32nd Space Symposium, Technical Track, Colorado Springs, Colorado, United States of America
Presented on April 11-12, 2016

THE GROWING CONVERGENCE OF DoD AND COMMERCIAL PROTECTED SATCOM REQUIREMENTS

Steve Williams
RT Logic, swilliams@rtlogic.com

Chris Badgett
RT Logic, cbadgett@rtlogic.com

ABSTRACT – THREE KEY AREAS OF CONVERGENCE

Reliance on SATCOM[*] has never been higher in both the DoD and Commercial sectors.

From a commercial perspective, SATCOM is used for critical national infrastructure services such as communications, financial and banking services, power grid operation, security, healthcare, transportation, disaster relief, and vital distribution systems for food, water, medicine, fuel and vital products.

From a DoD perspective, SATCOM is indispensable to command, control, reconnaissance, relief and warfare communications. As SPAWAR PMW/A 170 asserts, "Bandwidth is THE Key enabler of Information Dominance.[1]" For the US Navy in particular, SATCOM is the mainstay of long distance communications in peacetime, humanitarian operations and when on wartime footings.

SATCOM demand is ever increasing in response to unprecedented international data requirements from the human, military and financial sectors. This extraordinary demand is driving a convergence of commercial and DoD SATCOM requirements. This paper specifically addresses three key areas of converging requirements: Increasing Bandwidth Availability, Improved SATCOM Planning and Reliable Protected Communications.

Increasing Bandwidth Availability

The US Navy is experiencing steep SATCOM bandwidth growth, as shown in Exhibit 1. Even as new satellites come on-line, their bandwidth is immediately consumed, with requirements continuing to outrun bandwidth availability. Among many results, this leads to increasing utilization of commercial satellites to carry encrypted Navy communications within Commercial Broadband Satellite Program (CBSP) capabilities, as can be seen in Exhibit 1 as well.

Commercially, SATCOM bandwidth utilization doubles every 2 – 3 years[2]. In commercial space, this growth generates revenues that can, in part, accrue to new satellite development and launch. Even so, staying ahead of the SATCOM bandwidth demand curve is a daunting task.

In addition to deploying more satellites to meet growing bandwidth needs, the SATCOM market is also vigorously pursuing increased bandwidth utilization efficiencies as well as capabilities which support dynamic reallocation of available bandwidth. The rapid evolution and deployment of High Throughput Satellites (HTS) will

[*] All abbreviations are defined in the "Abbreviations" section of this paper.

supply additional available bandwidth[†], and requires budget availability to conduct needed R&D, construction, launch and upkeep operations. As well, advanced modem technologies leveraging concepts from Adaptive Coding and Modulation (ACM) techniques, wide band frequency hopping and direct sequence spread spectrum will be important.

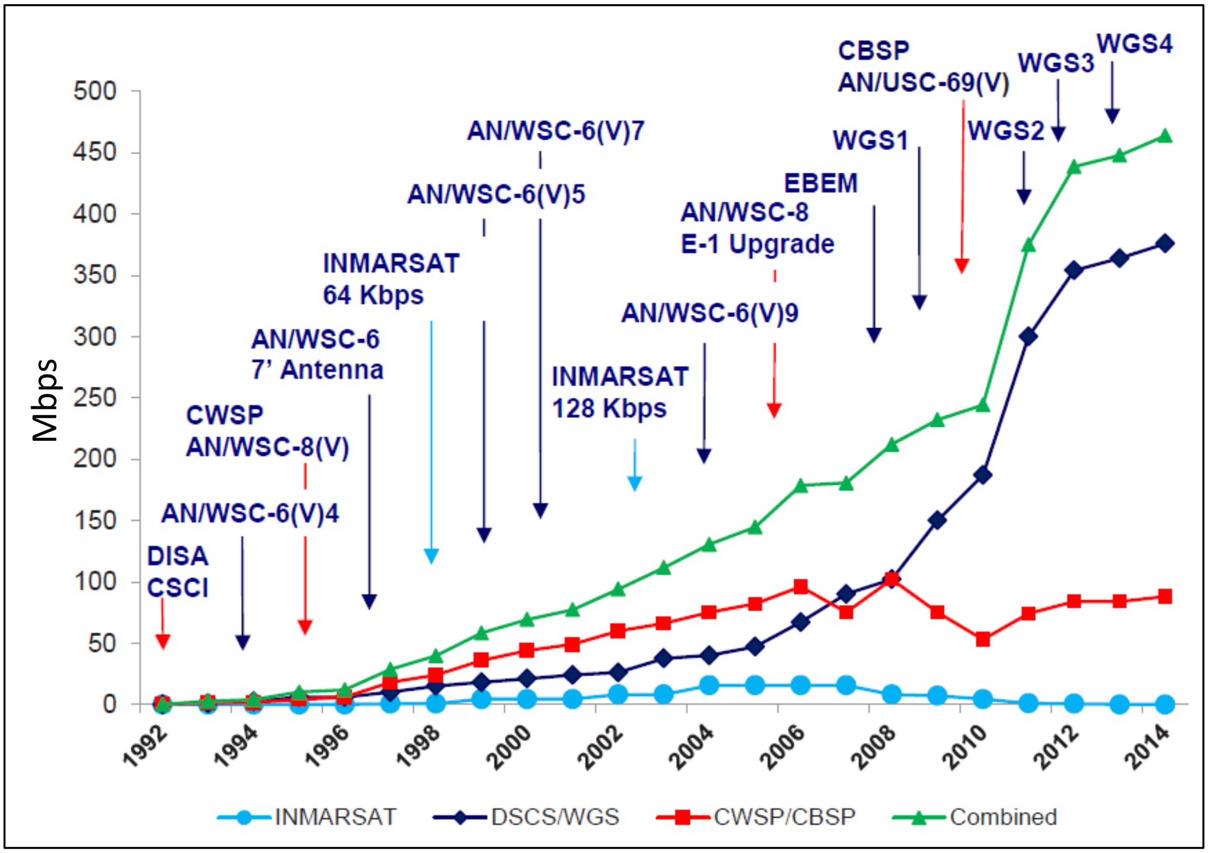


Exhibit 1: Worldwide Full-Duplex Navy Wideband SATCOM Throughput[3]. DSCS/WGS are DoD satellites, while CWSP/CBSP represents Commercial satellite use. Satellite names/types are shown above the plots.

Improved SATCOM Planning

As bandwidth becomes more available, the planning process for satellite, transponder and frequency procurement, authorizations and assignments must also keep pace with military and business needs. However, SATCOM planning isn't consistent or shared across the commercial and DoD space, can employ antiquated manual techniques and tools, involves numerous people in the control loop, and is often error-prone.

In peacetime, current planning processes for requesting SATCOM access can be time-consuming, non-agile and frustrating. As well, the process of reporting interference events or other outages into SATCOM planning operations is often manual, incomplete and overly burdensome for both the SATCOM user and the planner.

[†] HTS technologies also substantially improve interference rejection capabilities, since would-be interferers must be very close to the SATCOM users. This contrasts with wide coverage beams, which are more vulnerable to interference from remote sources.

Automated SATCOM planning and re-planning systems operating at electronic speeds, quickly adapting to dynamic bandwidth availability, smartly avoiding interference, and automatically adjusting equipment and settings at both ends of the SATCOM link must be developed and deployed. These systems will greatly facilitate operations in degraded environments, will provide badly needed fail-over capabilities, and may themselves deter many forms of intentional interference.

Reliable Protected Communications

"Protected Communications" is a general phrase representing actions taken beyond the normal SATCOM transmission to reliably transmit and receive signals. Protected SATCOM extends well beyond typical approaches related to increasing the overall link budget (e.g. larger apertures, more power, changing modulation types, etc.).

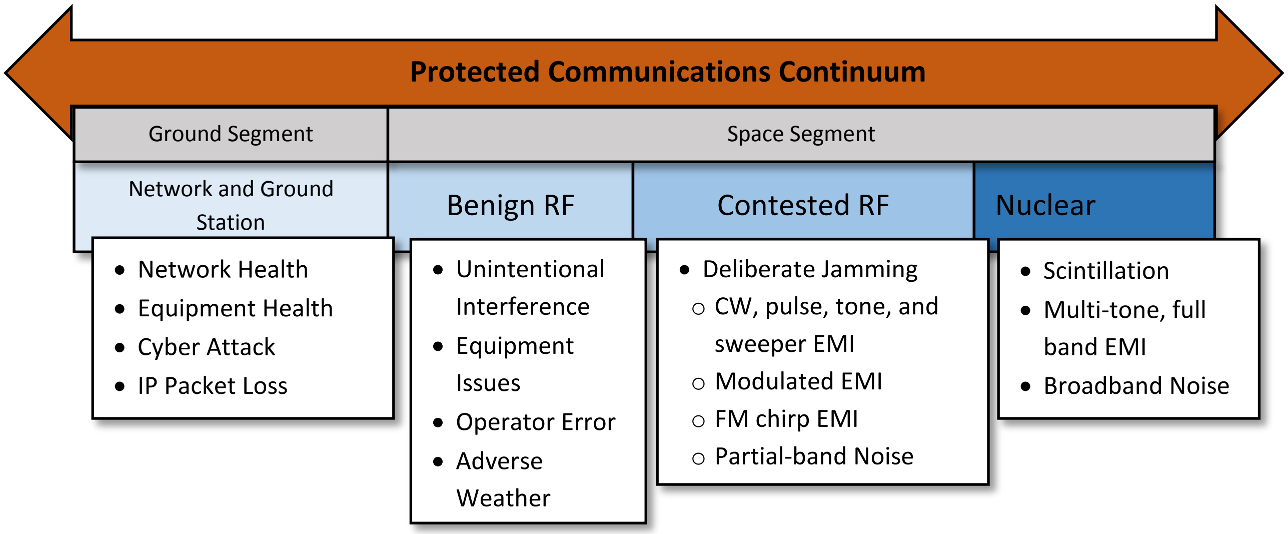
For the DoD, Protected MILSATCOM is often implemented by an EHF service with small-footprint SATCOM beams for strategic and tactical purposes.

- Strategically, Protected MILSATCOM must provide low probability of interception, detection and exploitation (LPI, LPD and LPE) and be survivable, to include anti-scintillation and anti-jam communications. Strategic Protected MILSATCOM must also provide robust command and control services in benign, contested and nuclear operational environments, as shown in Exhibit 2.

- Tactically, Protected MILSATCOM must provide anti-jam and LPI/LPD/LPE communications in both benign and contested environments.

For the commercial segments, Protected Communications attempts to minimize the effects of interference in benign environments, though recent events also suggest the need for anti-jam capabilities.

In all cases, the Terrestrial Network and Ground Station must be resilient to growing Cyber Attack threats, and must monitor and automatically compensate for overall network and equipment health issues, as well as data communications losses.



Protected Communications Continuum

Ground Segment

Network and Ground Station

- Network Health
- Equipment Health
- Cyber Attack
- IP Packet Loss

Space Segment

Benign RF

- Unintentional Interference
- Equipment Issues
- Operator Error
- Adverse Weather

Contested RF

- Deliberate Jamming
  - CW, pulse, tone, and sweeper EMI
  - Modulated EMI
  - FM chirp EMI
  - Partial-band Noise

Nuclear

- Scintillation
- Multi-tone, full band EMI
- Broadband Noise

Exhibit 2: A Protected Communications Continuum.

Generally, advanced systems, products and capabilities along the Protected Communications Continuum fall within a Protection Progression evolution as shown in Exhibit 3.

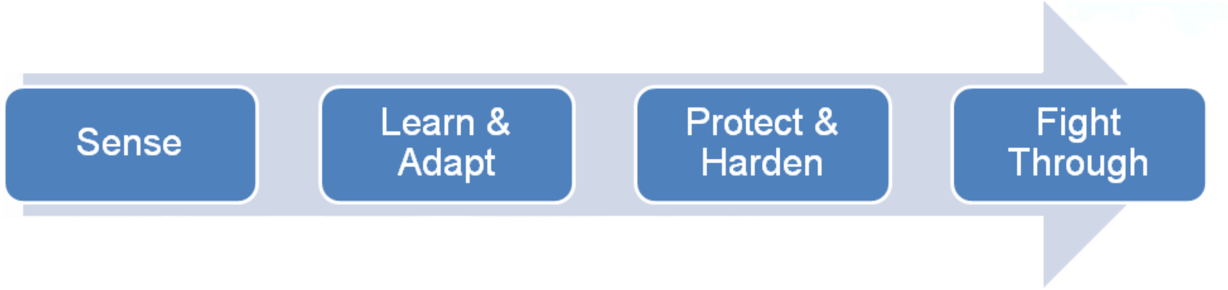


Exhibit 3: Protection Progression for products, capabilities and advanced systems.

From a threat **Sense** perspective, users and systems must quickly know when something is wrong and when communications are being degraded or interrupted. For example, for RF signals, automatic signal monitoring is a desired approach. For networks, network health monitoring, cyber-attack sensors and virus detection are good approaches.

Learn and Adapt tools provide insightful data trending and analysis that feeds understanding and automatic adaptation to the threat and risk occurring in the environment over time. Effective data logging and monitoring should store historical, time-tagged measurement data to support trending and analysis. Such a repository is useful for predicting equipment failures, communications outages, and impending electronic attack preceded by detectable signal trends and other indications. Historical data can also be exploited to differentiate equipment problems from operator error, and between accidental or intentional interference.

Protect and Harden is the next line of protection, and includes solutions that protect against threats. Signal Geolocation capabilities fall within this classification, as do devices that protect against cyber-attack or network transmission issues.

Fight Through capabilities utilize advanced signal processing, for example, to add robustness at the waveform level to enhance LPI/LPD/LPE. Wide band Frequency Hopping and Direct Sequence Spread Spectrum (DSSS) are typical methods to permit operation with active interference and jamming. Also from a fight-through perspective, the Protected Tactical Waveform (PTW) is a new approach using Frequency Hopping Spread Spectrum (FHSS) to provide enhanced anti-jam attributes. PTW combines features of the current MILSATCOM protected waveform and the commercial waveforms such as Digital Video Broadcasting (DVB.) This hybrid strategy strives to balance protection and affordability.

MISSION PROTECTION

Numerous systems, capabilities and technologies exist or are in active research and development toward the end goal of protected SATCOM. Many are already in dual DoD/Commercial use, or are rapidly converging for use within both domains. Many align with best practices for end-to-end protected SATCOM:

- SATCOM equipment must include Designed-in Protection capabilities for spectral monitoring, interference detection and interference cancellation.

- Ground System Protection much cover components and networks and must be impervious to network disruptions and intrusions, hacking, viruses and data exfiltration threats.

- Continuous, automatic Signal Monitoring at each SATCOM receive and transmit terminal must be implemented.

- Fast and automated response mechanisms to restore communications, including sophisticated Signal Geolocation Systems, dynamic bandwidth reallocation and rapidly steerable spot beams must be available.

- Ongoing on-site Training to enhance the interference recognition and response skills of operators is needed at both ends of a SATCOM link. This should include SATCOM, Signals and EMI training, as well as hands-on opportunities to operate equipment impacted by interference (e.g. modems, cryptos, routing devices, impacts on other users, etc.).

- Thorough and automatic link protection and SATCOM system Self-Testing at each SATCOM terminal to assure nominal operation of the terminal and link protection gear, and to provide early warning on pending system failures.

Designed-in Protection

RF link protection begins long before a satellite is launched or a ground station is designed. Channel Simulators, Transponder Simulators and Satellite Signal Emulators are extremely valuable during the research, development and test phases for modems, receivers, transmitters and waveforms. These advanced instruments can generate nominal and worst-case SATCOM test signals within a controlled lab environment. Engineers can then design and tune their firmware, software and hardware for unimpeded communications even under degraded signal conditions.

In the laboratory, Channel Simulators and Transponder Simulators create physics-compliant signals indistinguishable from their real world counterparts. These signals include propagation effects modeling, motion-related Doppler shift, atmospheric and multipath fading, path delay, and atmospheric noise profiles. Furthermore, these systems can simulate spacecraft equipment effects, duplicating amplitude and phase response and introducing linear and non-linear signal distortions.

These simulators, coupled with SATCOM Signal Generators, add further realism by supplying anything from perfect signals, to those impacted by multiple instances of advanced static and dynamic interference, both accidental and intentional. These instruments also generate signals perturbed by unexpected flight paths, attitude or antenna pattern issues.

High fidelity Satellite Signal Emulators accurately represent complex uplink and downlink signals, and are valuable tools for system developers, testers and trainers. These devices fully emulate complex wideband communications systems found on the emerging generation of channelized, multi-beamed HTS satellites, such as the WGS constellation.

These instruments give SATCOM hardware, firmware and software designers a huge advantage during the design and test process, enabling them to develop and test equipment that will be tolerant of natural signal degradation and resilient to a broad variety of attacks on the signal. Additionally, they support innovative development of interference cancellation capabilities, interference resilient waveforms, and automatic signal parameter negotiation (such as modulation types, power levels and data rates) between transmit and receive devices at each end of the SATCOM link.

Ground System Protection

IP traffic between ground system components and sites must be fast and reliable. However, wide area IP networks exhibit traits that can degrade performance: dropped packets, indeterminate latency, variable jitter, and packet duplication and reordering. For most users, Transmission Control Protocol / Internet Protocol (TCP/IP) masks these problems and delivers data acceptably. But many mission critical applications cannot tolerate TCP/IP's retransmit and acknowledge behavior when attempting to deliver consistent data at required rates.

To repair dropped packets, the Packet Forward Error Correction (PFEC) and Intelligent Retransmission Protocol (IRP) protocols should be utilized. PFEC helps improve network data delivery reliability without return transmission acknowledgements. IRP improves network throughput within bandwidth constraints and adds needed data reliability. Both protocols allow high throughput with low latency across lossy, long-haul links and give the user the flexibility to choose the best solution for each situation. Ground systems must provide extensive network performance analysis and diagnostics in addition to robust traffic protection.

In addition to packet loss, re-ordering and duplication can also impair WAN transport. Employed solutions should provide a constant latency re-ordering window that corrects out of order and duplicated packets without introducing unwanted latency. WANs also impose latency jitter, which can result in extremely bursty output that overwhelms end-device receive buffers. Here, deterministic end-to-end latency control is needed to eliminates the effect of latency jitter and allows the system designer to treat the WAN as a long wire with constant, known latency.

Additional capabilities for real-time network health monitoring and report are an important aspect of any ground station protection mechanism. As well, cyber-attack detection and real-time reporting via a National Information Assurance Partnership (NIAP)-certified Security Information and Event Management (SIEM) is highly desirable.

Cost-effective antenna site diversity capabilities for weather conditions (e.g. rain fade), and disaster recovery are also needed. These capabilities should precisely align signals received and packetized at two different locations within just several nanoseconds. This enables seamless switching between antennas, at any separation distance, without losing modem lock. Digital IF architectures enable site diversity and resiliency by digitizing spectrum from geographically separated antennas. The digitized spectrum is then transported via IP networks to modems at a centralized hub or processing center.

Signal Monitoring

With well-designed and tested SATCOM systems enhanced for link protection, the first operational line of defense is continuous and advanced monitoring of the received and transmitted signals to assure they match expectations.

Automatic signal monitoring must go beyond simple spectrum analyzer mask analysis of bandwidth, center frequency and power level. In-depth and real-time signal analysis must also include blind determination of modulation type, data rate, coding scheme, MER, EVM and BER.

Monitoring tools that support such analysis should mathematically decompose the signal of interest, searching for unauthorized signals within the protected bandwidth that could degrade QOS as shown in Exhibit 4.

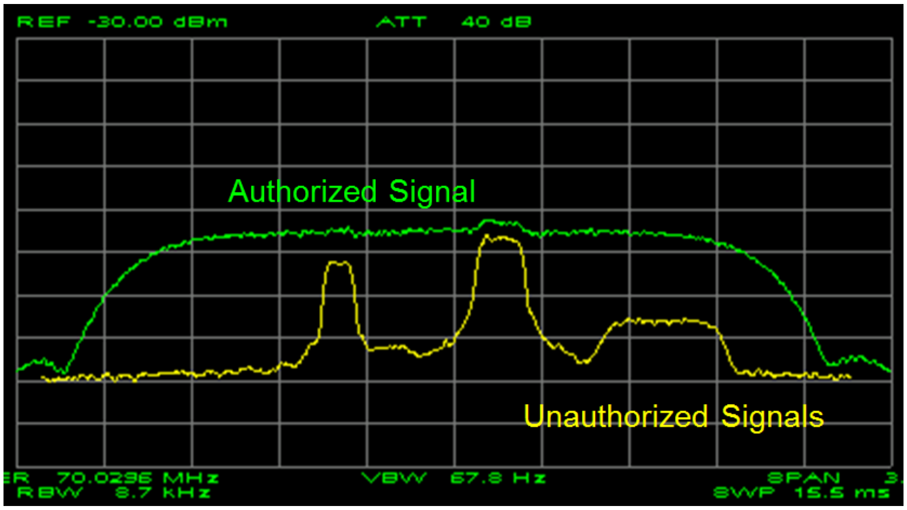


Exhibit 4: Advanced Spectrum Analysis with covert and overt interference detection and characterization capabilities.

Once these real-time measurements are complete, the monitoring system should match the results against expected values for each signal. Modulation type, data rate, center frequency, and power level differences between measured and expected values must be tolerable to the SATCOM system within the boundaries of the Satellite Access Authorization (SAA.)

All SATCOM modulation types should be supported by the monitoring system over high and low amplitude ranges, and narrow and wide bandwidths. This includes TDMA, spread spectrum, and others, as well as the usual array of phase-shift keying (e.g. BPSK, QPSK, 8PSK, APSK, etc.) and quadrature amplitude modulation (e.g. 16QAM, 32QAM, etc.) signals.

Ideally, the monitoring system should be field-adaptable to detect and characterize new modulation types, emerging interference types and evolving intentional interference techniques.

In the case of RF signals, when received or transmitted signals do not match parametric expectations, or are determined to be impacted by interference, automatic alerts and data logging must take place. This assures that already time-crunched operators are not relegated to constant vigil or control over the monitoring system.

This type of signal monitoring and logging can occur on a single SATCOM link, for an entire SATCOM gateway, across an enterprise or even a battle group. Consolidating information at the enterprise level allows users and operators a Common Operating Picture (COP) of the threat environment. A COP aids in enhanced decision-making, since users encounter all data in a single place.

An effective COP should be fully user-configurable and based on various Information Assurance requirements and bandwidth restrictions, can be a zero-client, browser-based implementation.˙ Data should be exportable in industry standard formats such as EXtensible Markup Language (XML) and Keyhole Markup Language (KML) for integration into other systems and COPs.

Libraries of known emitters, known signal types and prior SATCOM authorizations should be employed in order to facilitate the critical task of EMI attribution.

RF monitoring and data collection assets can measure and compare power and bandwidth utilization against authorized and/or planned levels. Such systems can identify unauthorized users and unused bandwidth segments, and can feed automated SATCOM planning tools, as shown in Exhibit 5. This type of data analysis can also point to under or overused transponders and support BW reallocation exercises.

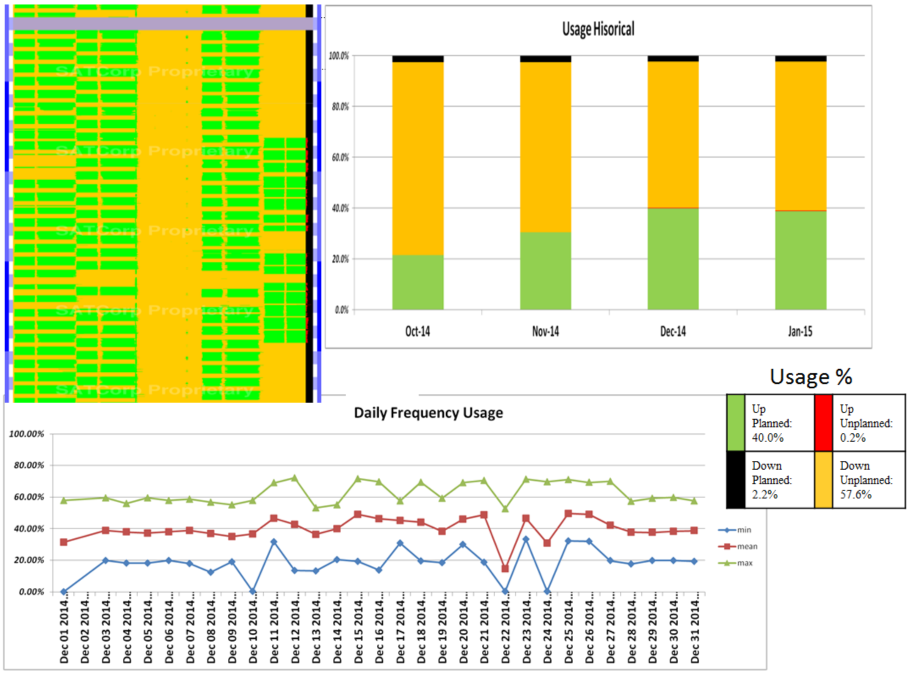
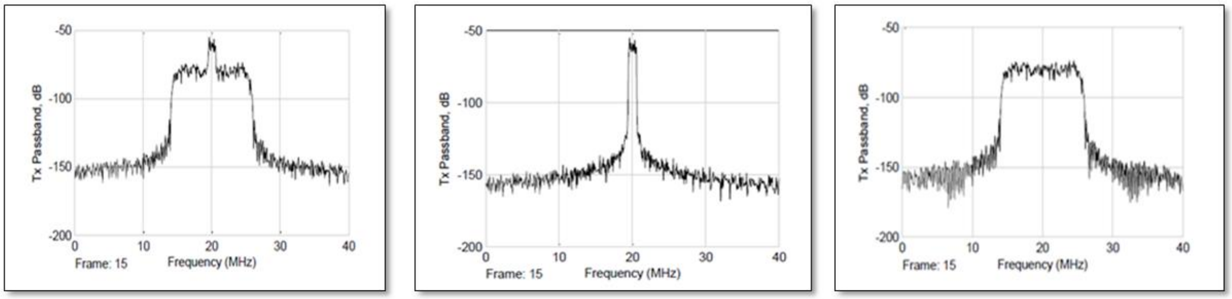


Exhibit 5: Satellite Bandwidth Utilization monitoring can help to identify unauthorized users, planning inefficiencies, and user/frequency assignment opportunities.

Interference cancellation capabilities can maintain communications even in some degraded RF environments, as shown in Exhibit 6. Interference cancellation techniques include dynamic and adaptive Digital Signal Processing (DSP) to fully isolate and reduce/remove the interferer.



Interference-impacted Signal

Isolated Interference

Reduction sufficient to increase MER for successful demodulation

Exhibit 6: Interference Cancellation systems provide SATCOM restoral opportunities.

Signal Geolocation

Signal Geolocation systems pinpoint Earth locations of disrupting signals. Once a physical location estimate of an offending transmitter is available, an assessment of friendly (accidental) or hostile (intentional) interference can proceed. Assisting in this determination, geolocation data can be combined with other location-specific intelligence.

The fastest and most accurate geolocation systems today receive SATCOM signals via two Earth-Satellite-Earth paths. High-accuracy geolocation systems typically look at four signals during a geolocation—the interfering signal and a reference signal from a known location both passing through a primary satellite and a nearby secondary satellite in a side lobe, as shown in Exhibit 7.

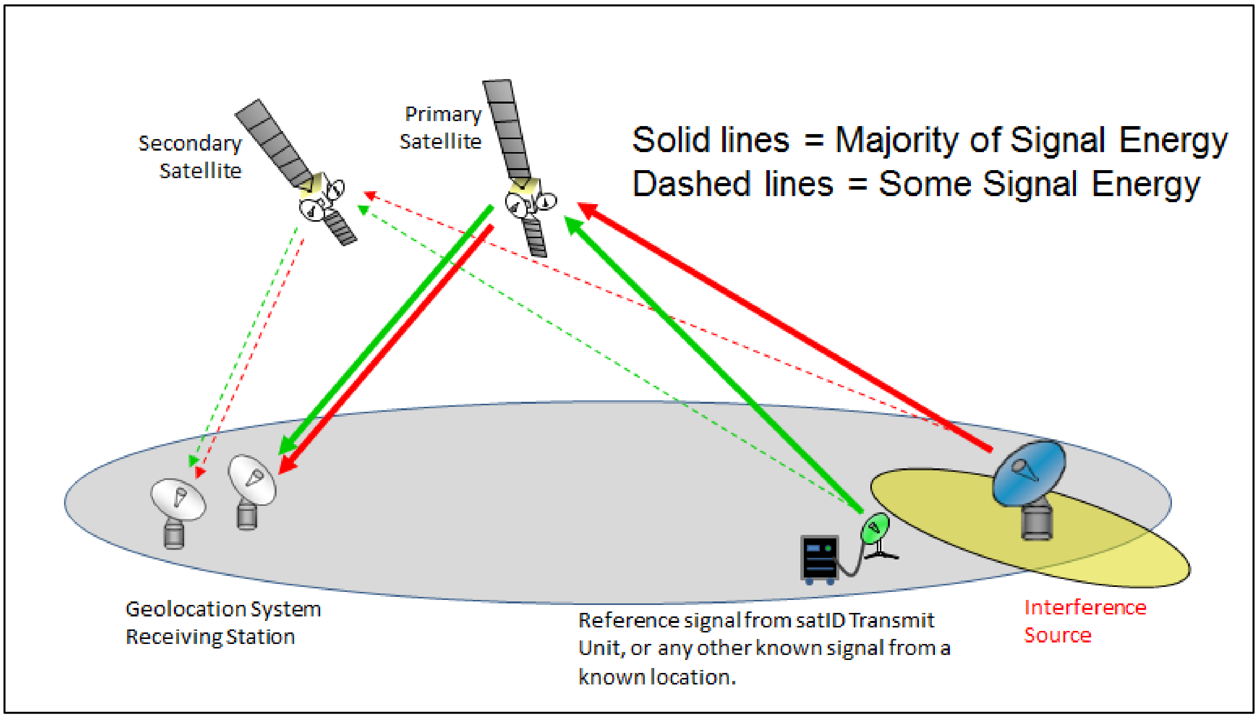

Secondary Satellite
Primary Satellite
Solid lines = Majority of Signal Energy
Dashed lines = Some Signal Energy
Geolocation System Receiving Station
Reference signal from satID Transmit Unit, or any other known signal from a known location.
Interference Source

Exhibit 7: Geolocation systems utilize the known location of a reference signal to determine the Earth location of an interference signal.

Training

Until SATCOM networks become fully self-healing, human operators and analysts will remain those who interact with ground equipment and link protection systems, interpreting their results and taking corrective restoral actions based on their indications. Operator familiarity with these systems and the threats to them dictates how quickly and correctly they can identify and resolve problems.

For example, effective geolocation system operators have achieved a deep understanding of scenario aspects that relate to geolocation accuracy. Satellite orbit characteristics, the distance between primary and secondary satellites and reference emitter locations are key, although a host of other factors contribute as well.

These devices can combine Channel Simulators and Signal Generators to create input signals, with and without EMI, that precisely represent those received by geolocation systems under any scenario imaginable. They connect to, or are integrated with Geolocation Systems, so training can be conducted 24/7 without need to attend distant and expensive schoolhouse events.

Similarly, Channel Simulators, Transponder Simulators, Signal Generators and Satellite Signal Emulators can be switched into ground station signal inputs instead of normal antenna/amplifier inputs. This allows the ingest of many nominal and worst case signals, with or without interference, and results in the ground station performing exactly as it would under real world degraded signal conditions, but without consuming vital satellite bandwidth or using live interferers.

Network Simulators can inject many different types of network impairments, active threats, slow-downs and lost packets, providing operators with hands-on experience as to the impacts of these degradations on the systems they use and maintain.

As shown in Exhibit 8, SATCOM, Signals and EMI training can be conducted via software-only packages for classroom instruction, self-study "what if" experimentation, and/or war-gaming involving multiple, linked students and instructors.

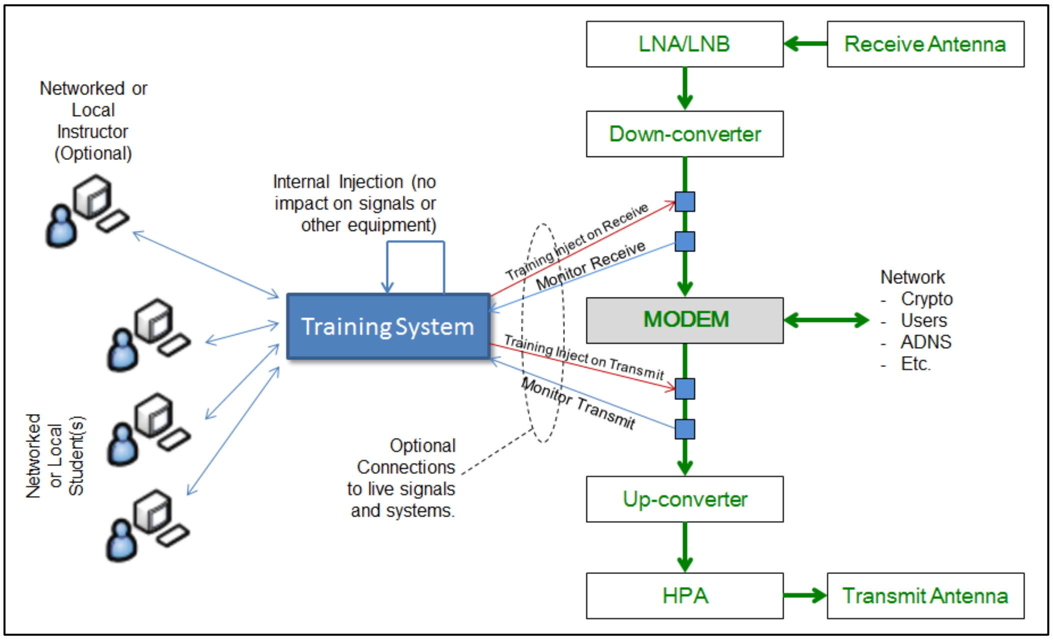

LNA/LNB
Receive Antenna
Networked or Local Instructor (Optional)
Down-converter
Internal Injection (no impact on signals or other equipment)
Training Inject on Receive
Monitor Receive
Network
- Crypto
- Users
- ADNS
- Etc.
Training System
MODEM
Training Inject on Transmit
Monitor Transmit
Networked or Local Student(s)
Optional Connections to live signals and systems.
Up-converter
HPA
Transmit Antenna

Exhibit 8: Effective training systems can be used stand-alone, or can be connected to actual SATCOM equipment for realistic downstream equipment and systems training.

Realistic training systems allow operator control of key waveform and EMI parameters for full realism, and show anticipated equipment behavior as a result of the training scenario. Effective training systems should display "received" SATCOM waveforms, "received" interference waveforms, and the combination of the two. Additional learning can be accomplished with trainers that include constellation diagrams, modem measurement results, and that convey impacts on data streams being impacted by the selected EMI.

By enabling deep, repeatable and continuous training strategies, operators can study SATCOM, signals, EMI and network issues, to understand exactly how their equipment will perform under challenging signal and network conditions, giving them valuable experience to hasten recognition of issues, differentiate causes, and restore operations.

Self-Test

Just as pilots run automated self-tests and manual checklists before and during flight, SATCOM professionals should periodically do the same to ensure the proper functioning of their link protection systems, ground systems, networks, etc.

At the command of human operators, and under computer control, Channel Simulators, Transponder Simulators, Signal Generators and SATCOM Signal Emulators can be switched into receiving system inputs where amplified antenna signals normally appear. These simulators can rapidly step through a series of pre-determined normal and degraded signals, adding interference if desired, and presenting these signals to link protection system inputs instead of the usually received SATCOM signals.

As these signals are presented, self-test software can check that each injected anomaly was properly detected and identified by the link protection capabilities. This assures proper functionality of link protection systems and algorithms, and can be an important differentiation step in isolating equipment faults, operator error, or actual link disruption.

Similarly, Geolocation Signal Simulators can be switched into geolocation system inputs in place of their usual antenna feeds. These simulators can then cycle through various combinations of satellites, ground stations, antenna patterns and other conditions to ensure anticipated geolocation results.

Network simulators, impairment generators and threat injectors can be utilized as well, testing against the system's ability to detect, fight-through and eradicate related issues.

INTEGRATED SOLUTIONS

An integrated solution combines primary equipment functions (e.g. a modem), with Mission Protection capabilities (e.g. spectral awareness, test/training, EMI cancellation, etc.) as depicted in Exhibit 9.

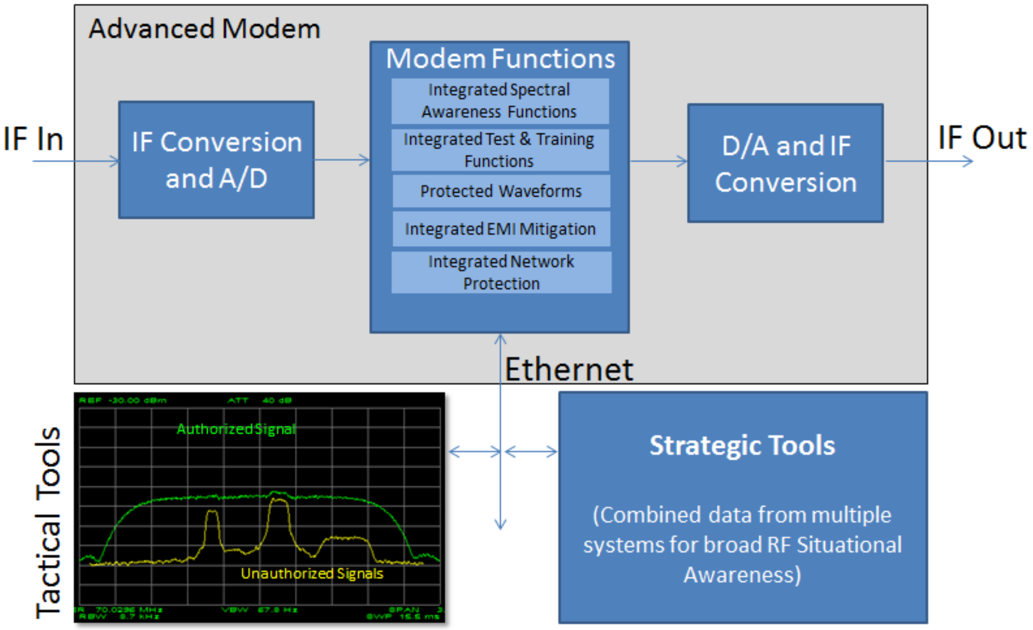


Exhibit 9: An advanced, spectrally aware modem integrates several Mission Protection functions.

With a spectrally aware modem, cognitive radio[4] capabilities can be furthered pursued. CR has applications in Ka-band HTS, and in numerous other areas. Cognitive approaches offer fresh ideas to increase spectrum utilization and efficiency. Ongoing research looks at CR applications to service future high density fixed satellite services while minimizing interference to existing users.

CONCLUSION[5]

Protected SATCOM covers a wide area of need, with a broad set of existing and evolving solutions that leverage capabilities from and to DoD and Commercial applications. SATCOM is a vital infrastructure element in commercial, as well as military C2 and data transport applications. Due to their mission-critical nature, the function and performance of these links must be protected with great attention, constancy and attention to detail.

From a design and test viewpoint, SATCOM equipment designers are applying innovative new ideas to architecting systems that are simultaneously aware of and tolerant of interference. As they evolve and innovate, they must have relevant, application-focused, precision instrumentation to support their crucial RDT&E work.

Efficient planning, allocation and use of bandwidth, both for conventional and HTS satellites, must be energetically pursued. SATCOM equipment should be connected directly into these processes and systems for fastest dynamic response. SATCOM Protection must extend from the SATCOM equipment itself, deeply into the supporting networks and ground systems.

In deployment, SATCOM operators must access an ever-evolving arsenal of effective interference detection, location and mitigation tools. Equally important, their interpretation skills and SATCOM understanding must be broad, deep and constantly refreshed through timely, realistic and site-specific training. Nothing less than full vigilance toward SATCOM Protection will keep our military and commercial SATCOM at peak performance.

ABBREVIATIONS

The following abbreviations appear within this paper.

16QAM	16-State Quadrature Amplitude Modulation
32QAM	32-State Quadrature Amplitude Modulation
8PSK	Eight Phase Shift Keying
ACM	Adaptive Coding and Modulation
APSK	Amplitude Phase Shift Keying
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
C2	Command and Control
C4I	Command, Control, Communications, Computers and Intelligence
CBSP	Commercial Broadband Satellite Program
COMSATCOM	Commercial SATCOM
COP	Common Operating Picture
CR	Cognitive Radio
CW	Continuous Wave
CWSP	Commercial Wideband Satellite program

DoD	Department of Defense
DSCS	Defense Satellite Communications System
DSP	Digital Signal Processing
DSSS	Direct Sequence Spread Spectrum
DVB	Digital Video Broadcasting
EHF	Extremely High Frequency
EMI	Electromagnetic Interference
EVM	Error Vector Magnitude
FHSS	Frequency Hopping Spread Spectrum
FM	Frequency Modulation
HTS	High Throughput Satellite
IA	Information Assurance
IP	Internet Protocol
IRP	Intelligent Retransmission Protocol
KML	Keyhole Markup Language
LPD	Low Probability of Detection
LPE	Low Probability of Exploitation
LPI	Low Probability of Intercept
MER	Modulation Error Rate
MILSATCOM	Military SATCOM
NDIA	National Defense Industrial Association
NIAP	National Information Assurance Partnership
PEO	Program Executive Office
PFEC	Packet Forward Error Correction
PTW	Protected Tactical Waveform
QOS	Quality of Service
QPSK	Quadrature Phase Shift Keying
R&D	Research and Development
RDT&E	Research, Development, Test and Evaluation
RF	Radio Frequency
SAA	Satellite Access Authorization
SATCOM	Satellite Communications
SIEM	Security Information and Event Management
SPAWAR	Space and Naval Warfare Systems Command
TCP/IP	Transmission Control Protocol / Internet Protocol
TDMA	Time Domain Multiple Access
USN	United States Navy
WAN	Wide Area Network
WGS	Wideband Global SATCOM
XML	EXtensible Markup Language

[1] Glover (USN), CAPT Mark. "Program Executive Office Command, Control, Communications, Computers and Intelligence (PEO C4I), Communications and GPS Navigation Program Office (PMW/A 170), NDIA San Diego Fall Industry Event" page 9. Navy.mil. US Navy, 28 October, 2015. Web. 28 March, 2016.

[2] Minoli, Daniel. “Innovations in Satellite Communication and Satellite Technology” page 97. John Wiley Publishers. February, 2015.

[3] Glover (USN), CAPT Mark. "Program Executive Office Command, Control, Communications, Computers and Intelligence (PEO C4I), Communications and GPS Navigation Program Office (PMW/A 170), NDIA San Diego Fall Industry Event” page 9. Navy.mil. US Navy, 28 October, 2015. Web. 28 March, 2016.

[4] Maleki, S. “Cognitive Spectrum Utilization in Ka-Band Multibeam Satellite Communications.” Institute of Electrical and Electronics Engineers (IEEE). IEEE Communications Magazine, volume 53, issue 3. March 2015.

[5] Portions of this paper were adapted with permission from;

- Williams, Steve and Badgett, Chris. “The Convergence Of DoD + Commercial Protected Comms Applications.” MilSatMagazine.com. MilSatMagazine, June, 2015. Web. 28 March, 2016.
- Williams, Steve. “Strategies For Comprehensive Link Protection.” MilSatMagazine.com. MilSatMagazine. April, 2013. Web. 28 March, 2016.