Strategies For Comprehensive Link Protection

By Steve Williams, Business Area Manager of Signals Instrumentation, RT Logic

Reliance on satellite communications (SATCOM) for critical communication links has never been higher, making the growing problem of link protection even more critical. Commercial satellite operators estimate that millions of dollars are lost in interference related events each year. Interference is a frequent problem in military operations, not just from unfriendly sources, but from inadvertent activities of friendly ones as well.

To withstand these accidental and intentional interference threats, mission assurance requirements increasingly demand an end-to-end strategy for link protection that spans all phases from equipment R&D and test, to planning to operations and training.

A thorough SATCOM link protection strategy includes...

1. *SATCOM equipment with designed-in, adaptable link protection capabilities to include interference detection and cancellation. Satellite Channel Simulators, Satellite Transponder Simulators and Satellite Signal Emulators can be applied with excellent results during the proof-of-concept, R&D, test and production phases of SATCOM equipment.*

2. *Continuous, automatic monitoring at each SATCOM receive and transmit terminal. Advanced signal interference detection systems sense and warn when accidental or intentional interference is present.*

3. *Fast and automated response mechanisms to restore communications, including sophisticated Signal Geolocation Systems that can locate interference sources, with appropriate agencies using these results to guide resolution steps.*

4. *Ongoing on-site training to enhance the interference recognition and response skills of operators at both ends of a SATCOM link. Geolocation simulation systems are critical to developing and maintaining operator currency on emergent interference types and techniques, as well as the practical problems users and systems experience under interference conditions.*

5. *Thorough and automatic link protection and SATCOM system Self-Testing at each SATCOM terminal. The systems mentioned above assure nominal operation of the terminal, of the link protection gear, and provide early warning as to potential system failures.*

Designed-In Link Protection

Link protection begins long before a satellite is launched. *Channel Simulators*, *Transponder Simulators* and *Satellite Signal Emulators* are extremely valuable during the development and test of link-protecting 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 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 instruments fully emulate complex communications systems found on the emerging generation of channelized, multi-beamed satellites, such as the ***Wideband Global SATCOM*** (**WGS**) constellation.

These instruments, often used as shown in *Figure 1* on the following page, 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.

Link Protection Through Effective Monitoring

With well-designed and tested SATCOM systems in place that are 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 should 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

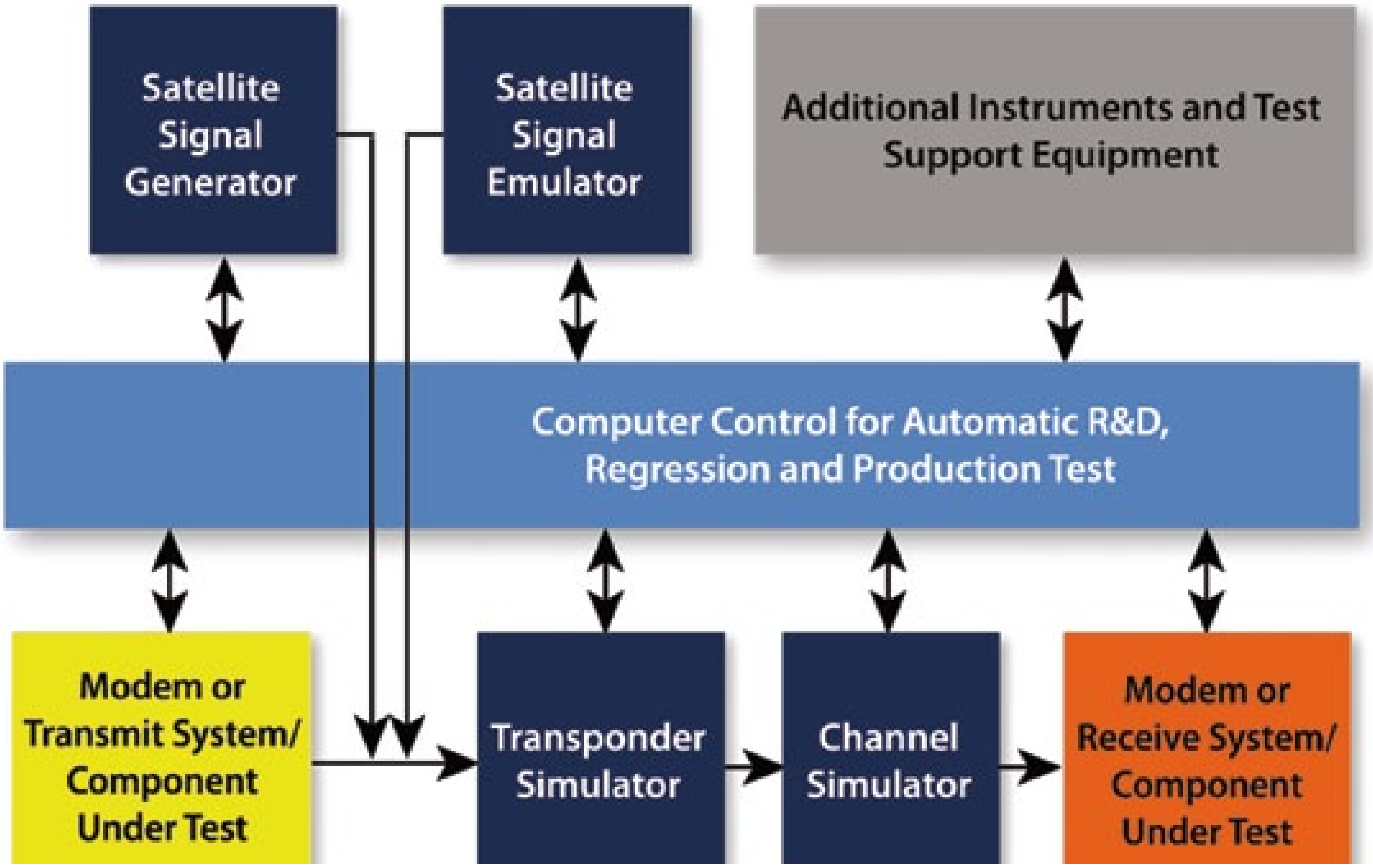

Satellite Signal Generator
Satellite Signal Emulator
Additional Instruments and Test Support Equipment
Computer Control for Automatic R&D, Regression and Production Test
Modem or Transmit System/ Component Under Test
Transponder Simulator
Channel Simulator
Modem or Receive System/ Component Under Test

Figure 1: Automated test equipment (ATE) setup for SATCOM device R&D, verification and validation.

type, data rate, coding scheme, modulation error ratio (MER), error vector magnitude (EVM) and bit error rate (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 quality of service (QOS), as shown in Figure 2 on the following page.

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 monitoring 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 time division multiple access (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.

When received or transmitted signals do not match parametric expectations, or are determined to be affected by interference, then 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.

Effective data logging should store historical, time-tagged measurement data for future trend analysis. Such a repository is useful for predicting equipment failures, communications outages, and impending electronic attack preceded by detectable signal trends. Historical data can also be exploited to differentiate equipment problems or operator error, and between accidental or intentional interference.

Link Protection Through Geolocation

When monitoring systems reveal unexplainable signal interference, the next step is to use *Signal Geolocation* systems to pinpoint the Earth location of the disrupting signal. Once a physical location estimate of the 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.

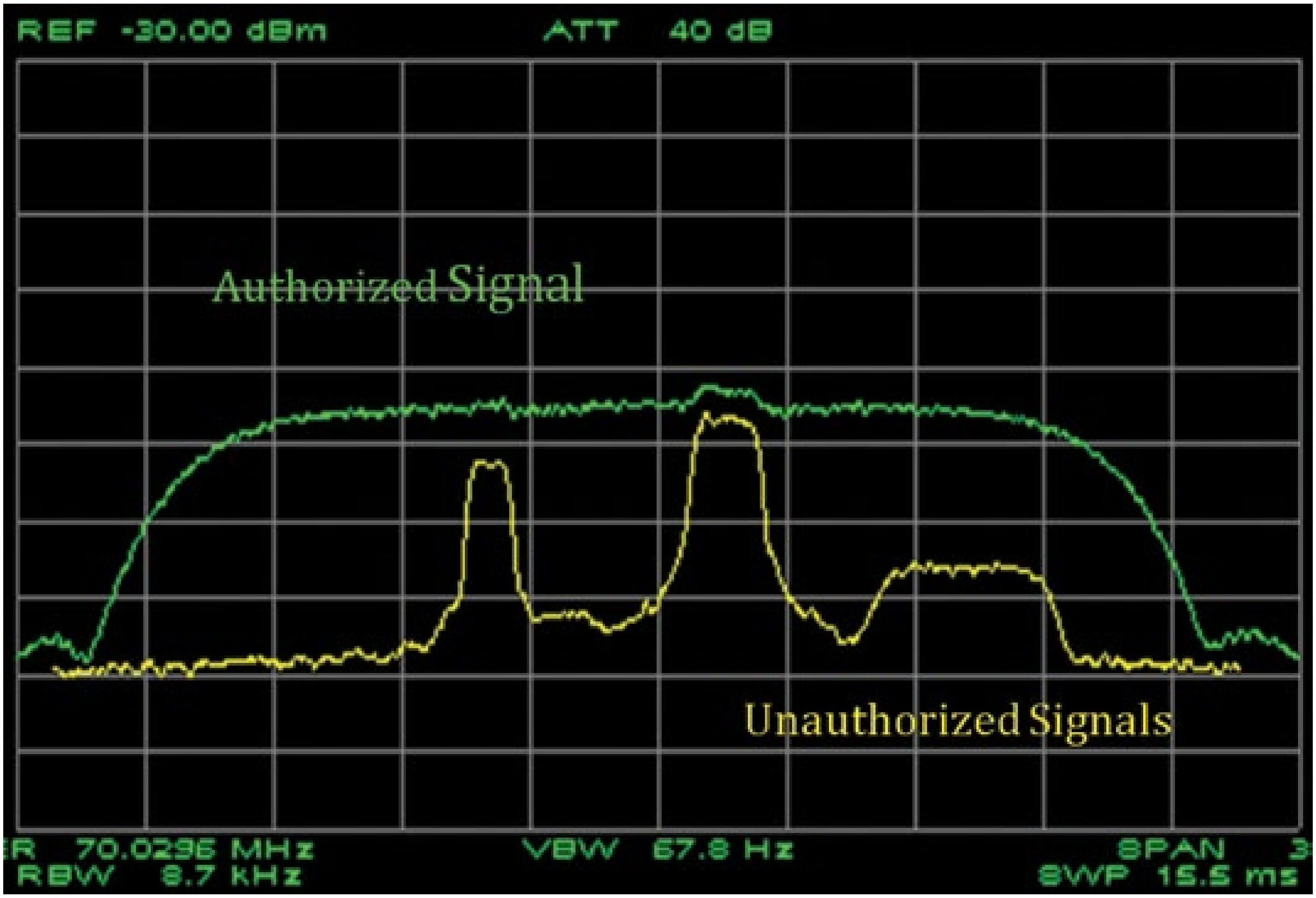


Figure 2: Capable interference detection systems reveal unauthorized signals invisible to standard spectrum analyzers.

The fastest and most accurate geolocation systems today receive SATCOM signals via two Earth-Satellite-Earth paths. They typically look at two signals during a geolocation—the interfering signal and a reference signal from a known location, as shown in *Figure 3* on the next page.

Geolocation systems analyze time difference, and Doppler shift-induced frequency difference between received signals to derive intersecting time difference of arrival (TDOA) lines and frequency difference of arrival (FDOA) lines. The conjunction of these lines represents the location of the interfering transmission source.

Link Protection Through Training

Unless SATCOM networks someday become fully self-healing, human operators and analysts will remain the ones who interact with link protection systems, interpret their results and take corrective action based on their indications. Operator familiarity with these systems dictates how quickly and correctly they can identify and resolve those problems.

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 can play in as well.

Training to high levels of geolocation understanding and effectiveness can be facilitated using sophisticated Geolocation Signal Simulators. These devices combine Channel Simulators and Signal Generators to create input signals 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.

These simulators allow operators to select ground locations for transmission and reception sites, choose satellites, enter antenna pattern information, and generate protected, interference and reference signals. They include simple setup, advanced underlying physics engines and full motion displays.

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.

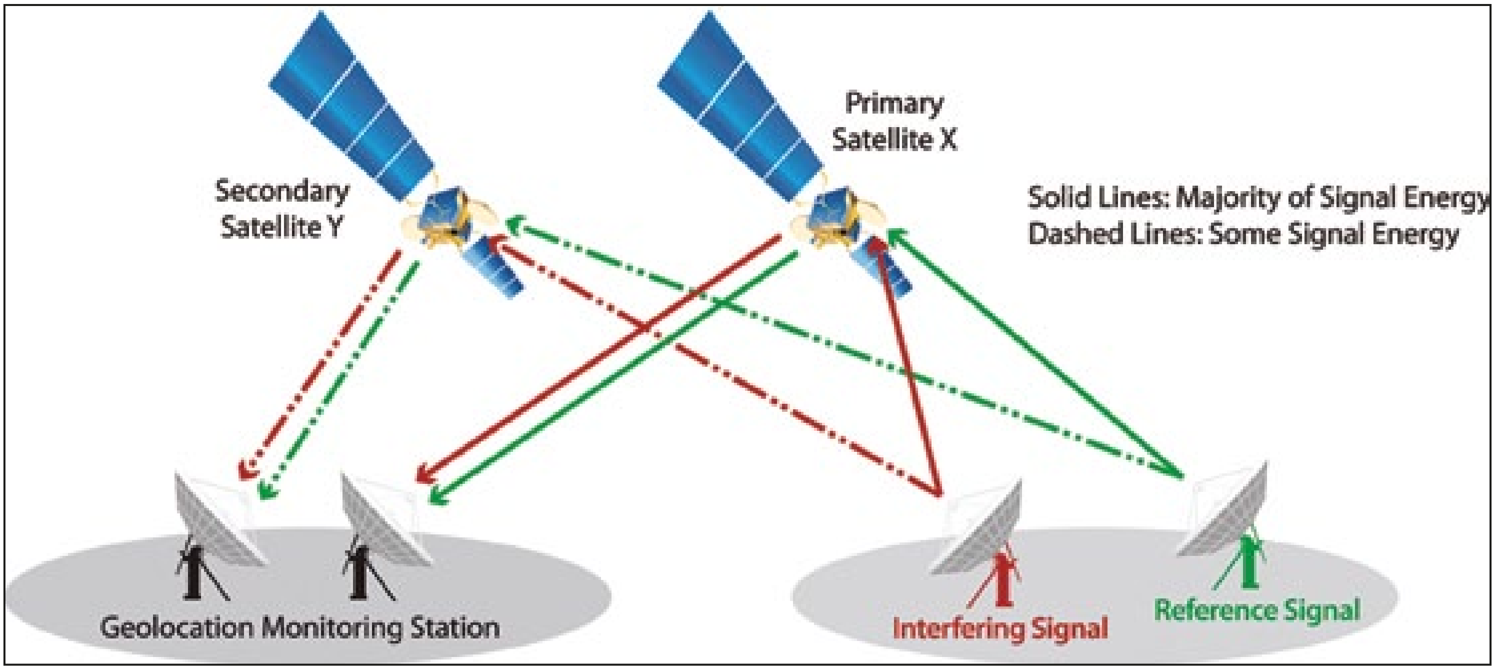

Primary Satellite X
Secondary Satellite Y
Solid Lines: Majority of Signal Energy
Dashed Lines: Some Signal Energy
Geolocation Monitoring Station
Interfering Signal
Reference Signal

Figure 3. State-of-the-art geolocation systems today use a two-path solution to find interfering signals.

By enabling deeper, repeatable, continuous training strategies these solutions allow operators to understand exactly how their equipment will perform under challenging signal conditions, giving them valuable experience to hasten recognition of signal issues, differentiate causes, and restore link performance and function.

Link Protection Through System 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.

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

An End-To-End Protection Strategy

SATCOM links are vital infrastructure elements in commercial, as well as military command and control (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 both aware and tolerant of interference. They must have relevant, application-focused, precision instrumentation to support their crucial RDT&E work.

In deployment, SATCOM operators must be able to 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. Nothing less than full life cycle vigilance will keep our military and commercial SATCOM at peak performance.

About the author

Steve Williams is the Business Area Manager of Signals Instrumentation at RT Logic and may be reached at ***swilliams@rtlogic.com.***

End-To-End Link Assurance Solutions

Kratos Defense & Security Solutions is focused on RF link protection solutions across the spectrum of mitigation touch points. The company's **RT Logic** and **SAT** subsidiaries specialize in developing COTS and tailored products for monitoring, detecting, characterizing and mitigating RF interference and other challenges to protected communications. RT Logic and SAT provide products and solutions to both commercial satellite operators and U.S. defense agencies on programs such as the U.S. Air Force's *Rapid Attack Identification Detection Reporting System* (**RAIDRS**), the *Joint Spectrum Center*'s **SPIRIT**, and the U.S. Army's *Wideband Remote Monitoring Sensor* (**WRMS**). Advanced products for RF link protection include:

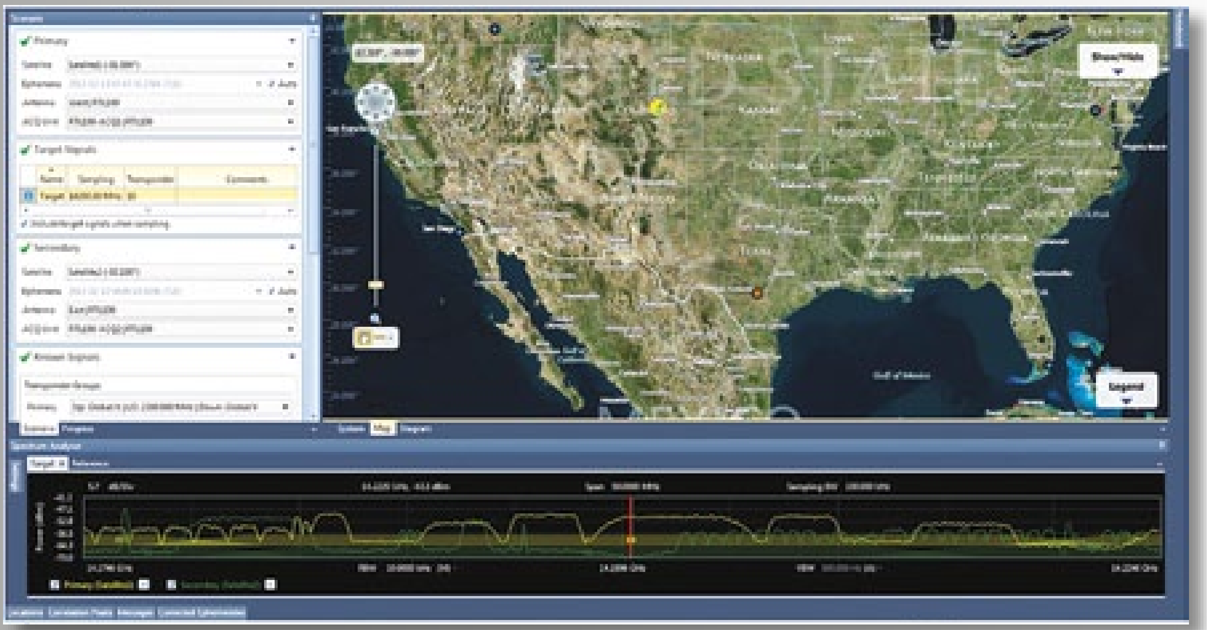
Channel Simulators: Building and Testing For Protection
RT Logic's family of Channel Simulators are used by SATCOM hardware, firmware and software designers to create hardware-in-the-loop tests that precisely simulate the punishing RF environments encountered on live missions. They create physics-accurate signals with characteristics such as dynamic time delay and phase offset allowing users to test the resilience of their modems and receivers against an array of natural and manmade disruptions. Armed with these results, engineers can innovate, tune and test their designs to create more robust and reliable communication systems.

Monics: Automated RF Interference Monitoring
Beyond built-in capabilities, reliable monitoring is the cornerstone for link assurance during mission operations. SAT's ***Monics***® is used by the majority of the satellite industry for networked advanced spectrum measurement and interference analysis as well as being the foundation of RT Logic/SAT tailored systems. Monics monitors satellite uplink and downlink performance while performing advanced interference detection and signal analysis. Highly scalable, Monics provides a fully distributed, autonomous solution for monitoring and detecting RF interference, including co-channel interference, as well as payload traffic and quality of service. To support truly comprehensive end-to-end (E2E) situational awareness, Monics is integrated into Kratos' ***Management Suite*** alongside it's ***Compass***™ satellite equipment *Monitoring & Control* **(M&C)** solution and ***NeuralStar***®, its enterprise "manager of managers" used by organizations such as the **Ballistic Missile Defense Agency**, the **U.S. Army**, **DISA** and other agencies.

satID: Integrated Monitoring And Geolocation
SAT's RF interference geolocation product, ***satID*** *(see screenshot below)*, is also integrated with Monics to deliver a seamless, accurate all-in-one solution for locating and identifying sources of interference due to equipment failure, operator error, intentional jamming, or unauthorized users. Employing the world's only global network of dual antenna sites, satID is available either as a product, or in a service-based model that can also include interference monitoring and managed network operations services.

satID GeoSim: Testing and Training
satID GeoSim is the newest product in RT Logic's testing and simulation portfolio, supporting a comprehensive link protection strategy in several ways. Starting at the earliest points in the process, engineers and planners use satID GeoSim to design link protection into their equipment and missions, as well as employing it as part of a comprehensive, automatic geolocation self-test strategy for ongoing peak performance. satID GeoSim also provides a solid foundation for continuous training efforts so that operators gain mission-critical experience and master essential techniques under a variety of conditions and interference scenarios. Because satID GeoSim's output is indistinguishable from the actual signals received from primary and secondary satellites in geolocation events (whether unintentional interference or deliberate jamming), it presents a dramatically more cost effective and repeatable solution over using actual satellites for these purposes.

For more information, please contact
satlinks@kratosdefense.com.


Primary
Target Signals
Secondary
Show/Hide
Legend