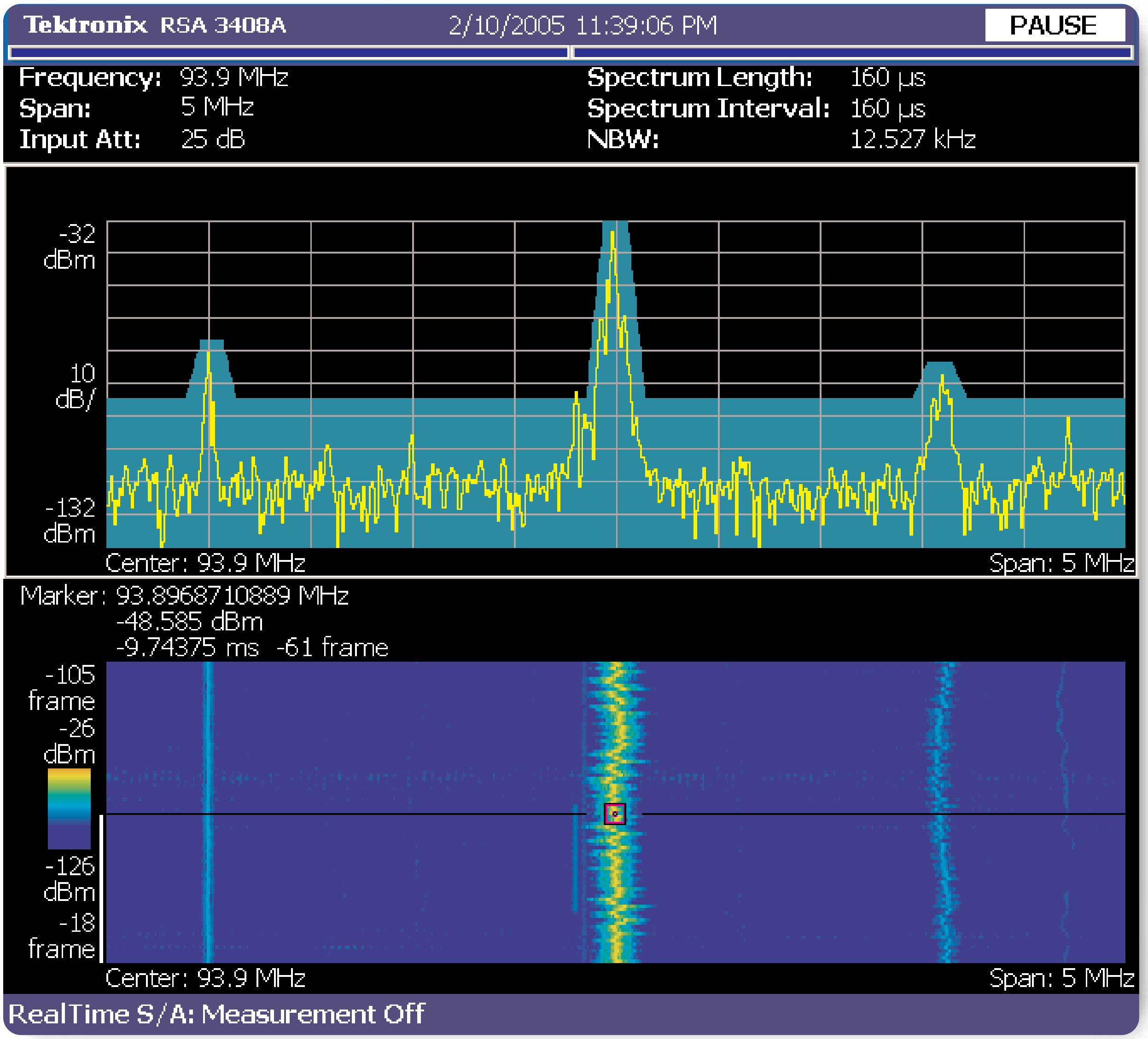
Application Note

Signal Monitoring, Surveillance and Real-Time Spectrum Analysis


Tektronix RSA 3408A 2/10/2005 11:39:06 PM

Frequency: 93.9 MHz
Span: 5 MHz
Input Att: 25 dB
Spectrum Length: 160 µs
Spectrum Interval: 160 µs
NBW: 12.527 kHz

Marker: 93.8968710889 MHz
-48.585 dBm
-9.74375 ms -61 frame

RealTime S/A: Measurement Off

Introduction

RF signal monitoring and surveillance applications have special equipment requirements that often go well beyond the typical radio receiver or spectrum analyzer. The Real-Time Spectrum Analyzer (RTSA) has many superior capabilities for signal monitoring and surveillance. In this application note, we review the basic challenges of intercepting and analyzing signals. Starting with overt compliance monitoring and advancing to the intercept of low probability of detection covert signals, RTSA technology for triggering, capturing and analyzing SIGnal INTelligence (SIGINT) is explained.

In recent years, the explosive growth of wireless devices and RF communications has created a significant challenge for the regulatory and intelligence communities. In this application note, we see how the RTSA technology can be used to gather key decision making information from today's challenging spectral environment.

To see how the RTSA can effectively capture the information needed, we begin with an overview of the technology followed by a brief look at its application to signal monitoring.

Next, the technical challenges of signal surveillance and key instrument performance traits are examined. This includes exploring the unique value of the RTSA's real-time frequency mask trigger technology for difficult to detect signals.

Finally, mining intelligence from captured waveforms with multi-domain demodulation measurements as well as some special features for working in a secure environment is presented.

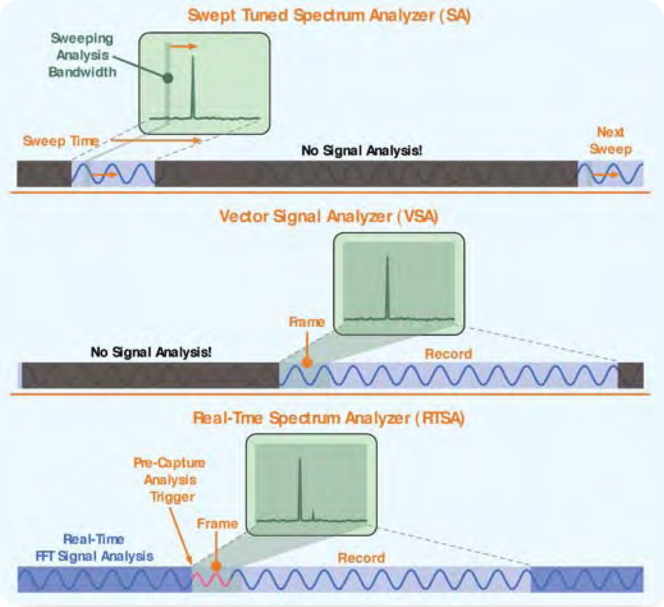

Swept Tuned Spectrum Analyzer (SA)
Sweeping Analysis Bandwidth
Sweep Time
No Signal Analysis!
Next Sweep
Vector Signal Analyzer (VSA)
Frame
No Signal Analysis!
Record
Real-Tme Spectrum Analyzer (RTSA)
Pre-Capture Analysis Trigger
Frame
Real-Time FFT Signal Analysis
Record

Figure 1. *The swept spectrum analyzer leaves large portions of time un-analyzed; similarly, the vector signal analyzer has little or no analysis ability in between signal recordings. The real-time spectrum analyzer can analyze the signal before and during a recording eliminating unaccounted for periods. This has made an important contribution to signal intelligence.*

RTSA Overview

The RTSA can trace its origins back to the demands of the signal intelligence community. Swept spectrum analyzers only capture intermittent samples of the RF spectrum. While sweeping across the span, only the very narrow resolution bandwidth is available for analysis. This leaves many spectral frequencies free to change undetected while they wait for the analysis bandwidth to reach them. The retrace periods in between sweeps are also unaccounted for, blanked out. Similarly, vector signal analyzers originally developed for repetitive CW modulations, have periods between recordings where no signal analysis occurs. Even with very long capture memories VSA's can miss important intermittent events.

To the intelligence community, these unaccounted for periods represent a significant problem. A signal burst could be quickly switched on and off to intentionally avoid interception with potentially grave consequences.

This problem led to the demand for a real-time spectrum analyzer that could pre-analyze the spectrum triggering only on significant signal events. This allows capture of important signal events and subsequent analysis of the signal in an efficient manner. Tektronix began pioneering this family of instruments over 20 years ago.

As signals grew in complexity, the need for precise event triggering became a critical requirement. Recording and analyzing long periods of inactivity quickly became impractical. This led to the development of the sophisticated real-time triggers now available in the modern RTSA.

The modern RTSA is designed to address the challenges associated with dynamic RF signals. The fundamental concept of real-time spectrum analysis is the ability to trigger in real-time on an RF signal's spectrum, seamlessly capture it into memory, and analyze it in multiple domains. This makes it possible to reliably detect and characterize signal energy that changes over time, essential to signal monitoring and surveillance applications.

The RTSA's RF front-end receiver can be tuned from DC to 8 GHz to down-convert the input signal to a fixed IF. The signal is then filtered, digitized by the Analog to Digital Converter (ADC), and passed to the Digital Signal Processing (DSP) engine that manages the instrument's triggering, memory, and analysis functions.

While many elements of this block diagram and acquisition process are similar to those of the traditional Vector Signal Analyzer's (VSA) architecture, the RTSA is optimized to deliver real-time triggering, seamless signal capture, and time-correlated multi-domain analysis. Its real-time capability enables the RTSA to capture certain signal bursts in complex spectral environments with 100% probability.

The RSA3408A has an analysis bandwidth of 36 MHz, a 3rd order intermodulation dynamic range of -78 dBc, a Displayed Average Noise Level (DANL) of -151 dBm/Hz at 1 GHz and a phase noise of -108 dBc/Hz @ 20 kHz. This combination allows the instrument to capture RF signals with excellent sensitivity under difficult spectral situations.

The RTSA supports a wide variety of modulation types and data rates, making it ideal for many monitoring and surveillance applications.

Broadcast Signal Monitoring

To illustrate the utility of the RTSA, let's look at its application to monitoring broadcast signals for regulatory compliance...

Regulatory Enforcement

The radio spectrum is a shared resource with extensive regulatory requirements necessary to avoid unwanted interference between users. Enforcement groups routinely monitor spectral emissions to ensure transmission equipment complies with regulations.

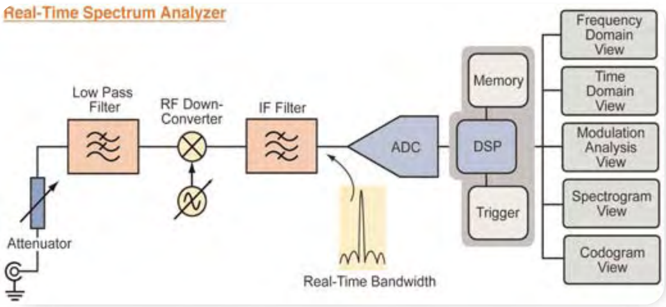


Figure 2. *The RTSA simplified block diagram showing the DSP, memory and real-time trigger.*

Compliance monitoring is often thought of as solely a governmental activity. In reality, many commercial enterprises continuously monitor signals. The growth of commercial signal monitoring applications has increased greatly with the explosion of wireless devices, global news coverage and frequency band auctions.

Determining fault in interference cases begins with monitoring of transmitted spectral emissions. Inadvertent interfering emissions can be very costly to cellular frequency band owners. Likewise, commercial broadcasters can lose substantial market audiences to a poorly controlled adjacent channel station. Satellite owner/operators require monitoring of their orbital assets. Similarly, teleport and gateway earth stations need to monitor signals not only for interference issues, but also for asset usage and billing purposes.

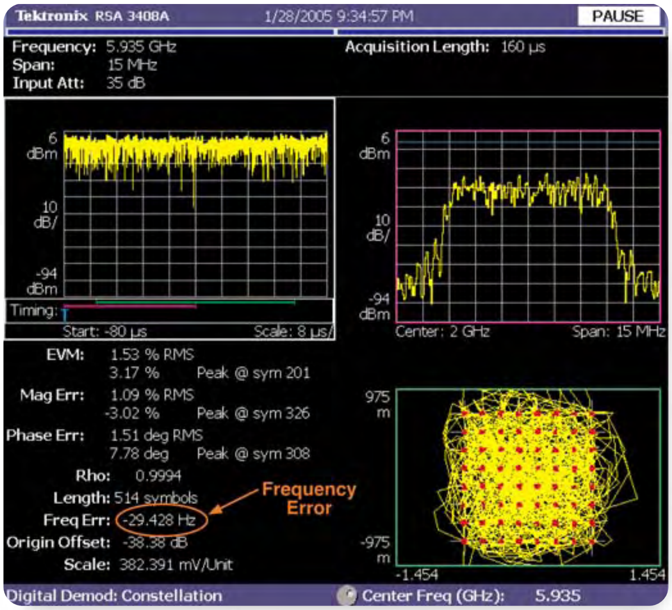
Spectral Measurements

Spectrum regulators usually specify several common spectral measurements to prevent interference. These primary measurements are can be monitored to determine if enforcement actions or fines are warranted.

Carrier frequency measurement ensures that the signal broadcaster is on the appropriate licensed channel. Determining the exact carrier frequencies for modern suppressed carrier modulations can be difficult. Unlike many swept spectrum analyzers, the RTSA can extract the frequency error from the actual signal. This is done by first setting the center frequency of the analyzer to the authorized channel frequency. The modulation parameters, symbol rate, filter type and shape, are then entered. The RTSA automatically locks to the signal and displays the channel frequency error in the Error Vector Magnitude (EVM) measurement mode. The frequency lock range of the instrument for demodulation of digital signals depends on the signal parameters, but can range between 15 kHz to the entire span of the instrument.

Once a regulator monitor finds the signal is on the right frequency, the next step is might be to validate it is the correct width. Occupied Band-Width (OBW) expressed as a percentage of the total transmission power, or Emissions Band-Width (EBW) expressed as an attenuation level in dB, are helpful in determining if the signal fits within the appropriate allocated bandwidth. The RTSA measures these signal characteristics at the touch of a button. The user can also alter the default measurement parameters such as bandwidth percentage or attenuation level, for special modulation requirements.

Spectrum management requires measurement of the signal levels present in each channel. RTSA incorporates an RMS voltage detector. This is helpful for determining the channel power statistics regulators use to judge if signal transmissions comply with legal requirements. Common envelope peak detectors used in many spectrum analyzers require a host of correction factors to estimate RMS signal power from peak voltages measurements. The RTSA's RMS detector can measure the signal power without peak to RMS correction factors. This is helpful for regulatory monitoring to determine the maximum and average power found in each channel.



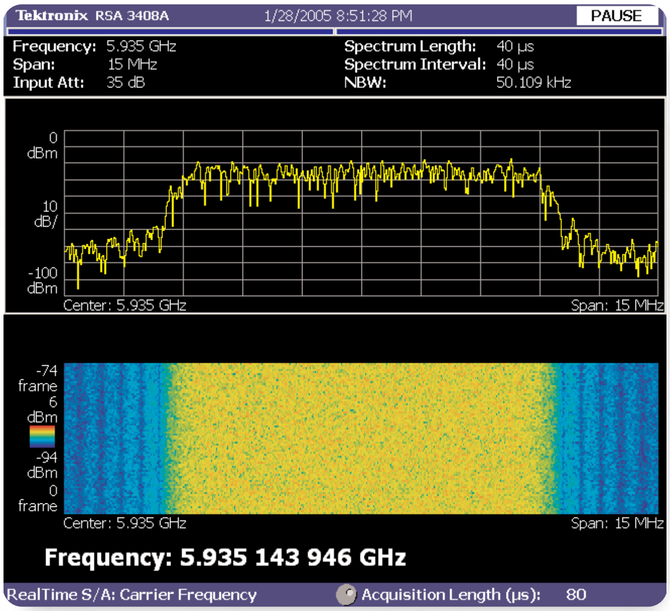
Tektronix RSA 3408A 1/28/2005 9:34:57 PM PAUSE

Frequency: 5.935 GHz
Span: 15 MHz
Input Att: 35 dB
Acquisition Length: 160 µs

EVM: 1.53 % RMS
3.17 % Peak @ sym 201
Mag Err: 1.09 % RMS
-3.02 % Peak @ sym 326
Phase Err: 1.51 deg RMS
7.78 deg Peak @ sym 308
Rho: 0.9994
Length: 514 symbols
Freq Err: -29.428 Hz
Origin Offset: -38.38 dB
Scale: 382.391 mV/Unit

Digital Demod: Constellation Center Freq (GHz): 5.935

Figure 3. *Signal frequency error of a 6 GHz, 64 QAM signal is measured in the EVM display revealing a -29.4 Hz error.*



Tektronix RSA 3408A 1/28/2005 8:51:28 PM PAUSE

Frequency: 5.935 GHz
Span: 15 MHz
Input Att: 35 dB
Spectrum Length: 40 µs
Spectrum Interval: 40 µs
NBW: 50.109 kHz

Frequency: 5.935 143 946 GHz

RealTime S/A: Carrier Frequency Acquisition Length (µs): 80

Figure 4. *The -40 dB emissions bandwidth EBW measurement shows that the signal fits within the 10 MHz regulatory requirements.*

Ensuring regulatory compliance by making spectral measurements often requires the use of remotely operated monitoring equipment. Remote or automatic operation in the field allows placement of the instrument in an optimal signal strength location. This improves the quality of the data collected without the expense or risks of placing a person in the field.

The RTSA's analysis software is Windows based and the equipment is LAN and IEEE-488 compatible. The Windows based software allows remote viewing of the display via popular software packages through the LAN connection. Adding a system controller enables RTSA, through its standard IEEE-488 bus or Ethernet connection with TekVisa, to be configured to automatically gather signal monitoring or intelligence data remotely in the field.

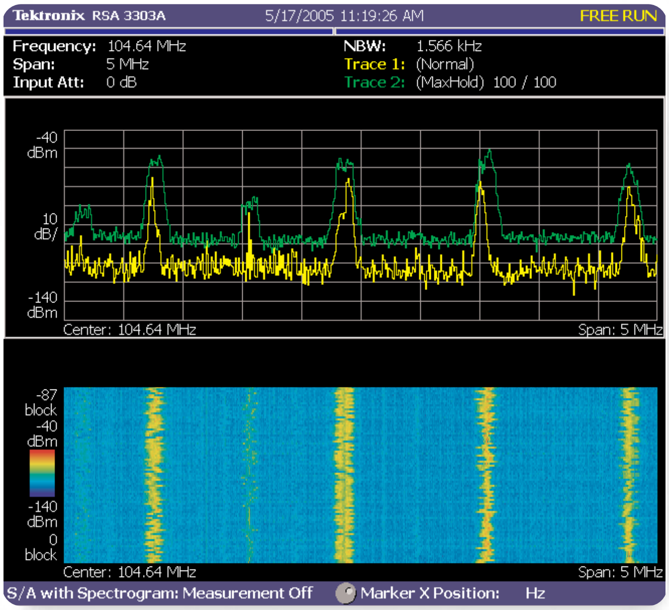
Challenges of Signal Surveillance

The terms signal surveillance and signal monitoring as used in this application note have different meanings. Signal monitoring means checking a signal primarily to prevent interference, maintain quality or take enforcement actions against the transmitter operator. Signal surveillance is used in the context of gathering information to survey the situation. Surveillance as used in this application note is primarily for the purpose of intelligence gathering. Surveillance is frequently done covertly so the target is unaware of the activity, whereas monitoring is often overt in nature.

Signal surveillance operations place additional demands on analysis equipment. Let's explore some of the well-known problems encountered with signal surveillance.

Sub-optimal Reception

The covert nature of RF signal surveillance usually requires the placement of an intercepting signal analyzer in a sub-optimal signal reception path relative to the intended receiver. Intercepting receivers are often placed far from the signal emitter of interest. Keeping the intercepting receiver in friendly territory, neutral airspace or international waters, eliminates the many challenges involved with placement and data retrieval from equipment located inside hostile territories.



Tektronix RSA 3303A 5/17/2005 11:19:26 AM FREE RUN

Frequency: 104.64 MHz
Span: 5 MHz
Input Att: 0 dB
NBW: 1.566 kHz
Trace 1: (Normal)
Trace 2: (MaxHold) 100 / 100

S/A with Spectrogram: Measurement Off
Marker X Position: Hz

Figure 5. *Max-hold and RMS detection are handy RTSA features for determining maximum and average power channel statistics for regulatory officials.*

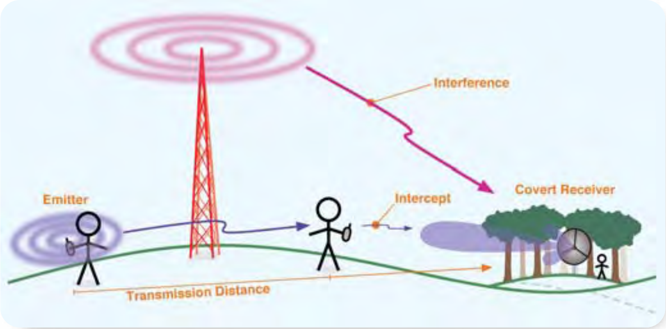


Figure 6. *Indirect reception paths often put the covert intercept at a significant signal disadvantage.*

Unfortunately, the long RF path characteristics associated with many surveillance missions, as well as covert antenna restrictions, usually translate to low received signal levels. Complicating matters further, strong interference from irrelevant commercial broadcasts can overload surveillance equipment. Additionally, the range of modulations presently encountered in the field has grown in recent years. Modern surveillance equipment needs the flexibility to intercept a wide variety of modulations including wireless standards to maximize the intelligence return for the cost and risks associated with deployment.

To overcome the sub-optimal conditions and complex signal environments, surveillance equipment needs to incorporate several important design attributes.

The Value of Dynamic Range

One important attribute of surveillance equipment is to have sufficient dynamic range and selectivity to avoid jamming from interferers closely located to the desired frequency.

Strong interferers can saturate Analog-to-Digital Converters (ADC's), blocking the reception of a desired weak signal. Strong interferers can also create intermodulation products in the analyzer that prevent successful demodulation of the desired signal. Unwanted intermodulation products also tend to clutter up the spectrum with meaningless signals that slow the spectrum survey process.

Having sufficient dynamic range allows the signal analyzer to separate weak signals in the presence of strong signals. The RTSA has 78 dB of intermodulation-free dynamic range, which enables the analyzer to handle a wide variety of surveillance applications. The RTSA's typical DANL of -151 dBm/Hz helps ensure that low-level signals are detected.

Low Phase Noise Receivers

Analyzer phase noise can also be an important attribute for many signal intercept applications. Even with outstanding dynamic range, if the analyzer's Local Oscillator (LO) phase noise is not sufficiently low, some signals may be impossible to receive. The LO in the analyzer's receiver can spread out adjacent signals to obscure the desired weak signal. Once obscured, the demodulator can no longer separate the two signals and the weaker signal is lost.

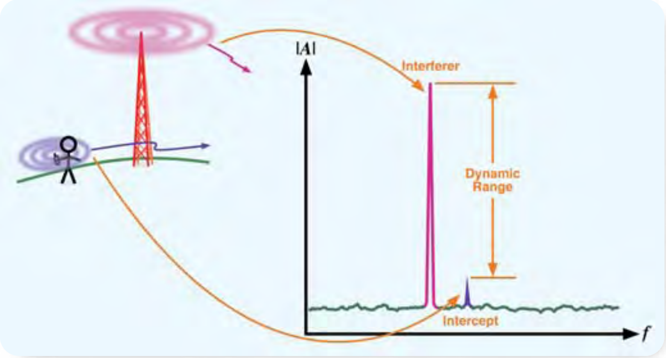


Figure 7. *Strong interferers can block reception, overloading analog to digital converters or creating intermodulation products in analyzers that don't have adequate dynamic range.*

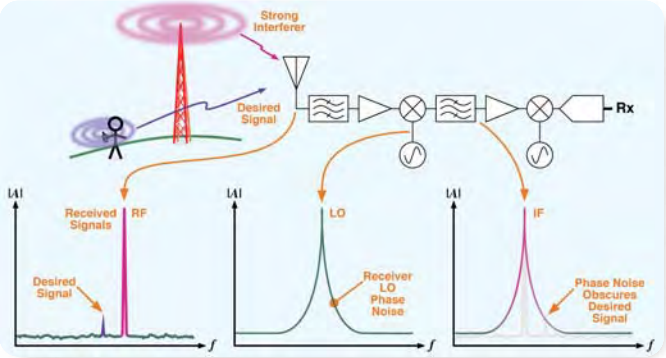
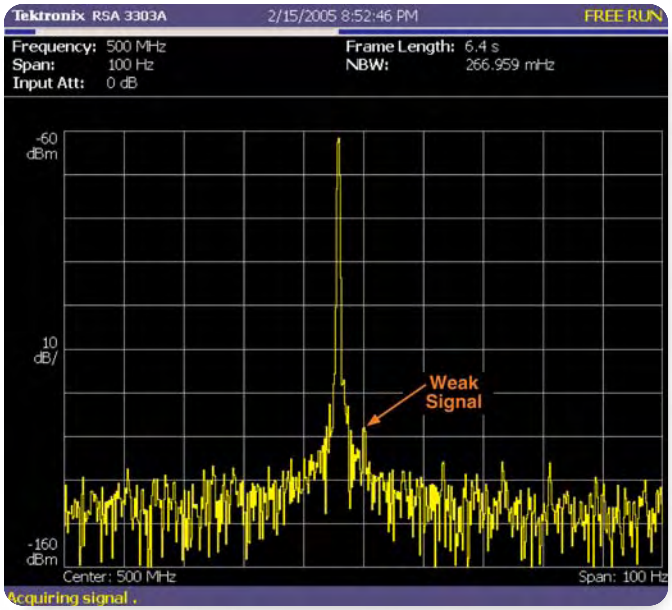


Figure 8. *Poor analyzer phase noise can prevent signal transmissions from being intercepted.*



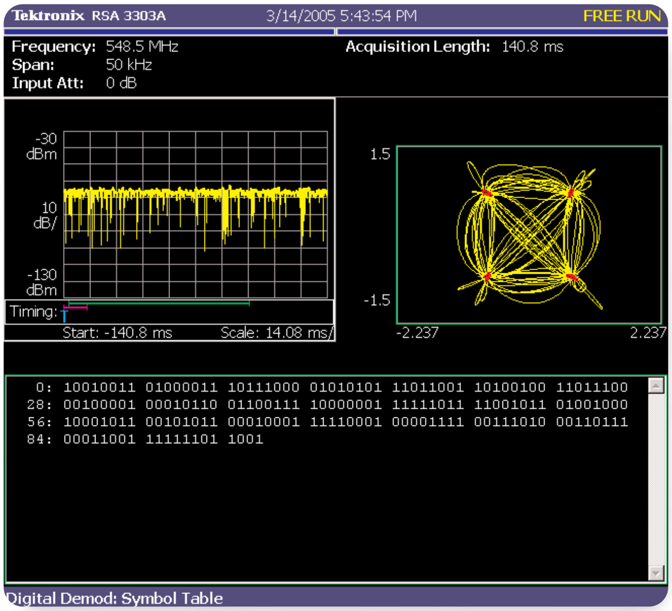
Tektronix RSA 3303A 2/15/2005 8:52:46 PM FREE RUN

Frequency: 500 MHz
Span: 100 Hz
Input Att: 0 dB
Frame Length: 6.4 s
NBW: 266.959 mHz

Center: 500 MHz Span: 100 Hz

Acquiring signal .

Figure 9. *RTSA's phase noise and dynamic range performance is sufficient to recover weak signals from difficult situations. A weak signal at the center of the span nearly 70 dBc below a powerful interferer and only 4 Hz away is not obscured by analyzer phase noise.*



Tektronix RSA 3303A 3/14/2005 5:43:54 PM FREE RUN

Frequency: 548.5 MHz
Span: 50 kHz
Input Att: 0 dB
Acquisition Length: 140.8 ms

Timing:
Start: -140.8 ms Scale: 14.08 ms/

```
 0: 10010011 01000011 10111000 01010101 11011001 10100100 11011100
28: 00100001 00010110 01100111 10000001 11111011 11001011 01001000
56: 10001011 00101011 00010001 11110001 00001111 00111010 00110111
84: 00011001 11111101 1001
```

Digital Demod: Symbol Table

Figure 10. *A good combination of dynamic range and low receiver phase noise allows the RTSA to capture difficult intercepts near strong emitters. A covert QPSK transmission is identified, captured and demodulated near a UHF television transmitter. In this case, a covert signal less than -60 dBm has been successfully detected then demodulated.*

Most high power transmitters generate signals with simple fixed frequency Local Oscillator (LOs) sources. Conversely, signal analyzers need highly tunable frequency sources. The tuning speed and frequency range of the analyzer sources can adversely affect its phase noise performance. Analyzers that have to tune broad frequency ranges often have poor phase noise in comparison to fixed tune, high-powered transmitters. This allows simple fixed tuned emitters to communicate with each other while many analyzers are unable to intercept their transmissions.

The RTSA, however, has solid phase noise performance of -108 dBc/Hz @ 20 kHz, allowing it to separate a wide variety of closely spaced signals of vastly different amplitude, where other analyzers fail.

Low Signal Level

The RTSA can also be equipped with an external preamplifier for applications where signal levels are near the thermal noise floor. The preamplifier is powered directly from the front panel of the instrument greatly improving weak signal performance. With the preamplifier, a DANL of -164 dBm/Hz at 2 GHz enables the RTSA to be quickly upgraded for weak signal intercept work.

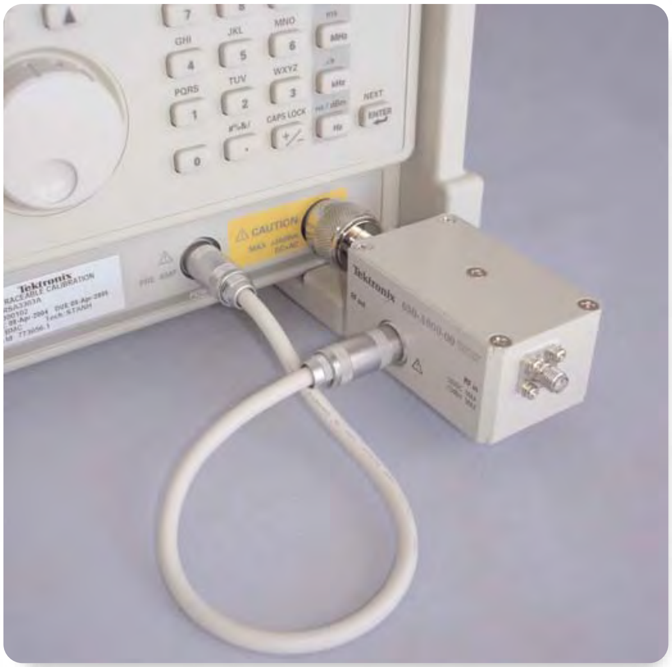


Figure 11. *Optional RTSA preamplifier lowers the analyzer noise floor and adds 20 dB of gain, improving reception performance. The preamplifier is powered directly from the RTSA.*

Good dynamic range, phase noise performance and noise figure are important analyzer prerequisites to combat the disadvantages of sub-optimal transmission paths. These attributes make the RTSA effective at intercepting normal signal transmissions under difficult circumstances.

Some signals, however, are designed to be difficult to intercept and demodulate. The RTSA offers some unique advantages over other analyzers in reliably intercepting these transmissions.

Surveillance of LPD Signals

There are two primary methods of preventing signal intercept: make signals that are hard to find or detect in the radio spectrum, and make signals that are difficult to demodulate/decode once found. Signals that are difficult to detect in the radio spectrum are said to have a Low Probability of Detection (LPD). Signals that are difficult to intercept information from, either because they are difficult to find or because they are difficult to demodulate/decode, have a Low Probability of Intercept (LPI).

One approach often used to avoid signal detection and interception is to hide the signal in the noise floor with spread spectrum techniques.

To uncover signals that are buried in a noise floor that appears flat, trace averaging can be used to reveal the shape of the spread spectrum signal hidden beneath.

Another approach to preventing signal detection is to send the information in a short burst. This approach to lowering the probability of detection attempts to slip a signal by the intercepting analyzer using the fact that most analyzers do not continuously analyze their signal inputs.

Signal Bursts

The signal burst or intermittent signal can be very difficult to detect. Long periods can elapse between very short transmissions. The intermittent signal can easily go undetected between the frequency samples of the conventional swept spectrum analyzer. Similarly, the unanalyzed periods between signal captures on the vector signal analyzer makes detection of intermittent signals a matter of chance. This forces many analyzers to rely on minimizing the sweep time and blanking time between captures, to improve the odds of detection. The classic approach has been to decrease the sweep time so the signal emitter is more likely to be discovered for a given burst length. Some signal analyzers are actually sold on their rapid sweep-time capability for improved probability of signal detection.

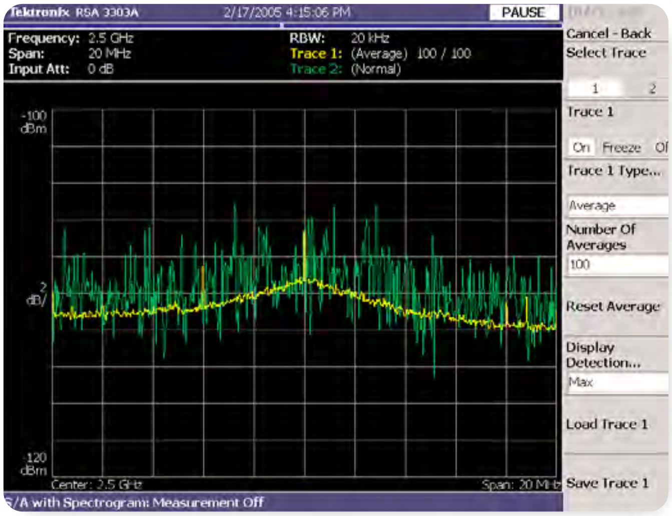

Tektronix RSA 3303A 2/17/2005 4:15:06 PM
Frequency: 2.5 GHz
Span: 20 MHz
Input Att: 0 dB
RBW: 20 kHz
Trace 1: (Average) 100 / 100
Trace 2: (Normal)
Trace 1 Type... Average
Number Of Averages 100
Display Detection... Max
Center: 2.5 GHz
Span: 20 MHz
S/A with Spectrogram: Measurement Off

Figure 12. *The use of trace averaging can make spread spectrum signals stand out from the noise floor. Two traces are turned on, one with averaging and one without. The averaging clearly shows something lurking in the noise.*

The RTSA presents a unique solution to reliably capturing the LPD signal. Its real-time pre-capture analysis ability can improve the probability of detection to 100%.

The reader may wonder exactly what makes a RTSA so unique and how it can reliably capture events, other analyzers cannot?

The RTSA's unique abilities come from its real-time Fast Fourier Transform (FFT) and Frequency Mask Trigger (FMT). To understand how the RTSA can pre-analyze and trigger a capture of critical events, let's have a closer look at the FFT process.

The FFT Process

The analyzer begins by taking time samples of the input signal at a rate of at least twice the frequency of interest (Nyquist rate) or greater to avoid signal alias effects. The time samples are grouped into frames of data. Each frame contains the exact integer set of data necessary for the FFT process.

The truncated data samples at each end of the frame can contain an abrupt discontinuity that will cause spectral spreading when transformed from the time domain to the frequency domain. To minimize the effect of this discontinuity, a windowing function is used to scale the amplitude of the time-sampled data. The RTSA offers a variety of popular windowing functions such as the Hanning, Hamming, Blackman, Blackman/Harris, Parzen, Welch and others.

After the frame's data has been scaled by the windowing function, the Fast Fourier Transform is calculated, transforming the data from amplitude versus time to amplitude versus frequency. The FFT requires the execution of a variety of data computations in order to determine the amplitude of each frequency segment or "bucket."

The greater the number of samples in each frame, the finer the frequency resolution after the transformation is complete. Unfortunately, this also means the greater the number of necessary data computations, to transform the frame. The FFT process is well known for its intense computational requirements.

Unique Real-Time vs. Common Post-Processing

The computational time required for transforming the time sampled frame to the frequency domain varies depending on the number of points to be transformed and the speed at which the computations can be performed.

If the necessary FFT computations can be performed in a period of time shorter than that required to time sample each frame, the FFT is a "real-time" FFT. If the FFT takes longer than the time sampling of one frame, it is not a real-time FFT.

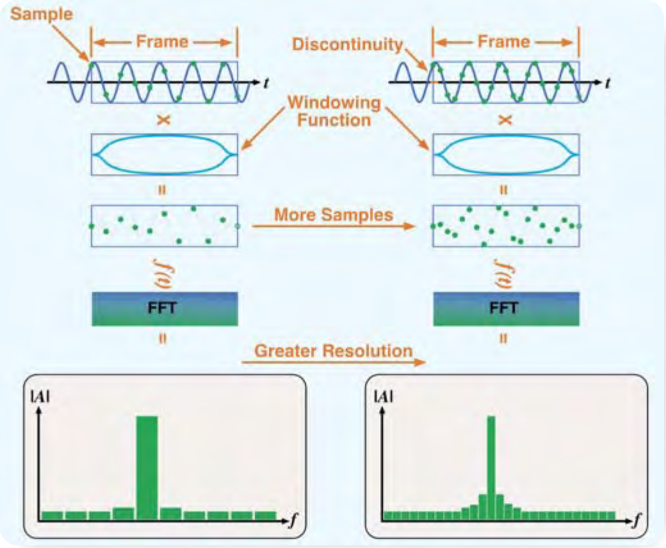


Figure 13. *The sampling and FFT process shows that more time domain samples increases frequency domain resolution, but this requires longer digital signal processing time to complete each FFT frame.*

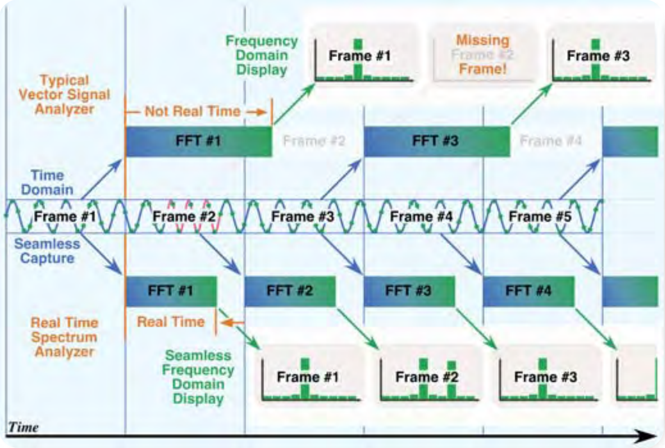


Figure 14. *The RTSA is unique in its triggering ability because it possesses a real-time DSP hardware FFT that is capable of converting each frame to the frequency domain prior to the completion of the time sampling of the next frame. This enables the RTSA to continually analyze the frequency content of the incoming signal prior to capturing the time-sampled data record.*

The digital signal processing speed required for wide bandwidth signals being sampled at high rates becomes quite intensive. For example, to execute a 1024-point FFT in 12 μs before the next data frame is ready requires a respectable amount of DSP horsepower.

To avoid this intensive DSP computational requirement, virtually all vector signal analyzers use batch post processing of the FFT. This means they capture the entire time-sampled data record and then batch post process each frame's FFT to create the frequency domain display. This common technique of post processing eliminates the need for very high speed DSP hardware and allows the use of low cost generic computers. Unfortunately, with batch post processing, spectral information is not available until after the complete data record is captured. This prevents vector signal analyzers from previewing the signals spectrum prior to capturing a data record.

Conversely, the RTSA with its real-time FFT capability can preview the signals spectrum continuously until an event of interest is detected and then capture the data.

The RTSA has the ability to do both real-time FFT processing of the input signal and batch post processing of the captured time-sampled record. This gives the RTSA the unique spectral preview capability associated with the real-time FFT as well as the in-depth analysis capability of post processing.

The advantages of the real-time spectrum analyzer's unique DSP capabilities are of particular interest in surveillance work. The ability to convert the time domain waveform samples into the frequency domain in real-time enables exclusive features like Tektronix's patented Frequency Mask Trigger (FMT). The FMT is ideal for reliably capturing elusive LPD signal bursts.

The Frequency Mask Trigger

Why is the FMT so useful for capturing LPD signals? LPD signals are frequently hidden amongst strong signals to make them more difficult to detect. To reduce their probability of detection further, short transmission bursts at low power may be used. Conventional IF power level detectors found on most vector signal analyzers cannot be used to trigger a capture of these LPD bursts. The IF level detector measures only the most powerful adjacent signals and fails to detect lower power signals of interest.

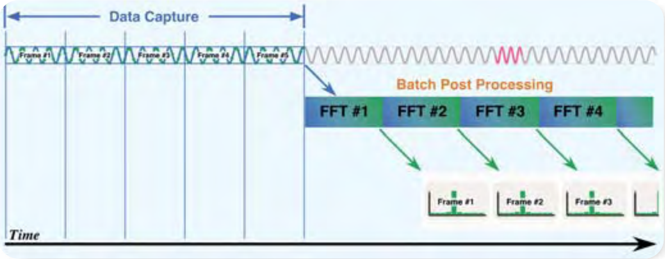
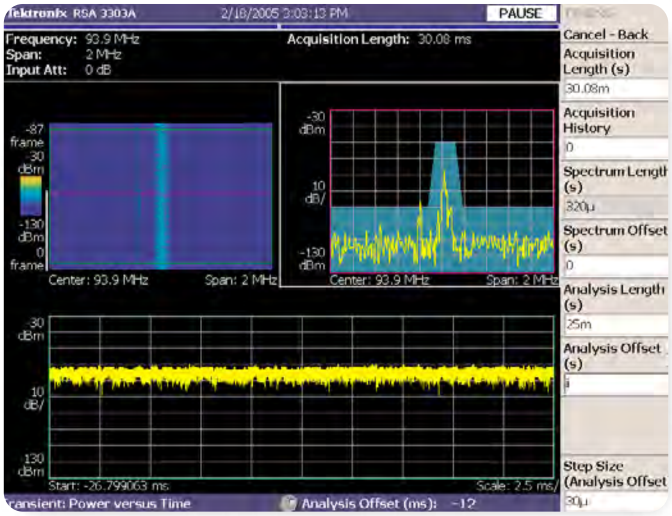


Figure 15. *Vector signal analyzer's capture the entire time domain data record and then convert it to the frequency domain by batch post processing the data with an FFT. Unfortunately, post processing the time-sampled data does not allow a spectral preview of the signal for transient events prior to capturing the time record.*


Tektronix RSA 3303A 2/18/2005 3:03:13 PM PAUSE

Frequency: 93.9 MHz
Span: 2 MHz
Input Att: 0 dB

Acquisition Length: 30.08 ms

Cancel - Back
Acquisition Length (s): 30.08m
Acquisition History: 0
Spectrum Length (s): 320µ
Spectrum Offset (s): 0
Analysis Length (s): 25m
Analysis Offset (s): i
Step Size (Analysis Offset: 30µ

Transient: Power versus Time
Analysis Offset (ms): -12

Figure 16. *TIF level remains constant, while the FMT captures a low power intermittent transmitter spectrogram. The constant IF level shows that conventional IF power level triggering would be useless.*

The FMT can analyze the input signal for transmission bursts and trigger a data capture recording of a signal event. The FMT is a user definable, frequency selectable trigger mask. Since the FMT is based on the real-time FFT, if any signal pops up out of the noise spectrum, it has a 100% probability of triggering a data capture. The real-time FFT has no blanking or analysis gaps like the swept spectrum analyzer or vector signal analyzer.

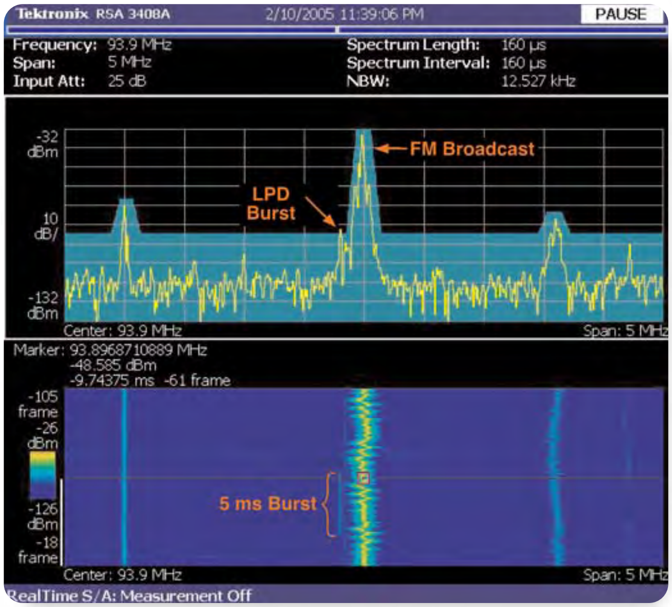
Many LPD transmission bursts occur intermittently, with long periods, hours or days, between bursts. Using the FMT to provide real-time analysis of the frequency spectrum before triggering eliminates the need to capture extremely long signal records to memory. This greatly reduces the memory requirements for the analyzer or external data storage system.

The FMT also eliminates the need for data searches to find the event of interest. Since the signal capture begins with the spectral event trigger, it is not necessary to search long captures after post processing to locate an event of interest. This also minimizes the amount of memory necessary to produce meaningful data intercepts.

To capture this important type of signal intercept the RTSA user begins by surveying the spectral band. This can be accomplished in Spectrum Analyzer (SA) mode with Spectrogram. SA mode emulates a conventional swept spectrum analyzer, allowing start and stop frequencies far wider than the RSA3408A's 36 MHz of real-time bandwidth. The analyst can use this wide band picture to look for emitters of interest.

Once the area of spectral interest is identified, the analyst may wish to set up a FMT to capture LPI burst signals that pop up.

The FMT is setup from the trigger menu. The RTSA offers the typical selections of trigger options: External, Power (IF Level) triggering; single or continuous captures; and the FMT.



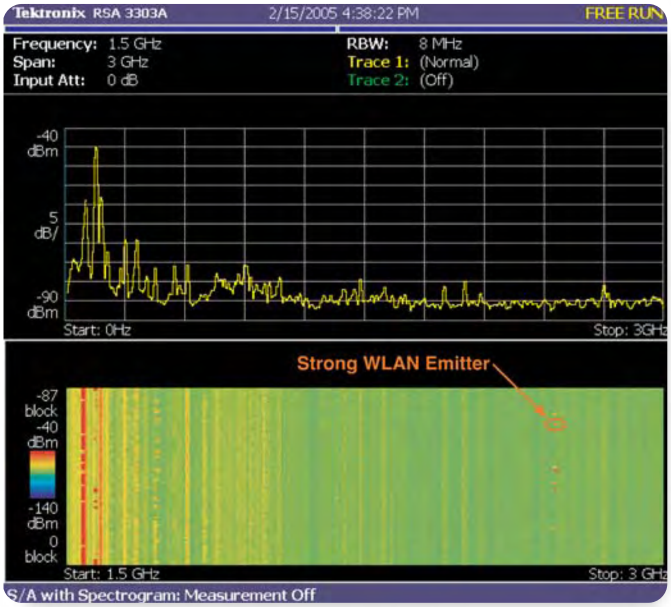
Tektronix RSA 3408A 2/10/2005 11:39:06 PM PAUSE

Frequency: 93.9 MHz
Span: 5 MHz
Input Att: 25 dB
Spectrum Length: 160 µs
Spectrum Interval: 160 µs
NBW: 12.527 kHz

Marker: 93.8968710889 MHz
-48.585 dBm
-9.74375 ms -61 frame

RealTime S/A: Measurement Off

Figure 17. *FMT triggers a capture of a low level transmission hidden in the presence of several strong FM broadcast radio stations. Nearly 100,000 times less power or 50 dBc below the strong FM signal and only 5 ms long, the RTSA triggers and captures an LPD burst for analysis.*



Tektronix RSA 3303A 2/15/2005 4:38:22 PM FREE RUN

Frequency: 1.5 GHz
Span: 3 GHz
Input Att: 0 dB
RBW: 8 MHz
Trace 1: (Normal)
Trace 2: (Off)

S/A with Spectrogram: Measurement Off

Figure 18. *SA with Spectrogram Mode emulates a swept spectrum analyzer. This allows the signal analyst to survey many spectral bands at once, finding interesting signals like the strong WLAN emitters at 2.4 GHz. The spectrogram captures signals that could go undetected with a conventional spectrum analyzer display.*

Complex frequency masks can be created by simply double clicking with the mouse to add points and dragging them to the appropriate location. The user is able to select many points and the mask is definable to -60 dB of full screen signal levels. Frequency masks can also be created by directly entering in the X (Hz) and Y (dBm) values for each point. Direct entry of the values is particularly useful for signal monitoring applications where regulatory masks are necessary. The user should be aware that since the FFT creates frequency "bins" or buckets based on the number of sample points included in each FFT frame, some quantization occurs with frequency mask points. In Real-Time mode, the number of FFT points in the span is fixed at 1024.

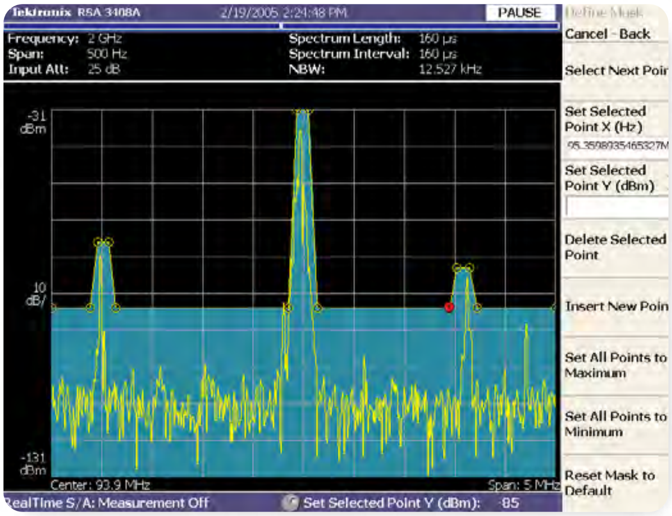
In continuous capture mode, the RTSA allows the user to see spectral captures while the mask is being adjusted. This is helpful for setting the mask sufficiently above the noise floor to avoid false triggers. The bottom of the mask is raised high enough to stop the noise from triggering the instrument. Using the Stop and Show Results key under the Trigger menu, a test trigger can be initiated to verify that the spectrum is properly contained within the mask. The instrument is then ready to capture the intermittent signal burst.

Under IEEE-488 Bus or Ethernet control, each triggered capture can then be saved for subsequent analysis.

Signal Identification & Intelligence

Once a signal of interest is detected and captured, the next step is to analyze the signal to extract useful information. Usually signal surveillance seeks to answer three basic questions: Who or what is out there? Where are they? What are they doing or going to do? There are many ways to mine information from transmitted RF signals to answer some of these questions.

The RTSA's multi-domain analysis ability and signal measurements can provide a wealth of information to the analyst.



Tektronix RSA 3408A 2/19/2005 2:24:48 PM PAUSE

Frequency: 2 GHz
Span: 500 Hz
Input Att: 25 dB

Spectrum Length: 160 µs
Spectrum Interval: 160 µs
NBW: 12.527 kHz

Center: 93.9 MHz Span: 5 MHz

RealTime S/A: Measurement Off Set Selected Point Y (dBm): -85

Set Selected Point X (Hz): 95.3598935465327M

Figure 19. *Frequency Mask trigger setup is easily done using either a USB mouse or the keypad.*

Extracting Key Information

Often the first step in extracting useful information from a received signal is not demodulating it, but rather identifying what it came from. Measuring some basic signal parameters can quickly help to identify the probable source, answering the question, "Who or what is out there?"

The frequency band of a signal often narrows the possibilities. Maritime radars, for example, work well at frequencies around 3.0 GHz because of its propagation characteristics and the physical size of common targets relative to the signal wavelength. Ground based vehicles might prefer lower frequencies like 30 to 50 MHz communication radios to improve non line of sight communications. The OBW or EBW can also be helpful in determining the probable source. Differing bandwidths can provide an indication of the nature of the radio application. Narrow-band signals are more likely voice information whereas wide-band signals more likely indicate video or multiplexed signal information. The RTSA provides signal bandwidth information automatically with a quick menu selection.

The RTSA also has an overlapping FFT capability that is helpful at narrow spectral spans.

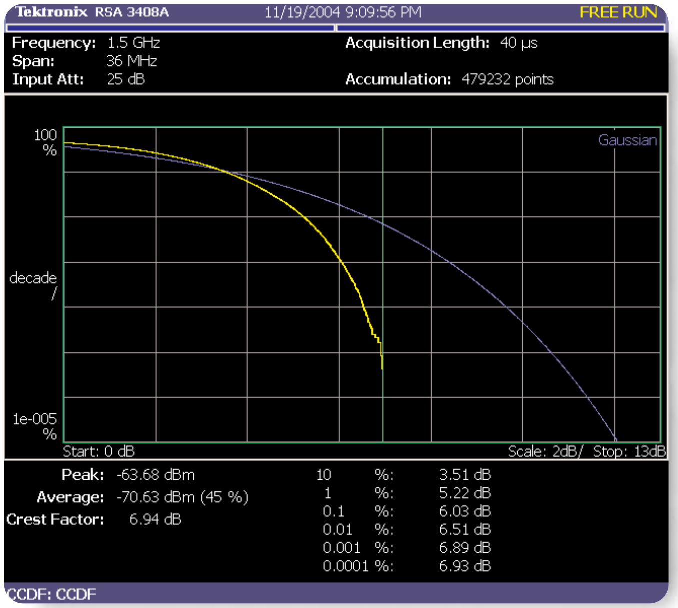
Measurements such as the Complementary Cumulative Distribution Function (CCDF) can provide additional information as to “what is out there.” Some transmitters operate in a class “C” mode with saturated power amplifiers, whereas some operate linearly in class “A” mode. Measuring the CCDF curve can be helpful in sorting out what type of transmitter is out there. CCDF signatures may even be useful in discriminating between identical models of the same type of transmitter. PA saturation characteristics can differ enough between some emitters to be visible on the CCDF plot. This can be employed for very low-level emitter specific identification problems.

Using these simple measurements, a significant amount of intelligence can be gained on RF transmitters.

The RTSA display also has the current time and date prominently shown on the screen. This is helpful for the analyst in determining the signal’s importance. Is the triggered capture on the display the 9:00 PM commuter flight departing or a contraband smuggler rumored to be departing at 9:10 PM?

Identifying the emitter with simple signal measurements is fast and easy with convenient single button measurements. They can help to rapidly classify what is out there. This allows the analyst to ignore the unimportant and focus on the important. Additionally, non-demodulated measurements don’t provoke the same level of privacy intrusion concerns as demodulated measurements can.

The RTSA display has a complete set of markers and dual trace capabilities for comparative measurements. These display capabilities can be helpful in estimating emitter range and comparing signal traces to previously captured data. Display configurations such as Max. Hold, Min. Hold and Averaging are also useful.



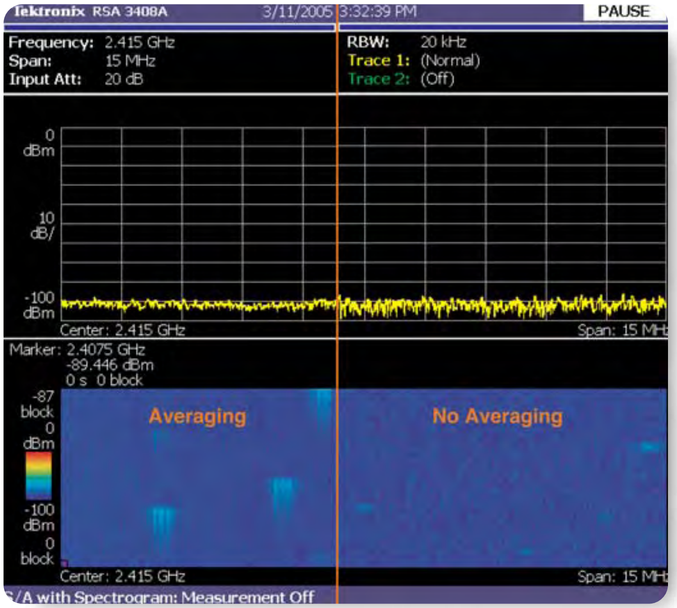
Frequency: 1.5 GHz
Span: 36 MHz
Input Att: 25 dB
Acquisition Length: 40 µs
Accumulation: 479232 points

Start: 0 dB
Scale: 2dB/ Stop: 13dB

Peak: -63.68 dBm
Average: -70.63 dBm (45 %)
Crest Factor: 6.94 dB

```
10     %:  3.51 dB
1      %:  5.22 dB
0.1    %:  6.03 dB
0.01   %:  6.51 dB
0.001  %:  6.89 dB
0.0001 %:  6.93 dB
```

Figure 20. *CCDF signatures can be helpful in determining what type of emitter and possibly which serial number unit produced the signal.*



Frequency: 2.415 GHz
Span: 15 MHz
Input Att: 20 dB
RBW: 20 kHz
Trace 1: (Normal)
Trace 2: (Off)

Center: 2.415 GHz
Span: 15 MHz

Marker: 2.4075 GHz
-89.446 dBm
0 s 0 block

Center: 2.415 GHz
Span: 15 MHz

Figure 21. *Two spectrograms of intermittent signals are compared. Adding a small amount of trace averaging, which also applies to the spectrogram, can make short duration events very apparent.*

The ability to quickly manipulate the display, frequency and span is important for many surveillance operations. Features such as marker to center frequency and other time saving commands need to be kept at top level menus or on dedicated keys to make the most efficient use of what is often limited signal observation opportunities. The RTSA incorporates the best practices of the industry by providing a simple, fast and intuitive front panel access to important functions.

Once signals are captured and classified, emitters of particular interest may warrant further detailed modulation analysis.

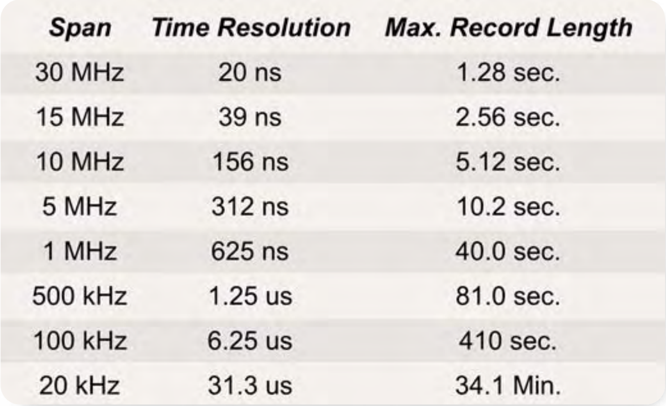
Modulation Analysis

Demodulation of a signal can provide a wealth of data including the information content of the transmission. The information content of a signal can be used to help answer the question, “What are they doing or going to do?” Demodulation of the information content does create many ethical and legal issues of privacy invasion, so information collection units must exercise good judgment as to its use.

Using the RTSA’s demodulation capabilities significantly expands the signal identification measurements possible over simple time or frequency domain metrics. Precise carrier frequency information for suppressed carrier signals, constellation geometries and other parameters useful for identification can be measured. Most importantly, the actual data in the signal transmission can be accessed.

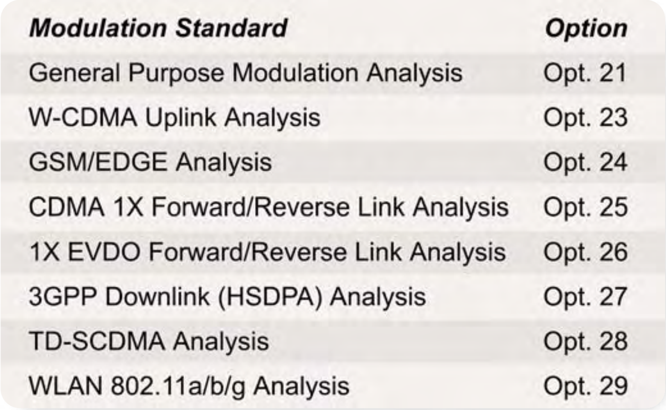
It is important to note that the RTSA’s onboard demodulator is a block demodulation instrument. This means the actual demodulation takes place after the signal has been recorded to memory. Block demodulation places limitations on the amount of time available for a signal to be demodulated before the memory block is exhausted.

Short transmissions, such as half duplexed air traffic control communications or police radio communications, are easily captured and demodulated with a block demodulation instrument. Continuous wideband communication signals generally require a real-time dedicated demodulator to prevent data loss. The RTSA can also be useful for continuous wideband applications as a front end down converter and digitizer.



Span	Time Resolution	Max. Record Length
30 MHz	20 ns	1.28 sec.
15 MHz	39 ns	2.56 sec.
10 MHz	156 ns	5.12 sec.
5 MHz	312 ns	10.2 sec.
1 MHz	625 ns	40.0 sec.
500 kHz	1.25 us	81.0 sec.
100 kHz	6.25 us	410 sec.
20 kHz	31.3 us	34.1 Min.

Table 1. *Memory limits the available recording time for block demodulators. A narrowband RF signal occupying 100 kHz, such as an FSK cordless phone, can be recorded for several minutes. Broadband devices can only be recorded for a few seconds or less.*



Modulation Standard	Option
General Purpose Modulation Analysis	Opt. 21
W-CDMA Uplink Analysis	Opt. 23
GSM/EDGE Analysis	Opt. 24
CDMA 1X Forward/Reverse Link Analysis	Opt. 25
1X EVDO Forward/Reverse Link Analysis	Opt. 26
3GPP Downlink (HSDPA) Analysis	Opt. 27
TD-SCDMA Analysis	Opt. 28
WLAN 802.11a/b/g Analysis	Opt. 29

Table 2. *Available modulation ‘standards’ based analysis options.*

The RTSA’s built in block demodulator supports many modulation standards and has the flexibility to demodulate a variety of common modulation types for many collection operations. Each modulation type further allows users to control symbol clock rates, base-band filtering type and filter shape (alpha).

Popular wireless communication modulation standards used throughout the world are also supported by the RTSA. This makes collection and demodulation of information content simple to set up. In the field, it is easy to begin producing useful intelligence quickly.

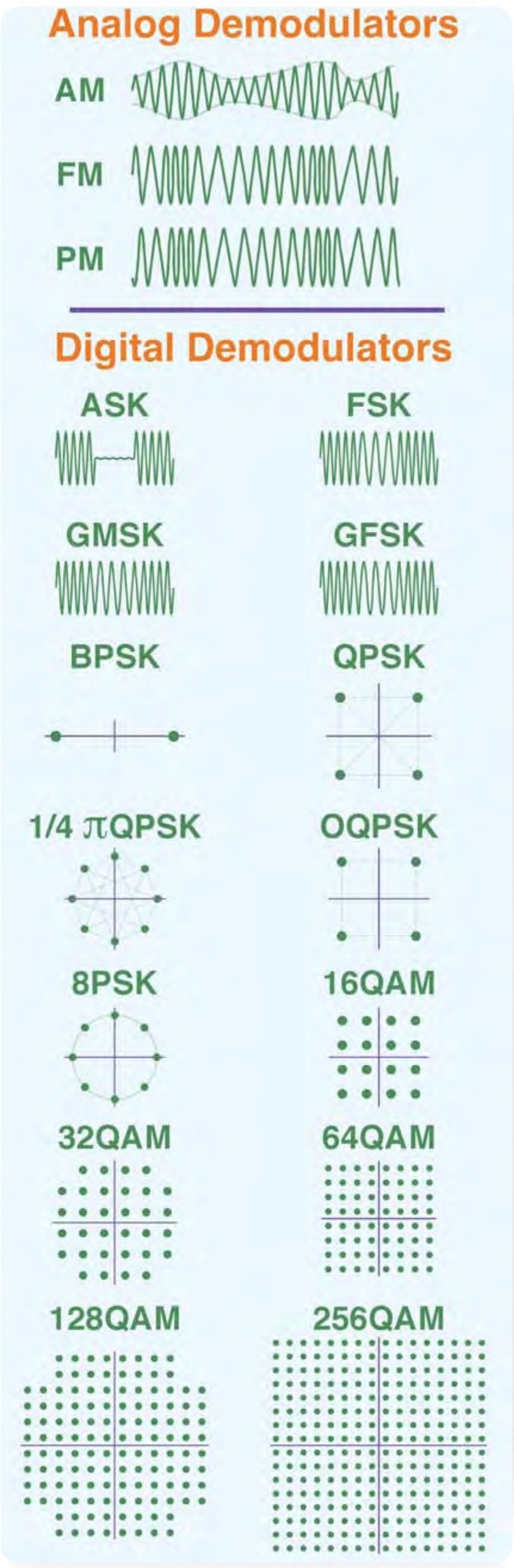


Table 22. *RSA3408A Supported Modulations.*

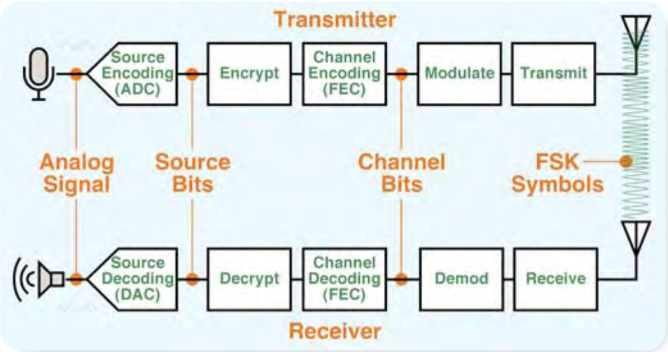


Figure 23. *Source bits are unencrypted and have no error correction encoding. Channel bits are delivered to the modulator and recovered in the demodulator. Symbols are modulated representations of the channel bits.*

Less common modulations, or those that require continuous demodulation for long periods, can be supported with external demodulators driven from the optional RTSA real-time I-Q outputs. I-Q outputs can be important for many operations that initially begin as a routine collection of intelligence and expand as new signal energy is discovered. Expansion capability minimizes the required capital expenses to keep up with new emitters.

The RSA3408A also features bit decoding for Amplitude Shift Keying (ASK) and Frequency Shift Keying (FSK) digital modulations. Many analyzers provide Amplitude Modulation (AM) and Frequency Modulation (FM) demodulators but do not provide the actual bit decoding for the digital versions of these modulations. The RTSA has three popular bit decoding schemes built in: NRZ-L, Manchester and Miller. This enables the instrument to decode ASK or FSK modulations to the channel bit level for easy analysis.

Once a modulation is demodulated and decoded, the recovered bits or symbols can be saved to a BINary (BIN), OCTal (OCT) or HEXadecimal (HEX) file for subsequent decryption and analysis.

Using IEEE-488 commands, the entire process of information collection can be automated and accessed through a LAN or Internet connection. This allows a remotely placed instrument to trigger on key signals, capture the RF waveforms, demodulate them, decode the data and save the recovered information for analysis.

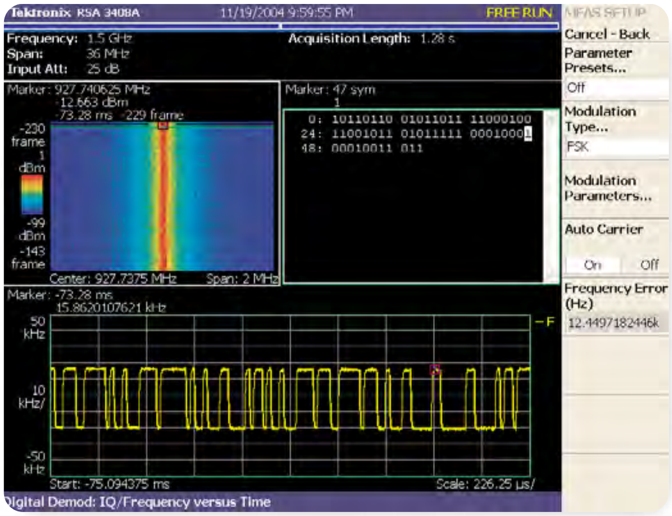
The RSA3408A's 36 MHz of instantaneous bandwidth is sufficient to handle popular broadband signals such as WLAN. WLAN standards such as IEEE 802.11a/b/g are captured and analyzed at the touch of a button. The RSA3408A's software can automatically detect the type of WLAN signal and set up the instrument appropriately. Many WLAN devices support both the older Complimentary Code Keying (CCK) format and the newer Orthogonal Frequency Domain Modulation (OFDM) format. The RSA3408A can automatically distinguish between formats and demodulate them appropriately, even in a mixed signal burst pattern. This eliminates the need for operator intervention and provides a smooth continuous flow of intercepted data.

The RTSA's built in demodulation capability covers many of the most common signal identification and information intercept situations. In the next section, we will look at non-standard signals that are intentionally designed to be difficult to intercept.

Demodulation of LPI Signals

Depending on the transmission path constraints, the amount of data transfer required, and security desired, some signal transmissions might be designed for a low probability of interception. Though an LPI signal may also be difficult to detect (LPD), the primary focus is to prevent demodulation of the message content.

Sophisticated LPI signals often use modulation formats and coding techniques that are specialized, making intercept of their messages difficult without the appropriate demodulator.



Tektronix RSA 3408A 11/19/2004 9:59:55 PM FREE RUN

Frequency: 1.5 GHz
Span: 36 MHz
Input Att: 25 dB
Acquisition Length: 1.28 s

Marker: 927.740625 MHz
-12.663 dBm
-73.28 ms -229 frame

Marker: 47 sym
1

```
 0: 10110110 01011011 11000100
24: 11001011 01011111 00010001
48: 00010011 011
```

Center: 927.7375 MHz Span: 2 MHz

Marker: -73.28 ms
15.8620107621 kHz

Start: -75.094375 ms Scale: 226.25 µs/

Digital Demod: IQ/Frequency versus Time

Modulation Type... FSK
Parameter Presets... Off
Frequency Error (Hz) 12.4497182446k

Figure 24. *RSA3408A decoding NRZ-L channel bits from an FSK modulated 927 MHz cordless phone signal intercept. Time correlated multi-domain markers show corresponding markers on spectrogram, demodulated FM and FSK bits.*

Proprietary Modulations

Sophisticated LPI signals based on proprietary non-standard modulation techniques can present a significant challenge to the signal analyst. Unfortunately, these proprietary modulations cannot easily be anticipated so it is not possible for signal analyzer manufacturers to provide built in demodulators for them. Subsequent decrypting after demodulation can also present a significant challenge well beyond the computational power of the RTSA's internal microprocessor.

Specialized demodulators and decryption equipment are required for the sophisticated LPI signal.

The RTSA can accommodate the challenging LPI signal by functioning as a signal capture device. This allows the analyst to use the RTSA's FMT, phase noise and dynamic range performance to acquire a recording of the signal. The captured data can then be exported to a flexible software tool such as Matlab or MiDAS with the ability to demodulate and decipher challenging LPI signals.

Data Export

The RTSA allows the user access to the I-Q data samples in two ways. I-Q data records can be accessed through the LAN port on the RSA3408A or the user can gain access to the raw I-Q data coming directly from the Analog to Digital (ADC) converter via a special hardware option. Both approaches enable data export to software demodulators for more detailed analysis. The RSA3408A has the ability to export I-Q sampled data at the full bandwidth of the instrument, 36 MHz. The two methods of data access on the RSA3408A offer different benefits for LPI applications.

The Ethernet connection enables the calibrated, corrected data that is captured and stored in the analyzer to be easily exported to a wide range of computer systems. Not only are the RTSA's own .iqt files supported, but translators for ASCII are available to allow generic software access to the IQ sample data.

Using the Ethernet connection, record lengths are limited by the available memory in the RTSA. Thus downloading the captured data through the LAN port is ideal for signal bursts that fit within the instrument's maximum record length of 16 Msample IQ pairs, expandable to 65 Msample IQ pairs. The data downloaded from the instrument's memory is also calibration corrected for the RTSA's RF performance and is ready for specialized demodulation algorithms.

What does one do if the LPI modulation of interest is continuous and exceeds the instrument's memory capacity?

Tektronix has equipped the RSA3408A with an optional high-speed Low Voltage Differential Signaling (LVDS) connection that allows direct access to the output of the analog to digital converter. This special port enables the expert user to continuously access a stream of I-Q data for external demodulation. Raw data coming directly from the RTSA ADC has not yet had gain flatness, phase flatness or calibration corrections applied to it.

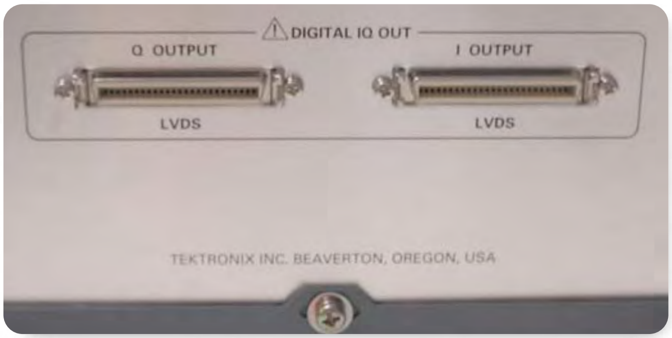


Figure 25. *Equipped with LVDS ports, extracting I-Q records continuously in real-time is easily accomplished with the RTSA.*

These correction factors normally applied in the instrument need to be applied to the raw data external to the instrument before digital demodulation. Use of this port is intended for advanced data capture applications where the user can provide and support high speed capture hardware.

The ability to access the raw high-speed data sampling of the RSA3408A provides the user with the flexibility to demodulate difficult continuous LPI signals encountered in the field.

The LVDS port on the RTSA is also useful in developing specialized signals. It is possible to test complex digital modulations without costly hardware development by using the digital output of I and Q as a substitute for an expensive receiver. Using an arbitrary waveform generator, the RTSA and a computer, an RF data link can be created with only software development. The time savings possible when creating new LPI signals or responding to the unexpected signals in the field by using reliable test equipment solutions for the RF frequency conversion and digitization portions of a data link can be significant. Eliminating the need to validate RF hardware and focus solely on software creation slashes development time. Short development times can be particularly important when urgent national security threats arise.

Working in a Secure Environment

Surveillance work dictates the handling of sensitive message intercepts or other data that requires restricted access. On occasion however, surveillance equipment requires calibration or repair by individuals not cleared for access into sensitive areas. Similarly, in the development environment, test equipment is often shared between sensitive projects with restricted access and unclassified projects with unrestricted access.

Equipment that contains data recordings of sensitive information must have that information thoroughly removed before being allowed into an unrestricted access areas or a security violation would occur. If information is accidentally left on the analyzer or incompletely removed from it, a skilled calibration technician or other "un-cleared" security risk could gain access.

Many signal analyzers pose a difficult problem to the security officer when used in a classified environment. On board flash memory and computer disks that are difficult to remove or thoroughly erase, often dictate that the equipment must remain in the restricted area for its entire service life. The costs associated with calibration and maintenance inside a classified area can be significantly higher than a non-restricted area.

The RTSA was designed to make mixed operation in secure and non-secure areas simple. A convenient hatch located on the top of the instrument allows access to the internal hard drive for quick removal.

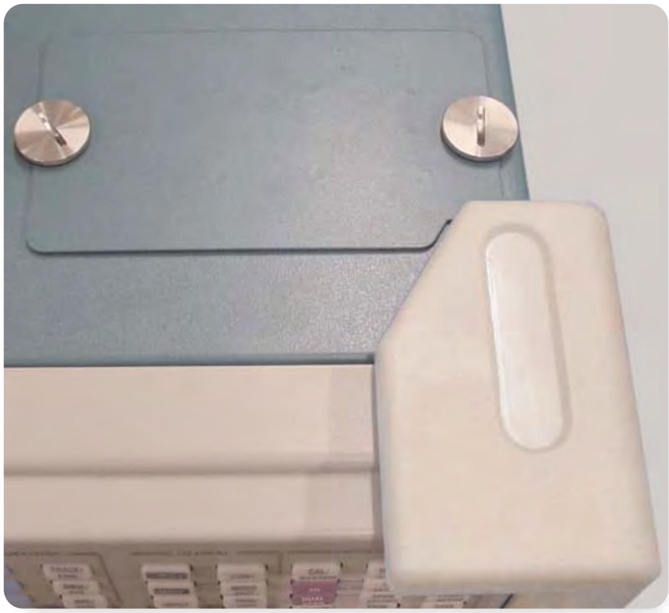


Figure 26. *The RTSA has a convenient access hatch for removing the hard drive that contains information stored on the RTSA. This allows sensitive information to be quickly removed from the instrument so the analyzer can be moved to non-secured areas.*

The instrument stores all non-volatile memory information to the hard drive. Taking out the hard drive and inserting another enables positive removal of sensitive information. Inserting a second hard drive then allows the instrument to work in an unrestricted access environment. Not only does swapping hard drives allow much better equipment utilization in mixed security environments, it can also facilitate a means to quickly dispose of sensitive information in the field should the need arise.

Summary and Conclusions

Signal monitoring and surveillance applications have grown more challenging with the exponential growth of wireless devices and communications links in recent years. The RSA3408A RTSA can be applied to signal monitoring and surveillance missions offering a host of features essential for successful operations.

The RSA3408A's wide bandwidth, good dynamic range and phase noise are essential prerequisites for many surveillance applications. Unique RTSA features such as the real-time FMT, removable hard drive, full bandwidth continuous I-Q data export capability and multi-domain analysis support for popular modulation formats can be critical elements for reliable collection and intelligence production. The real-time spectrum analyzer's patented trigger capability and optional preamplifier also offer substantial intercept advantages where difficult LPD or LPI signals are encountered.

A more detailed briefing or demonstration on how the RTSA technology can benefit your specific mission requirements can be arranged by contacting your Tektronix representative.

Contact Tektronix:

ASEAN / Australasia / Pakistan (65) 6356 3900
Austria +41 52 675 3777
Balkan, Israel, South Africa and other ISE Countries +41 52 675 3777
Belgium 07 81 60166
Brazil & South America 55 (11) 3741-8360
Canada 1 (800) 661-5625
Central East Europe, Ukraine and Baltics +41 52 675 3777
Central Europe & Greece +41 52 675 3777
Denmark +45 80 88 1401
Finland +41 52 675 3777
France & North Africa +33 (0) 1 69 86 81 81
Germany +49 (221) 94 77 400
Hong Kong (852) 2585-6688
India (91) 80-22275577
Italy +39 (02) 25086 1
Japan 81 (3) 6714-3010
Luxembourg +44 (0) 1344 392400
Mexico, Central America & Caribbean 52 (55) 56666-333
Middle East, Asia and North Africa +41 52 675 3777
The Netherlands 090 02 021797
Norway 800 16098
People"s Republic of China 86 (10) 6235 1230
Poland +41 52 675 3777
Portugal 80 08 12370
Republic of Korea 82 (2) 528-5299
Russia & CIS 7 095 775 1064
South Africa +27 11 254 8360
Spain (+34) 901 988 054
Sweden 020 08 80371
Switzerland +41 52 675 3777
Taiwan 886 (2) 2722-9622
United Kingdom & Eire +44 (0) 1344 392400
USA 1 (800) 426-2200

For other areas contact Tektronix, Inc. at: 1 (503) 627-7111

Last Updated June 15 2005

For Further Information

Tektronix maintains a comprehensive, constantly expanding collection of application notes, technical briefs and other resources to help engineers working on the cutting edge of technology. Please visit **www.tektronix.com**

8/05 DV/WOW 37W-18576-1

Tektronix
Enabling Innovation