rapidly grown over a short period of time.

Smallsats will provide the capability for evolving concepts, such as responsive imagery direct to the warfighter, monitoring of deforestation, Maritime Domain Awareness — and perhaps, someday, lunar or Mars communication infrastructures, dissimilar spacecraft-borne sensors orbiting Europa, and many others... **large dreams can fit into compact packages**.

Adcole Maryland Aerospace was formed in April 2017 through the merger of Maryland Aerospace, Inc. (MAI) and the Adcole Corporation's aerospace division. MAI has long been a leading provider of Small Satellite and CubeSat components as well as end-to-end space systems. Adcole Corporation, now in its 60th year, has been the trusted supplier of radiation hardened and high reliability sun sensors for hundreds of LEO, GEO, and interplanetary space missions. More information about the company is available at www.adcolemai.com.

Darko Filipi is the Director of Business Development for Adcole Maryland Aerospace, LLC. In this position, he leads business development across all sectors. Before joining Adcole Maryland Aerospace, Mr. Filipi was the Deputy Director of Operations and Engagement Program Manager for the ARES Corporation in Vienna, Virginia. While with ARES, he planned and executed project tasks, and managed customer relations for the office and programs within NASA Headquarters OCT, OSMA, HEOMD, and OCE.

Mr. Filipi also worked at Orbital ATK/Orbital Sciences Corporation, in Dulles, Virginia, as a Systems Engineering for eight years. There, Mr. Filipi lead human rating efforts for two key elements of the NASA Orion Launch Abort System. As part of the Orbital ISS Commercial Resupply Services (CRS & COTS) programs, he supported the Program VP for Operation, Chief Engineer, Lead Systems Engineer in implementing incremental changes to the program, based on internal and customer direction. For the Stratolaunch Orbital Launch Vehicle, Mr. Filipi organized key reviews, including a PDR, and established the Risk Process for the program.

SATNEWS PUBLISHERS

DIGITAL EDITIONS

SatMagazine • MilsatMagazine • SatNews.com

» *Free subscription and access*

Timely news and editorial «

» *Complete archives*

Join at: *satnews.com/reg*

THE AEROSPACE CORPORATION: AN ANALYSIS

Launching U.S. government payloads on foreign soil

By Barbara M. Braun and Eleni M. Sims

The emergence of new, venture-class launch providers for small satellites has led to questions about the suitability of these launch providers for U.S. government missions.

In particular, many of these emerging launch providers, including Rocket Lab USA and VOX Space, are subsidiaries of foreign companies or maintain launch sites in foreign countries. As a set of policies and laws exist that require U.S. government satellites to be launched on U.S. launch providers, many U.S. government agencies are investigating the legal and policy implications of launching with these providers.

Several U.S. law and policy statements require launch vehicles for U.S. Government satellites to be manufactured in the United States. Title 51 of U.S. Code (National and Commercial Space Programs)[1] requires "the Federal Government [to] acquire space transportation services from United States commercial providers." Title 51 goes on to define a United States commercial provider as one that is "more than 50 percent owned by United States nationals."

Additionally, Title 41 of U.S. Code, Sections 8301-8305 (the "Buy American Act")[2] stipulates that for an item to be considered manufactured in the United States, at least 50 percent of all its components, by cost, must be manufactured in the U.S.

In addition to the laws documented in U.S. Code, multiple policies exist that dictate which launch vehicles can be used by U.S. government programs. The National Space Transportation Policy (NSTP) states as a goal, "United States Government payloads shall be launched on vehicles manufactured in the United States unless an exemption is coordinated."

Department of Defense Instruction (DODI) 3100.12, "Space Support," states that "DoD payloads shall be launched on U.S. manufactured launch vehicles" and that "U.S. commercial space launch services shall be utilized to the fullest extent feasible… in accordance with [the National Space Transportation Policy] and [the Commercial Space Act of 1988]."

These laws and policy statements establish a two-part test to determine if a launch vehicle is manufactured in the United States and thus allowed to launch U.S. government satellites. The two tests are:

1. Is the launch vehicle company more than 50 percent owned by United States nationals? (required by Title 51 of U.S. Code and DODI 3100.12)

2. Are 50 percent or more of the launch vehicle components, by cost, manufactured in the United States? (required by Title 41 of U.S. Code and the National Space Transportation Policy)

Most government launch agreements are also subject to the Federal Acquisition Regulation. The Federal Acquisition Regulation states that the place of manufacture of an item is "*predominantly in the U.S. … if the total anticipated price of offered end products manufactured in the United States exceeds the total anticipated price of offered end products manufactured outside the United States.*"

This is similar to the second test listed above, but Part 52.225-18 of the Federal Acquisition Regulation also defines the "*place of manufacture*" as "*the place where an end product is assembled out of components.*" Although U.S. government launch agreements exist that are governed by transaction authorities other than the Federal Acquisition Regulation, they sometimes use similar language.

This language appears to establish a third test to determine if a launch vehicle is manufactured in the United States; namely, is the end product assembled out of components in the United States?

However, most argue that this third test does not apply to launch vehicles because the government typically buys a launch service (the delivery to orbit), not the launch vehicle itself. In these cases, the government does not take possession of the launch vehicle, and, therefore, the launch vehicle is not an "end product," as defined by the Federal Acquisition Regulation.

Also, a launch vehicle can often only be assembled into its launch configuration at the launch site. It is not clear if the Federal Acquisition Regulation considers final integration with the payload an "*assembly out of components*" for the purposes of determining if the launch vehicle is manufactured in the United States. If so, it could have the unintended consequence of precluding all U.S. government launches from outside the United States.

Recently, leadership from NASA and the DoD have issued determination letters indicating that Rocket Lab USA, which meets the first two tests but which launches out of New Zealand, is considered a United States commercial launch provider for the purposes of launching U.S. government experimental payloads.

Given that determination, NASA and the U.S. Air Force are planning launches of experimental small satellites on Rocket Lab USA Electron vehicles. Both determination letters note that this is an "*interim position*," however, and not "*dispositive of future decisions*."

As venture class vehicles are proliferating, and the U.S. Government is looking to expand launch partnerships across the globe, clarifying the regulatory landscape surrounding launches from foreign soil will be necessary. The U.S. government will need to balance policy decisions that protect the domestic launch industry and its U.S. government payloads, while assuring access to space by fostering competition and opening doors to more launch providers and sites.

www.aerospace.org/policy

References

[1] *Title 51, United States Code, National and Commercial Space Programs, December 18, 2010, http://uscode.house.gov/view.xhtml?path=/prelim@title51&edition=prelim.*

[2] *Title 41, United States Code, Public Contracts, January 4, 2011, http://uscode.house.gov/view.xhtml?path=/prelim@title41&edition=prelim.*

Barbara M. Braun joined The Aerospace Corporation in 2000 and has supported multiple small satellite and rideshare missions for the Department of Defense Space Test Program, the Operationally Responsive Space Office, and NASA. She served in the U.S. Air Force for 21 years, on active duty and in the reserves, where she worked on space safety policy for the U.S. Air Force Safety Center.

Eleni M. "Sam" Sims is a project engineer in the Space Innovation Directorate. She provides technical support to the Air Force's Advanced Systems and Development Directorate — specifically, the DoD Space Test Program — by architecting advanced science and technology missions. She is the lead technical support for three satellites on the STP-2 mission, which is scheduled to launch in 2018.

About the Center for Space Policy and Strategy

The Center for Space Policy and Strategy is dedicated to shaping the future by providing nonpartisan research and strategic analysis to decision makers. The Center is part of The Aerospace Corporation, a nonprofit organization that advises the government on complex space enterprise and systems engineering problems.

BOOK BY 28TH SEPTEMBER TO SAVE £100

SMi Group's 20th Annual

SMi
LINKING BUSINESS *with* INFORMATION

Global MilSatCom

CONFERENCE & EXHIBITION 2018

Europe's Leading Military Communications Event for Satellite Professionals

Focus day: Monday 5th November 2018 | St. James' Court, London, UK
Conference: Tuesday 6th November - Thursday 8th November 2018 | Queen Elizabeth II Centre, London, UK

HOST NATION KEYNOTE ADDRESSES:

- **Name to be Confirmed,** Minister for Defence Procurement, **UK Ministry of Defence**
- **Captain David Moody,** SATCOM & Strategic Networks, **UK MoD**
- **Mr Nick Ayling,** Cyber and Space Policy, **UK MoD**
- **Dr Michael O'Callaghan,** Space Programme Manager, **Dstl**
- **Mr Julian Knight,** Head of the Networks Delivery Team, **UK MoD**
- **Mr Mike Rudd,** Head of Telecommunications Strategy, **UK Space Agency**

KEYNOTE ADDRESSES:

- **Colonel Jae Soong Lee,** Chief, Defence Communication Command, **Republic of Korea Armed Forces**
- **Colonel Shinichiro Tsui,** Counsellor, National Space Policy Secretariat, **Japanese Cabinet Office**
- **Ms Deanna Ryals,** Chief, International Programmes Division, Military Satellite Communications Systems (MILSATCOM) Directorate, Space and Missiles System Centre (SMC), Air Force Space Command, **US Air Force**
- **Dr Brian Teeple,** Deputy Chief Information Officer, CIO (C4IIC), **US DoD**
- **Colonel Cameron Stoltz,** Director General of Space, **Canadian Armed Forces**
- **Colonel Laurent Jannin,** Head of French SATCOM Programs, **DGA**

MILITARY AND GOVERNMENT SPEAKERS ALSO INCLUDE:

- **Brigadier General Carlos de Salas,** Head JC4ISR & Space Programs, **Spanish MoD**
- **Colonel Jeffrey Schroeder,** Director of J6 Command and Control Directorate, **US AFRICOM**
- **Wing Commander Paul Drysdale,** JSO1 Joint Communication and Information Systems, **New Zealand Defence Forces**
- **Lieutenant Colonel Michael Hose,** Deputy Director – Australian Defence SATCOM System Joint C4 Capability Branch, **Australian Defence Forces**
- **Lieutenant Colonel Luigi Mauro,** SATCOM Systems Section Head, **Ministry of Defence, Italian MoD**
- **Lieutenant Colonel Eric Trias Phd,** Commander, Space Command Cyberspace Support Squadron, **US Air Force**
- DISA **Ms Clare Grason,** Division Chief, Satellite Communications, **Defence Information Systems Agency (DISA)**

NEW FOR 2018

5TH NOVEMBER: SMALL SATELLITES AND DISRUPTIVE SPACE TECHNOLOGY FOCUS DAY SPEAKERS INCLUDE:

- **Squadron Leader Adrian Holt,** Innovation Scout, JHub, **UK MoD**
- **Dr Fred Kennedy,** Director, Tactical Technology Office, **DARPA**
- **Dr Robert Bond,** Head of Future Propulsion, **Reaction Engines Ltd**
- **Mr Luis Gomes,** Chief Technical Officer, **Surrey Satellite Technology Limited**
- **Mr Andrew Strain,** Chief Technology Officer, **Clyde Space**
- FCC **Mr Jose Albuquerque,** Chief, Satellite Division, **Federal Communications Commission**
- **Mr Simon Gwozdz,** CEO and Founder, **Equatorial Space Industries**

*Subject to Final Confirmation

LEAD SPONSOR

SES Networks

GOLD SPONSOR

AIRBUS

SPONSORS

COMSAT eutelsat GOV SAT HUGHES INTELSAT General Corporation KRATOS
Lockheed Martin Newtec Raytheon SES THALES Viasat

EXHIBITORS

COMTECH DATAPATH ExoAnalytic inster INTEGRASYS
PlaneWave INSTRUMENTS SCISYS XTAR

To keep updated with programme developments or to reserve your place, please visit:

www.globalmilsatcom.com/milsatmag

in Global MilSatCom Community #GlobalMilSatCom @SMiGroupDefence

CPD CERTIFIED

NORSAT INTERNATIONAL: TECH

Mitigating vibration effects on the performance of the synthesizer in a block upconverter

By Mehdi Ardavan, RF Antenna Systems Engineer, and Lewis Siempelkamp, Mechanical Engineer

Electronic equipment used in Communications-on-the-Move (COTM), or airborne applications similar to what is shown in *Figure 1*, can be exposed to mechanical vibration.

Standards such as RTCA/DO-160 or MIL-STD-810[1] [2] define a set of environmental conditions, including vibration, under which the equipment is expected to maintain a satisfactory performance. Among all communication equipment, synthesizers and, thus, block upconverters (BUC) are known to be susceptible to vibration.

The problem can be mitigated at the circuit and system design levels. At the circuit design level, modifying some electrical parameters such as the phase-locked loop filter bandwidth can decrease the susceptibility to vibration[3]. At the system level, using vibration isolators may prove effective. This article focuses on the use of vibration isolators and the mechanical aspects of mounting the synthesizer printed circuit board inside a BUC.

To measure the susceptibility to vibration of a synthesizer usually phase noise (PN) and jitter are used. The phase noise is the deviation of an amplifier or synthesizer from its expected frequency. The frequency contents of a supposedly sinusoidal signal at frequencies adjacent to its center frequency is plotted against the offset frequency with respect to the total power of the signal. Presented are the single side band (SSB) phase noise plots for an offset frequency range of 10 Hz to 100 MHz. A certain type of vibration may have different effects on different subsections of the offset frequency range, hence the shape of the PN curves are important as they answer the question of how the vibration affects the phase noise of a device.

To answer the question of how much in total the phase noise is affected by vibration, a single value, the integrated phase noise (IPN) is used. The IPN, expressed in radians, is equal to the square root of twice the integral of the SSB phase noise in the desired offset range. The jitter, measured in seconds, is a time domain parameter which measures the deviations from the periodicity of a signal and is equal to the IPN divided by the angular frequency of the main signal. We discuss the phase noise results only as the jitter can be directly determined from the IPN and center frequency.

Figure 1. A military aircraft equipped with communication devices

Both PN and jitter represent some component-level behavior of the synthesizer or the BUC. To investigate the system-level effects, the bit error rate (BER) is used in a RF loop back system which is explained later in the article.

The synthesizer of a 25W Ka-band Norsat ATOM BUC prototype is used to conduct this investigation. To reduce the number of unknowns, we limited the scope of the investigation. A BUC has several boards, and each might have certain sensitivity to vibration. However, the synthesizer, by far, is the most susceptible part in the BUC to vibration.

Other blocks, such as the SSPA, have negligible sensitivity to vibration compared to the synthesizer[4]. In this investigation, the authors expose only the synthesizer to vibration. Fortunately, anticipating vibration-related issues, the Norsat synthesizer board was designed and implemented on a separate printed-circuit board (PCB) to facilitate isolation. Therefore, the synthesizer board connections were extended in order to bring it out of the BUC and mount it on the vibration table. Although all sub-assemblies of the BUC are part of the test setup, the synthesizer board is the only component in vibration.

In this article, the PN of the BUC and the BER of an RF loopback system when no vibration is present is measured and then the problem when vibrations of different intensities in two different dimensions are applied to the synthesizer board with no vibration isolators are demonstrated. Then the effects of two different vibration isolators are investigated. At last, some recommendations are presented to improve the vibration isolation in future design revisions.

I. Vibration Profiles and Isolators

Satellite COTM refers to a ground, maritime, or airborne vehicle equipped with an antenna system capable of maintaining communication while in transit. The antenna system, and therefore the BUC, is mounted to the vehicle which exposes the system to vibration produced by the vehicle and its interactions with the medium it is transiting on/through (ground, water, air).

The vibrating environment from a given COTM application can be recorded by taking measurements from an accelerometer, from which a statistical representation of that recording, its vibration profile, can be generated. The vibration profile can be later played back on an electrodynamic shaker with a capable controller that effectively emulates the vibration seen by the system in a real COTM environment.

Emulating the vibration environment in a lab reduced the need to qualify a product in situ and allows for testing to be performed earlier in development than possible otherwise. Various standards (see MIL-STD-810G[1], RTCA/DO-160G[2], IEC 60068-2-64[5] have cataloged vibration profiles across a broad array of ground, maritime, and airborne vehicle models and environments.

A review of vibration profiles presented in MIL-STD-810 Method 5.14 shows a general trend of increasing harshness of vibration from maritime shipboard environments to ground transport and then to airborne applications having the most extreme operating environments.

A single airborne vibration profile was selected to measure the performance of the BUC against, DO-160G - Section 8 - Category S – Curve C (Fixed Wing Aircraft – Fuselage). This curve is closely matched by MIL-STD-810G – Figure 514.6C-5 Jet Aircraft Cargo "General Exposure." The selected profile's acceleration spectral density (ASD) curve is shown in *Figure 2*. This profile will be referred to as the 160G-8SC profile.

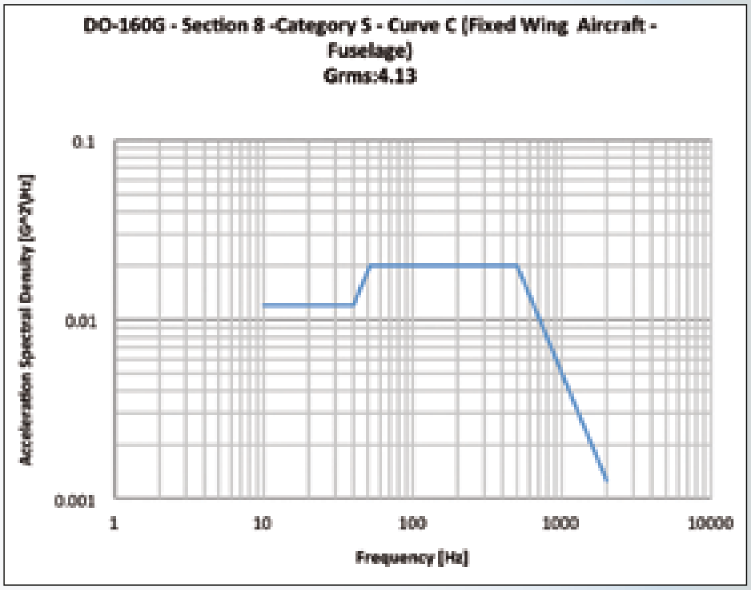


Figure 2. The acceleration spectral density of the 160G-8SC vibration profile

Just as gaskets are used to isolate the internal environment of the BUC from external moisture and dust, elastomeric mounts are used to provide passive isolation of the BUC's structure and sensitive internal circuitry to vibration exposure from the operating environment. These mounts come in a variety of geometries, load ratings, stiffnesses, and materials that dictate the vibration transmissibility of each mount which can be chosen to suit the environment and application.

In this series of tests, the performance of the BUC is measured in a small array of mounting configurations comparing rigid mounts to isolated mounts while only the synthesizer board is exposed to the selected vibration profile. The two isolating mounts used in this round of testing, type A and type B, have similar load ratings, stiffnesses, and construction but their material and geometry differ, suggesting that their vibration transmissibility may as well. One purpose of this test is to determine how these differing properties will impact the phase noise and in what way.

II. Test Method

The phase noise of the BUC and the BER are measured while the synthesizer board is both at rest and exposed to vibration first in x and then in y dimension. The vibration table provides vibration only in one dimension. We mount the device in different orientations to achieve vibration in different dimensions.

The BUC is opened, and the connection cables of the synthesizer board are extended to allow its mounting on the vibration table. As a baseline measurement, the synthesizer is mounted using rigid standoffs and the phase noise and BER are measured with no vibration in effect. The measurements are repeated for different vibration intensities of 5, 10, 25, 50 and 100 percent, first in x and then in y direction. The 100 percent intensity is the 160G-8SC profile.

The rigid standoffs are replaced with type A isolators and the measurement is repeated in the two directions and with different vibration intensities. Then type A isolators are replaced with type B isolators and the tests are repeated. The test setups are explained as follows.

a. Phase Noise Measurement

The SSB phase noise of the BUC in Ka-band is measured for the 10 Hz to 100 MHz range by a spectrum analyzer. The spectrum analyzer also directly provides the IPN and jitter.

b. Bit Error Rate Measurement

The BER can be measured building an RF loop where the BER measurement device is connected to the modem. The transmit port of the modem is connected to the BUC which is connected to a test loop translator (TLT). The TLT is connected to a low-noise block which is then connected to the receive port of the modem through a noise generator. The noise generator is used to decrease the signal-to-noise ratio without having to decrease the signal power to the detection threshold of the modem.

The modem provides a QPSK modulation with ½ Viterbi coding and all power levels and attenuations are adjusted such at the (C+N)/N of the received signal at the modem is approximately 6.8 dB (theoretically equivalent to an Eb/N0 of 5.8 dB when the symbol rate is equal to the bit rate that is 2048 kbps) and the modem measures an Eb/N0 of about 5.5 dB. This Eb/N0 was chosen because it leads to a BER at the order of 1E-7 which stabilizes in a reasonably short time and also if it degrades even by three or four orders of magnitude, the modem usually is still capable of maintaining a receive lock. This tolerance for degradation in the BER allows for a quantitative measurement of the vibration effects.

III. Results

The results are presented in this section and analyzed in the following section.

a. The Synthesizer on Rigid Mounts

The synthesizer board, after extending its cable connections, is mounted on the vibration table using rigid screws. The phase noise of the BUC, and the BER are measured while the synthesizer is at rest and while exposed to vibrations of different intensities at x and y directions.

Figure 3 presents a picture of the synthesizer board on the vibration table and Figure 4 shows the phase noise plots of the BUC for a range of 10 Hz to 100 MHz. All results are summarized in ***Table 1*** placed later in this article, where BER values are reported only if the modem maintains the link.

The phase noise curve of the baseline measurement, i.e. the 0 percent vibration intensity, is below the rest as expected. It yields an IPN of 44.6 mrad and a steady BER of 3E-7 is measured. From Figure 4, it is evident that (a) the phase noise is raised significantly as vibration intensity increases for offset frequencies of less than 1 MHz, and (b) that the increase in the phase noise is more severe when the vibration is in x direction.

b. Synthesizer on Type A Mounts

The rigid mounting screws are removed, and the synthesizer is connected to the table using the type A vibration mounts. The phase noise, jitter, and BER are measured while the synthesizer is exposed to vibrations of different intensities at all directions, and the phase noise plots are shown in ***Figure 5***.

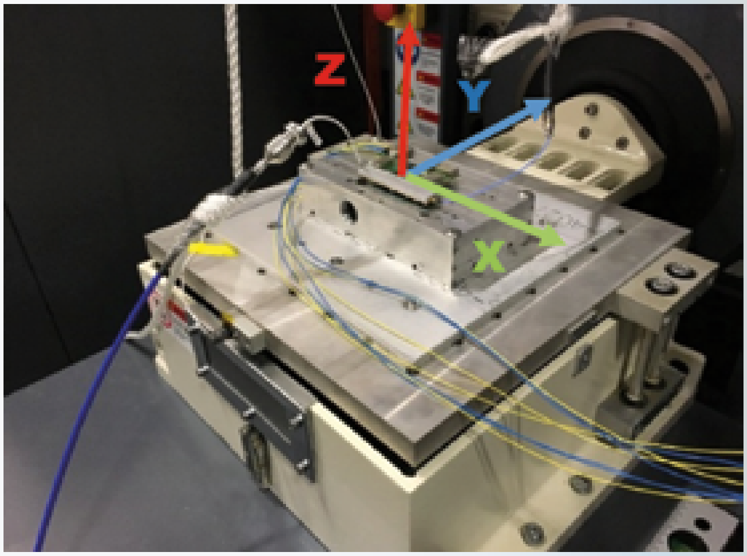


Figure 3. Synthesizer board on vibration table.

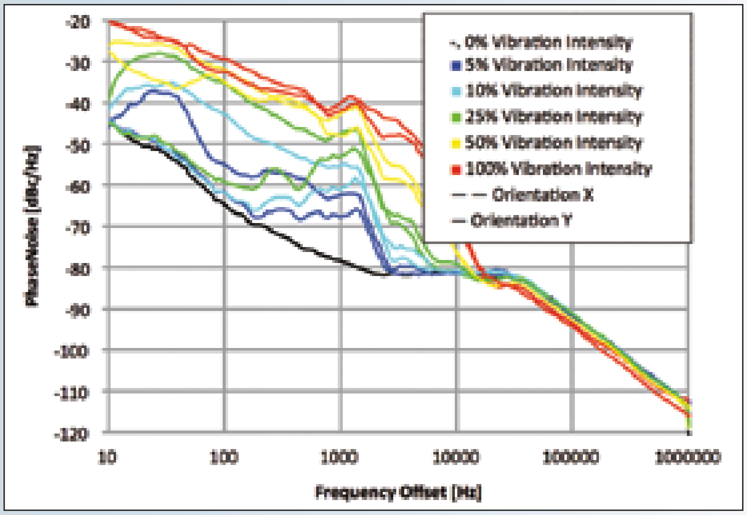


Figure 4. Phase noise of the BUC while the synthesizer is on rigid mounts. The color defines vibration intensity as specified in the legend. Dashed and solid color curves indicate vibration in x and y directions respectively. Black dash/dot curve indicates no vibration.

Comparing the dashed curves to those in *Figure 4*, observe that in x direction the improvements are negligible. Even at 5 percent vibration rate, no BER could be measured as the modem cannot maintain the receive lock. In y direction, some improvements are seen such that at 25 percent intensity, the communication link at the BER test is maintained and a steady BER of 5E-6 is observed.

Whether the situation can be improved by using a different set of vibration mounts is what we aim to answer in the following subsection.

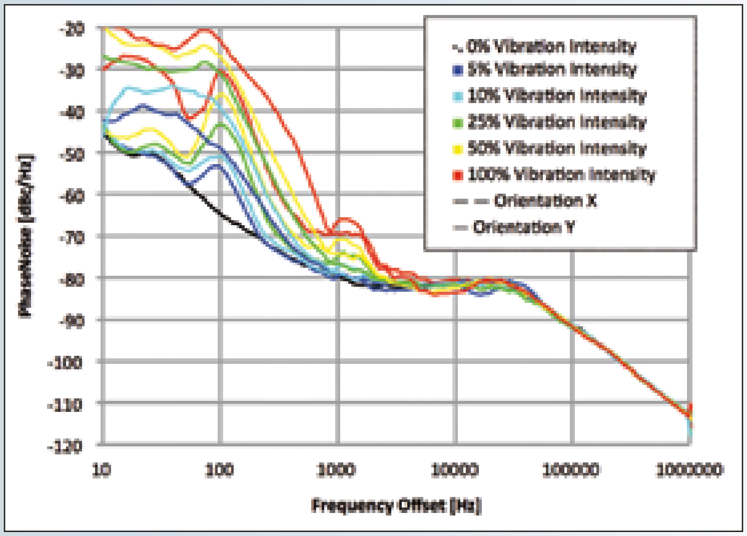


Figure 5. Phase noise of the BUC while the synthesizer is on type A mounts.

c. Synthesizer on type B Mounts

The phase noise plots of the synthesizer on type B soft mounts are presented in *Figure 6*.

Observe that there is no benefit in using type B mounts. In fact, at 25 percent vibration intensity in y direction, type A mounts provide better isolation and lead to an IPN of 87.67 mrad, compared to 127.2 mrad with type B. It is only with the type A isolators that the modem receive lock is maintained and a BER becomes achievable at this vibration intensity.

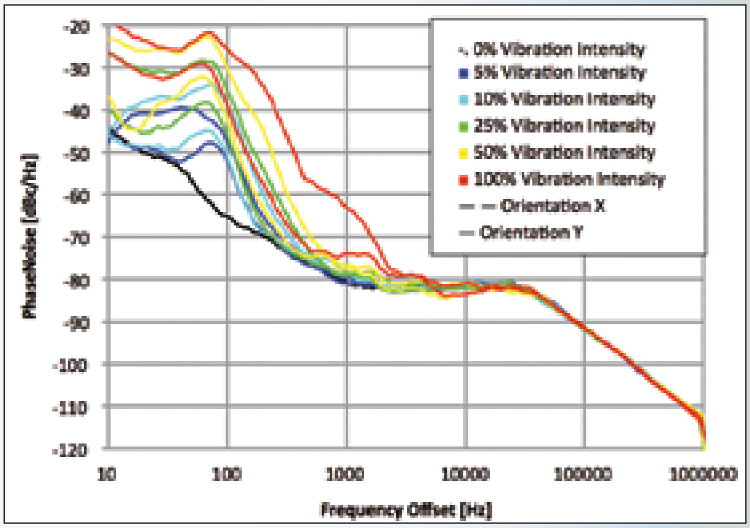


Figure 6. Phase noise of the BUC while the synthesizer is on type B mounts

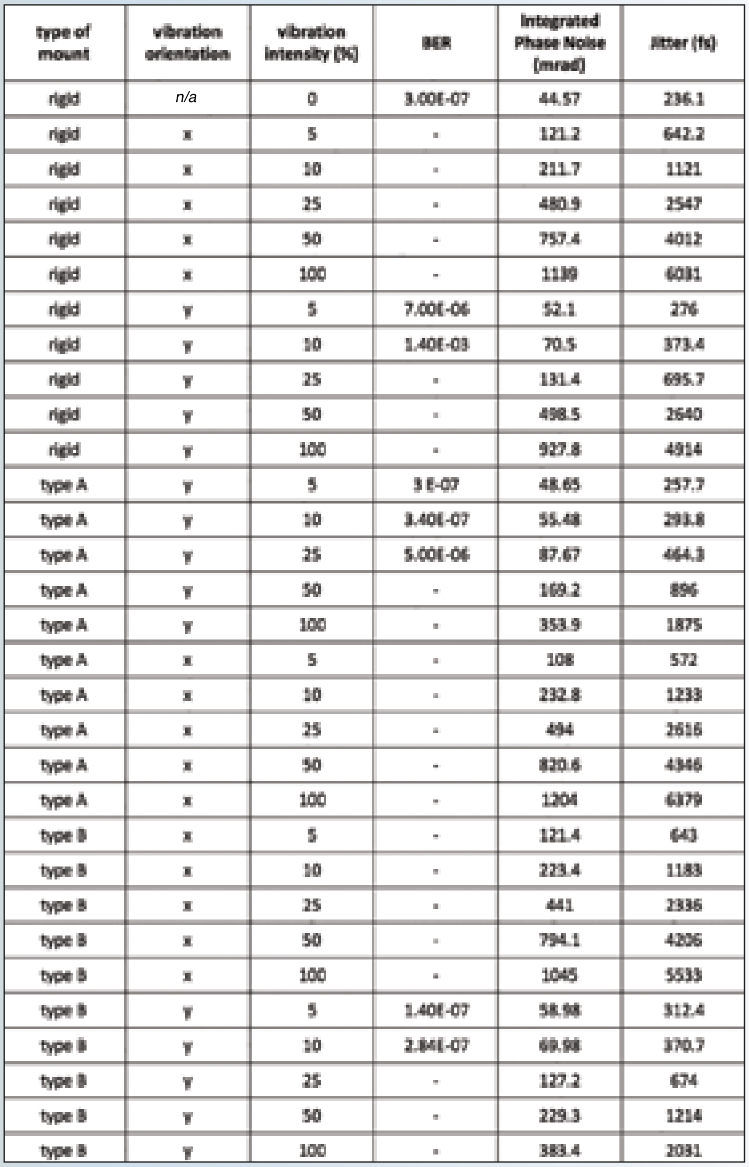
IV. Analysis

The results are discussed in this section and to summarize all the phase noise results, *Figure 7* and *Figure 8* are presented.

Figure 7 presents the phase noise of the BUC at 100 percent vibration intensity. It is seen that at both x and y directions, even with the rigid mounts the phase noise is not more than the phase noise of the case with 0 percent intensity for offset frequencies more than 20 kHz, indicating that most of the attention must be paid to the range 10 Hz to 20 kHz when choosing vibration isolators.

In *Figure 7,* it is seen that at around 70 to 80 Hz and when vibration is in x direction, the phase noise values of type A and type B cases are higher than when rigid mounts were used. The absence of this behavior in the y direction vibration indicates that the synthesizer board with the current soft mounts and their asymmetric 3-screw mounting pattern may have a natural mechanical oscillation in x direction around this frequency.

In the y direction (solid green and blue curves), at around 65 Hz, type A and B curves behave in opposite ways. While type A delivers considerable mitigation, type B does not offer any improvement. For the 150-1000 Hz range, type B mounts lead to smaller phase noise values, almost appearing to cancel out the effect at the interval around 65 Hz. Hence one would expect similar IPN and BER results for both type A and B. *Table 1* (*next page*), at 100 percent vibration intensity, confirms this prediction by showing similar IPN values 353.9 and 383.4 mrad.



type of mount	vibration orientation	vibration intensity (%)	BER	Integrated Phase Noise (mrad)	Jitter (fs)
rigid	n/a	0	3.00E-07	44.57	236.1
rigid	x	5	-	121.2	642.2
rigid	x	10	-	211.7	1121
rigid	x	25	-	480.9	2547
rigid	x	50	-	757.4	4012
rigid	x	100	-	1139	6031
rigid	y	5	7.00E-06	52.1	276
rigid	y	10	1.40E-03	70.5	373.4
rigid	y	25	-	131.4	695.7
rigid	y	50	-	498.5	2640
rigid	y	100	-	927.8	4914
type A	y	5	3 E-07	48.65	257.7
type A	y	10	3.40E-07	55.48	293.8
type A	y	25	5.00E-06	87.67	464.3
type A	y	50	-	169.2	896
type A	y	100	-	353.9	1875
type A	x	5	-	108	572
type A	x	10	-	232.8	1233
type A	x	25	-	494	2616
type A	x	50	-	820.6	4346
type A	x	100	-	1204	6379
type B	x	5	-	121.4	643
type B	x	10	-	223.4	1183
type B	x	25	-	441	2336
type B	x	50	-	794.1	4206
type B	x	100	-	1045	5533
type B	y	5	1.40E-07	58.98	312.4
type B	y	10	2.84E-07	69.98	370.7
type B	y	25	-	127.2	674
type B	y	50	-	229.3	1214
type B	y	100	-	383.4	2031

Table 1 BER, IPN and jitter values.

The frequency response of the vibration isolators may play an important role as the vibration profile is usually frequency-dependent. In *Figure 2*, it is shown that the vibration increases to its full value at 50 Hz. As mentioned previously, it is seen in *Figure 7*, that types A and B isolators behave very differently at around 65 Hz. Hence the shape of the vibration profile together with the frequency response of the vibration mounts will play a major role in determining which type of isolation should be used.

Figure 8 shows that the effectiveness of the vibration isolators of both types in reducing the IPN increases as the y-direction vibration intensity increases. For example, type A mounts reduce the IPN from 131.4 mrad with rigid mounts to 87.67 mrad at 25 percent vibration intensity whereas in the case of the 100 percent vibration intensity, type A mounts reduce IPN from 927.8 to 353.9 mrad which is a reduction by a considerable factor of about 2.6.

As a result, one would expect to see more significant improvements in the BER rates at higher vibration intensities. However, *Table 1* shows that, at higher vibration intensities, using vibration isolators does not lead to sufficient improvements in the system performance and the modem is still incapable of demodulating the signal.

At the lower intensity of 5 percent, type A mounts decrease the BER from 7E-6 to 3E-7, which is an improvement by a factor of 23. At 10 percent vibration intensity the improvement factor, compared to the rigid mounts, is more than 4000. At the 25 percent intensity, where no link was present with the rigid mounts, type A isolators enable to modem to maintain a link. Hence, although the effectiveness (with respect to IPN) of types A and B vibration isolators increase with vibration intensity, their overall advantage in assisting the modem to maintain a loopback link is negligible at higher vibration intensities.

Table 1 and *Figure 8* both show that type A isolators are more effective than type B for vibrations in the y direction.

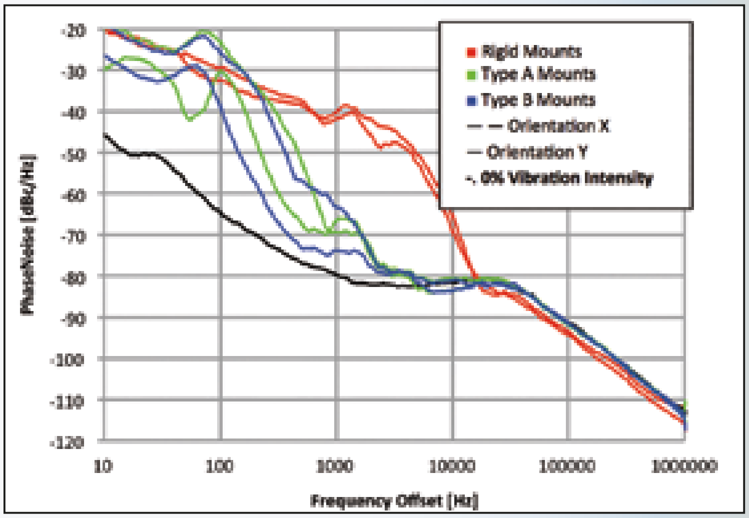


Figure 7. Phase Noise of the BUC at 100% intensity for each mount type and vibration direction.

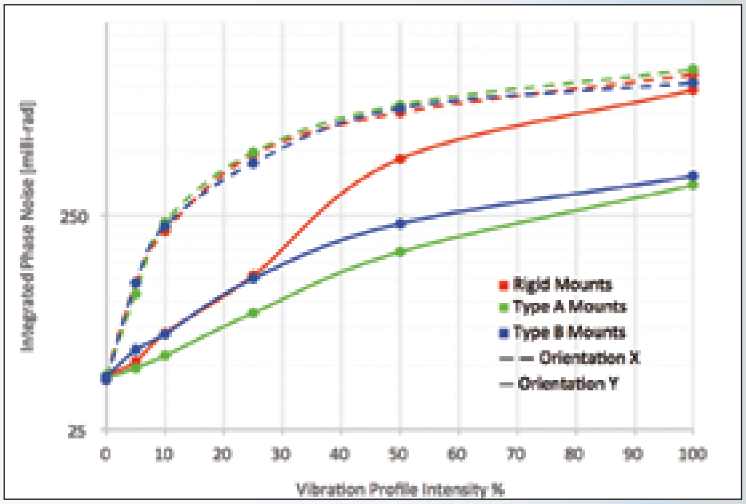


Figure 8. Integrated phase noise increases with vibration intensity. The type A mounts reduce phase noise only if the vibration is in y direction. The effectiveness of the type A mounts in y direction increases with vibration intensity.

Type A and type B mounts behave similarly when vibration is in x direction and offer almost no improvement. The BER results in *Table 1* and *Figure 8* show that the soft mounts prove useful only in y direction. The authors speculate that asymmetries in the mounting hole pattern relative to the center of mass of the synthesizer is one contribution to the difference in the effects of vibrations in difference directions.

V. Conclusion

Mechanical vibration can affect the phase noise and signal quality severely. Mounting the synthesizer board on vibration isolators can reduce the phase noise and increase signal quality. The Norsat ATOM BUC separates the synthesizer board and allows space for its internal mounting on vibration isolators.

Attention must be paid to mount the synthesizer board properly. The size and weight of the board will determine how many screws and what mounting hole pattern is required to mount the synthesizer board inside the BUC.

Vibration isolator must be chosen considering both the intensity and frequency contents of the vibrations present in the environment and the physical characteristics of the product. Considering a vibration profile similar to 160G-8SC, and the size and weight of our synthesizer board, type A isolators have shown to offer better performance over the type B counterparts.

To further reduce the sensitivity to vibration, the user can mount the BUC using external isolators if required.

www.norsat.com

References

[1] *DO, RTCA. "160G." Environmental conditions and test procedures for airborne equipment (2010).*

[2] *FORCE, AIR, and Air Force Sustainment Center-Oklahoma City. "MIL-STD-810G." (2008).*

[3] *N. Sood and P. Sen, "Optimizing performance of phase locked oscillator for high vibration environment," 2015 IEEE MTT-S International Microwave and RF Conference (IMaRC), Hyderabad, 2015, pp. 220-223.*

[4] *Norsat International Inc Internal Report, "REP000174_r1.0 Vibration Test Report for the ATOM 50W BUC"*

[5] *IEC-60068-2-64. "Environmental testing–Part 2–64: Tests-Test Fh: Vibration, broadband random and guidance." (2008).*

A GLOBECOMM ADVISORY

Empowering the U.S. Government's response to international disasters

By Paul Scardino, Senior Vice President, Sales Engineering and Marketing

The 12 months of 2017 delivered a devastating series of natural and human disasters — floods in Peru — an earthquake in Mexico City — outbreaks of violence in Nigeria — and the double-whammy of Hurricanes Irma and Maria in the Caribbean.

Insurers estimated economic losses at $306 billion from just one year. Plus, the human toll was beyond counting.

The U.S. Government (USG) responds to international disasters through the Office of U.S. Foreign Disaster Assistance (OFDA), part of USAID. OFDA responds to an average of 65 disasters in more than 50 countries every year, helping to save lives, alleviate suffering and reducing the social and economic impact of disasters worldwide.

From Zero to Sixty

OFDA's mission requires a streamlined day-to-day operational capacity. However, it also needs to respond quickly and effectively to disasters anywhere in the world. In other words, OFDA requires the ability to get from zero to sixty and back again in the least possible time. To meet that need, OFDA relies on private-sector partners for expertise, materials and technology — and the flexibility to turn on a dime when necessary.

Among those crucial partners is Globecomm, which developed an Operations Center for OFDA in Arlington, Virginia. The Ops Center provides warehousing and deployment of information and communications technology for OFDA staff and contractors and its staff is ready on a 30 minute notice to support the agency anywhere in the world. In addition to the Operations Center, Globecomm also has staff at OFDA's headquarters and backup locations in Washington DC as well as a Costa Rican facility that provides quick deployment in the Caribbean, a true hurricane hotspot.

When a disaster is declared, a Communications Officer quickly assembles a detailed plan that includes the landscape of the disaster area, its infrastructure, and available communications, power, transportation, security and housing. The plan determines the deployment of equipment and staff assignments. The Operations Center maintains enough equipment to support eight concurrent disaster response and management teams, plus ongoing individual deployments of OFDA personnel. Globecomm's field support teams are ready for deployment on a four hour notice.

Matching Service to the Need

In September of 2017, Hurricane Irma struck the Caribbean islands as a Category 5 storm, with winds of up to 280 miles

Hurricane Maria that devastated the Caribbean.

per hour, destroying thousands of homes, leveling tourist hotels and collapsing power, communications, roads and bridges. That was the costliest storm in Caribbean history — until, just two weeks later, when another Category 5 storm, Maria, blasted through the region. In response, OFDA and Globecomm teams deployed to Haiti, the Bahamas, Antigua and Barbuda, St. Maarten, Curacao, Dominica and Guadeloupe, each supported from the Operations Center and Globecomm offices.

The surge of technology into the field rapidly used up available satellite channels. Globecomm operates a global satellite, teleport and fiber network and was able to double capacity over the Caribbean within 24 hours.

Moving beyond disaster response, the company made it possible for residents to call family and friends within days of the hurricane by equipping local cellular base stations with wireless service connecting to the company's hosted 4G/LTE switching platform. A satellite link back to the company's Hauppauge, New York, headquartered teleport provided access to major telecom carriers.

Globecomm also restored FAA communications antennas damaged by the storm and provided people and equipment when no other freight forwarder could accommodate shipments. Globecomm monitors, manages and provides field service for a 43-site satellite network that carries radar and cockpit voice traffic for America's air traffic control system, under contract with Harris. Globecomm calls this offering DRaaS, *i.e.*, Disaster Recovery as a Service.

Preparation Counts

The 2017 string of disasters may have been out of the ordinary, but hurricanes and cyclones are a known risk in the Caribbean and south Pacific, just as earthquakes are in the "ring of fire" where tectonic plates intersect.

The work of OFDA makes clear that disaster preparedness is better — and ultimately less expensive — than hurried spending on disaster response. The partnership between government and the private sector ensures that this preparation does not go to waste.

As the 2018 summer months come to an end and the hurricane season arrives, the Globecomm DRaaS teams stand ready to assist on a moment's notice with equipment, personnel and expertise based on proven emergency communication solutions.

globecomm.com

Paul Scardino is the Senior Vice President, Sales Engineering and Marketing and is responsible for Globecomm's technical solutions, products, sales operations and marketing.

In his previous positions at Globecomm, he was Vice President, Corporate Sales and Marketing as well as Senior Director EMEA Region responsible for the P/L within Europe, the Middle East and Africa as well as customer specific global accounts. Mr. Scardino serves on the board as Northeast Chapter president of Space and Satellite Professionals International (SSPI), director of Long Island Software & Technology Network (LISTnet) and senior advisor of the Telecommunications Industry Association (TIA).

The Globecomm teleport in Happauge, New York.

SATELLITE INNOVATION SYMPOSIUM

THE SILICON VALLEY SATELLITE BUSINESS SHOW

October 8th - 11th, 2018

NETWORK WITH INNOVATORS

STAY AHEAD OF THE MARKET

SATINNOVATION.COM

The **2018 Satellite Innovation Symposium** aims to pinpoint key imminent market changes that will become obvious in years to come. While infrastructure and capital status have dominated for decades, key innovations will continue to cause major disruptions to the established marketplace. ***What innovations will define the satellite communications industry going forward?***

The full itinerary of sessions, breakfast, lunch, refreshments and a cocktail reception are included with admission to the event. Optional workshops and a wine tasting tour with invited speakers and other satellite professionals are also available the day prior to the event.

JOIN A DYNAMIC GROUP OF EXECUTIVES FROM ORGANIZATIONS ADDRESSING EXCITING INNOVATIONS AND THE MARKET FORCES THAT WILL FRAME THEIR DEVELOPMENT