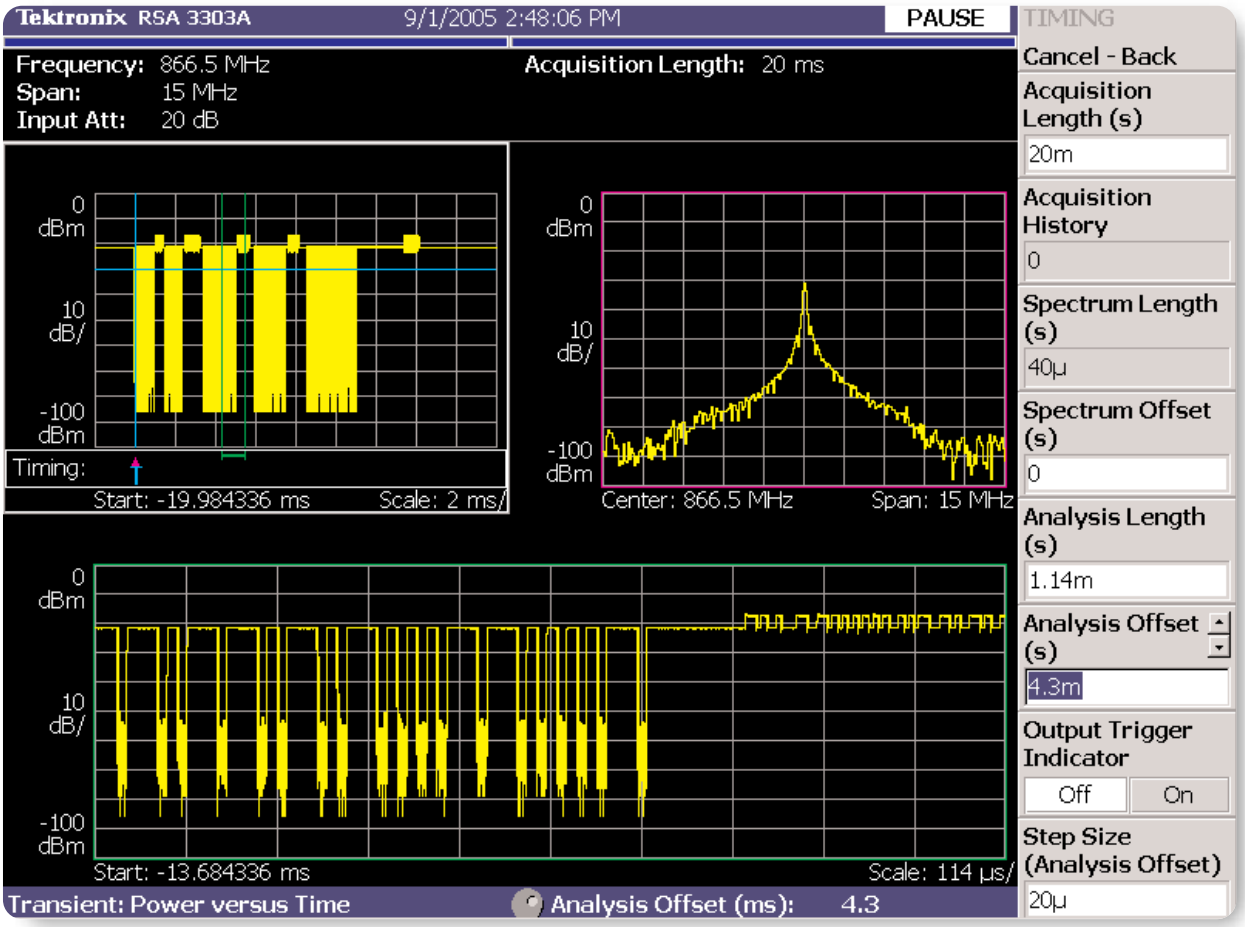
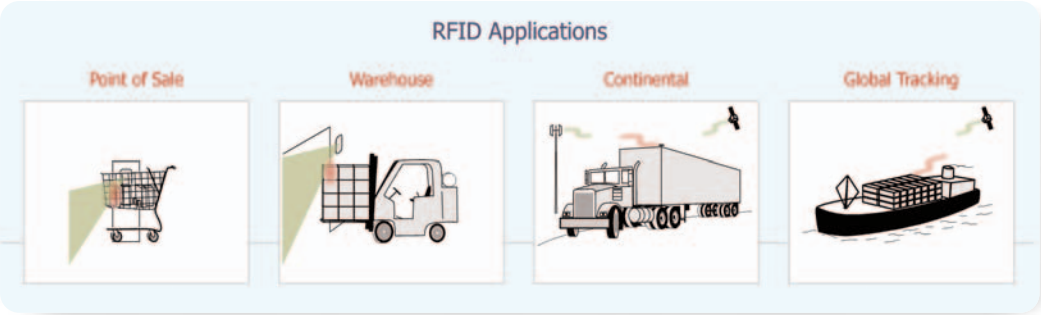
RFID and NFC Measurements with the Real-Time Spectrum Analyzer



Introduction

RFID applications are rapidly growing as equipment prices drop and global markets expand. Moreover, many short-range Near Field Communications (NFC) links using similar technology are also enjoying a period of rapid growth. RFID & NFC technologies share a variety of uncommon engineering measurement challenges. Transient signals, bandwidth inefficient modulations, backscattered data, and passive tags all require special measurement capabilities not commonly found in traditional test instruments. The Real-Time Spectrum Analyzer (RTSA) is the first analyzer to offer an RFID specific measurement package in addition to its extraordinary real-time capabilities. This combination provides an outstanding solution for RFID & NFC device characterization. The RTSA can rapidly diagnose development problems, sort out pre-compliance testing performance, and support efficient production of tags and interrogators. In this application note, we examine the challenges of RFID measurements and the RTSA's ability to provide diagnostic insight.

Tektronix
Enabling Innovation



▶ **Figure 1.** *RFID technology and data links span a tremendous range of applications. Systems have been developed for short distance point-of-sale applications, to global tracking of assets and inventory.*

RFID technology has been commercially available for over two decades, tracing its roots back to military Identification Friend or Foe (IFF) systems of the 1940s. Recent advancements in submicron Complementary Metal Oxide Semiconductors (CMOS) promise to make RFID technology ubiquitous. The lure of precision supply chain management, instant checkout transactions, and post sales marketing intelligence, is fueling rapid deployment of the technology.

We begin our discussion with an overview of RFID technology. After reviewing RFID technology, specific signal characteristics and design challenges differentiating RFID data links from other communications systems are examined. The real-time spectrum analyzer's unique capabilities as the first comprehensive RFID test instrument are then highlighted. This leads to a discussion on the specifics of how to make essential RFID measurements by applying the RTSA technology. Some tips for properly validating pre-compliance performance with the RTSA, prior to test certification at an outside laboratory are also given, followed by a brief summary and conclusion.

There are many types of RFID and NFC systems. Throughout this application note a special emphasis is placed on the RFID Electronic Product Code (EPC) formats. The EPC Gen2 format pending adoption by the International Standards Organization (ISO) as ISO 18000-6 Type C embodies many of the typical measurement challenges faced by RFID and NFC engineers. The reader is reminded that the RTSA supports many other RFID and NFC applications. The ISO 18000-6 Type C emphasis is primarily for simplified illustration purposes.

RFID Technology Overview

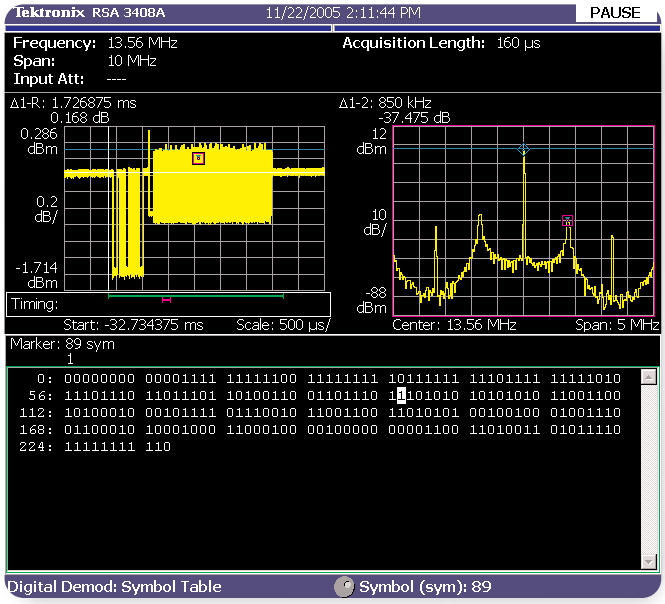
In the broadest sense RFID technology includes a wide range of systems that are used to identify objects. Electronic toll collection, implanted dog tags and product security tags are all forms of RFID systems. The RFID and NFC industries cover an incredible array of RF data links and communications techniques. RFID applications span the gamut from data links measuring a few centimeters reading passive tags powered only from the RF signal illuminating them, to battery powered tags with many meters of range. There are even RFID systems that use cell phones, GPS and satellite communications to track high value assets globally. The technology used in RFID systems is truly very diverse.

Communications technology for many of these novel asset-tracking systems has opened up new RFID opportunities outside of the inventory management segment of the industry. Indeed, the short-range data link technology used in RFID tags has also found applications in NFC systems like tire pressure measurement devices and other similar data links. NFC applications are rapidly growing too, and can also benefit from the flexible RFID measurement capabilities of the RTSA.

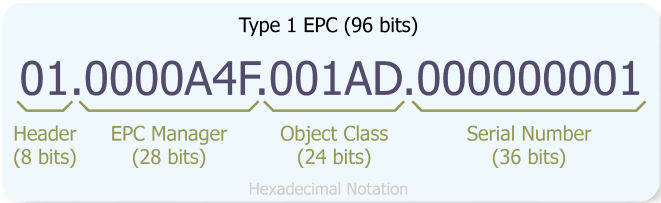
A significant portion of the RFID & NFC industries are based on proprietary signal formats for applications that are not focused on identifying products on their way to market. For example, the proximity card used to unlock doors for authorized personnel is a well-established RFID application with its own test needs. The real-time spectrum analyzer's measurement flexibility, extensive demodulation and decoding abilities easily lend it to applications such as the ISO 14443 proximity card.

Even RFID systems that operate on a global scale can benefit form the RTSA's extensive flexible support for cellular measurements and demodulation of popular satellite signal structures.

Equally important, the costs for submicron passive CMOS tags are reaching record lows. As the cost for the passive tag drops, inventory applications increase rapidly. Some estimates indicate that as the price for the passive tag continues to fall virtually every product sold will have an RFID tag in it. Some in the industry believe the EPC may be the next generation of the Universal Product Code (UPC), the familiar General Trade Identification Number (GTIN) imprinted in the barcode on a majority of products sold today.



▶ **Figure 2.** *A 13.56 MHz proximity card interchange is examined in power versus time, spectral and data symbol domains on the RTSA.*



▶ **Figure 3.** *The 96-bit EPC number identifies more than the UPC barcode. A header identifies the type of EPC number, the manager identifies the company, the object class is similar to the barcode's Stock Keeping Unit (SKU) and the serial number identifies over 68 billion unique items for each object class.*

The EPC actually contains more information than the UPC. Specifically, the EPC has product serial number information and, unlike the bar code, can be modified.

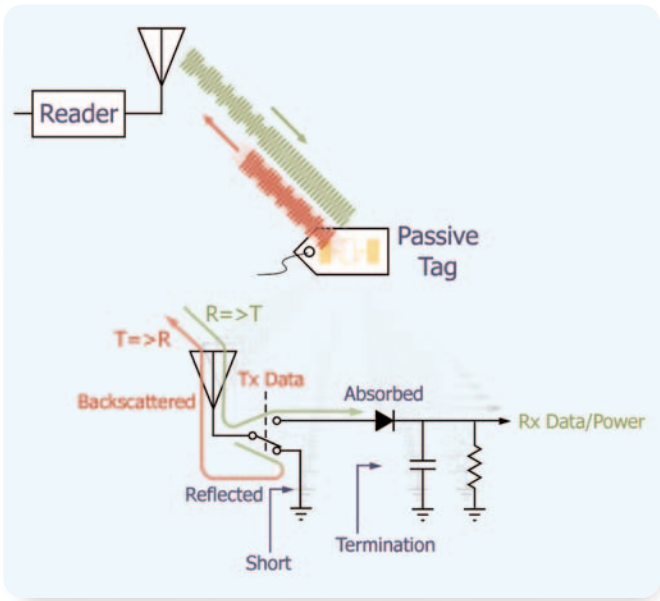
With standard formats for the EPC emerging, the cost and value begin to rival the barcode. The EPC RFID tag could rapidly become one of the most produced designs in recorded history. Virtually every product sold would need one. As tag applications rapidly expand, the possibility of the EPC replacing or augmenting large portions of UPC applications seems more and more plausible, especially as several major retailers have already mandated its early adoption.

There is more to the EPC RFID tag than a rapid check out at the cash register for the consumer. Active tags can automatically wake up periodically and measure the temperature of food products on the way to market through what is termed the 'cold chain,' ensuring food safety. Meat and dairy products will be traceable from the individual animal's history to the consumer's purchase. X-ray tag reads through other merchandise might make checkout nearly instant. Items not properly paid for and removed from the retailer's inventory can be sensed leaving the premises to activate the necessary security alarms.

The EPC's serial number feature will allow merchants to track and sell unique one-of-a-kind items, which current barcodes do not support. The inventory process is also greatly simplified with mobile tag readers passing through the store to tally shelf contents in a matter of minutes. Finally, with tags embedded inside products, a wealth of marketing intelligence is available for anyone with an interrogator seeking to intercept the information. Personal possessions can be quickly identified, providing instant consumer profiles to optimize promotional media. It will also allow invisible searches of people and vehicles for security.

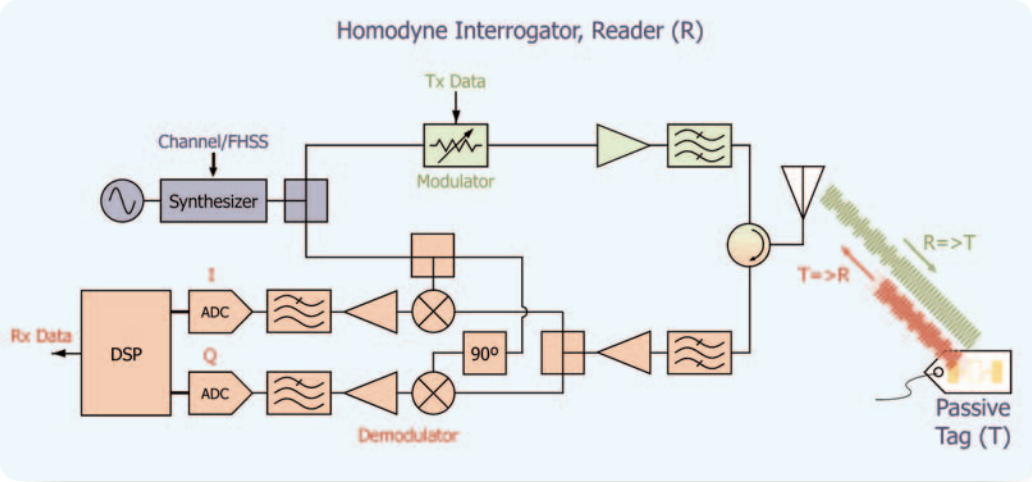
EPC Class	*Definition*	
Class 0	Read Only	Passive
Class 1	Write-Once	Passive
Class 2	Rewrite-able	Passive
Class 3	Rewrite-able	Semi-passive
Class 4	Rewrite-able	Active
Class 5	Readers	Active

▶ **Table 1.** *EPC classes are based on the device's memory properties and transmit capability.*



▶ **Figure 4.** *The passive tag backscatters the interrogator's CW carrier, modulating it by changing the absorption characteristics of the antenna. The passive tag also rectifies the RF energy to create a small amount of power to run the tag.*

The varying applications of EPC RFID tags have moved the industry to classify the basic types of RFID devices, ranging from 1 to 5 according to the tag's read/write capability and passive or active power source.



▶ **Figure 5.** *A typical homodyne interrogator or tag reader simplified block diagram. Using a precision f requency source the transmitted carrier is modulated and sent to the tag. On the reader's receive side, a single frequency conversion down to base-band of the backscattered I and Q signal gets processed into the received ID data.*

The passive class 1 tag in the 900 MHz and 2.45 GHz frequency ranges is of interest for many high volume applications. The high frequency allows the interrogator to read the tag from a greater distance. Passive tags at higher frequencies also work with smaller, less complicated antennas making them more suitable for consumer applications.

To read the tags, a 'reader' or interrogator is needed. Architecturally, reading passive tags is somewhat different than the traditional full duplex data link. Unlike traditional active data links, the passive tag relies on the RF energy it receives to power the tag. Passive tags also do not generate their own transmit carrier signal. Rather, they modulate some of the energy being transmitted by the interrogator to the tag in a process known as backscattering.

By changing the loading of the antenna from absorptive to reflective, a Continuous Wave (CW) signal from the interrogator can be modulated. This process is very similar to using a mirror and the sun to signal someone at a distance. It also eliminates the need for precision frequency sources and power hungry transmitters in the tag. Since reader and tag share the same frequency they must take turns sending information. Backscattering thus restricts communications between reader and tag to a half duplex system.

Passive tag readers are typically configured as a homodyne or single frequency conversion receiver. A precision frequency source in the interrogator generates both the transmitter signal and the local oscillator for the reader's receiver.

Since the uplink from the Tag (T) to the Reader (R) (denoted T=>R) is modulated from the interrogator's CW signal, it is possible to use spread spectrum techniques such as frequency hopping. Any spreading on the interrogator's signal will automatically be removed in the homodyne down conversion of the receiver, since it shares the same Local Oscillator (LO) signal.

After down conversion the interrogator's homodyne receiver has separated In phase (I) and Quadrature phase (Q) signals. The down-converted base-band signal is then digitized with Analog to Digital Converters (ADC) and digitally processed to determine the tag's ID.

The unique homodyne architecture of the Class 1 RFID system presents some unusual challenges for the engineer. The backscattered modulation is typically far weaker than the CW signal from the reader's transmitter used to power the tag during backscattering. At base-band in the reader's receiver, the CW leakage translates to a large DC offset that can saturate sensitive amplifiers and digitizers.

Another challenge encountered with the passive tag RFID system is the powering of the tag from received RF energy. Even though submicron CMOS requires very little power to operate, at a range of only a few meters very little power (- 10 to -15 dBm) is available. Complicating matters further, regulatory bodies worldwide have different maximum Effective Isotropic Radiated Power (EIRP) limits. The available energy to power the tag affects not only the read distance but also the time it takes to write to the tag's flash memory as higher voltages must be produced on board the tag.

The most recent standards recognize these issues and have provided improvements in modulation, encoding and protocols to help prevent power starved tags. Additionally, data rate improvements have also been made. For example, ISO 18000-6 Type A & B are limited to 160 kb/s whereas Type C can reach a speed of 640 kb/s.

RFID Standard

Application	*Standard*	*Name*
Animals Management	ISO 11784	Code Structure
	ISO 11785	Technical Concept
	ISO 14223	Expand Code Structure & Encoding
Freight Containers	ISO 10374	Automatic Identification
	ISO 18185	Electronic Seals for Security
Item Management	ISO/IEC 18000-1	Reference Architecture
	ISO/IEC 18000-2	Air Interface Below 135 kHz
	ISO/IEC 18000-3	Air Interface at 135 kHz
	ISO/IEC 18000-4	Air Interface at 2.45 GHz
	ISO/IEC 18000-6	Air Interface at 860 MHz to 960 MHz
	ISO/IEC 18000-7	Air Interface at 433 MHz
	ISO/IEC 15961	Data Protocol: Application Interface
	ISO/IEC 15962	Data Protocol: Data Encoding Rules
	ISO/IEC 15963	Unique ID
	TR 18001	Application Requirements
	TR 18046	Performance Test Method
	TR 18047	Conformance Test Method
Identification	ISO/IEC 14443-1	Physical Characteristics
"Proximity" Card	ISO/IEC 14443-2	Radio Frequency & Power
(mm to cm's)	ISO/IEC 14443-3	Initialization & Anti-collision
	ISO/IEC 14443-4	Transmission Protocol
Identification	ISO/IEC 15693-1	Physical Characteristics
"Vicinity" Card	ISO/IEC 15693-2	Air Interface & Initialization
(cm's to 0.7 m)	ISO/IEC 15693-3	Anti-Collision & Protocol
Near Field	ISO/IEC 18092	Near Field Communication
Communication		Interface & Protocol

▶ **Table 2.** *Many international RFID standards like these from ISO/IEC exist to help assure compatibility between systems and vendors.*

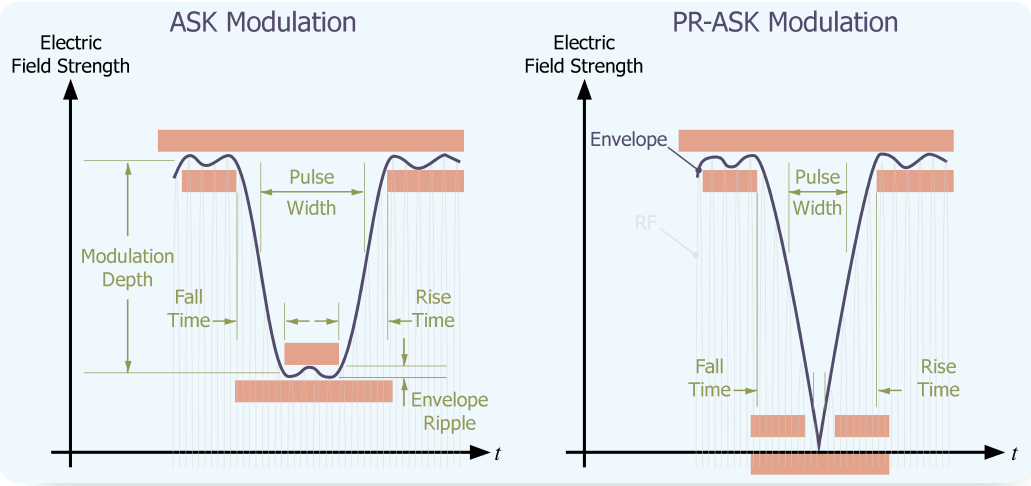
The many international RFID standards available for different applications are occasionally revised or supplemented to enhance performance and market potential. As markets grow, the spectral congestion of the available bands also becomes a concern.

Regulatory emission requirements vary worldwide for RFID readers. In some countries lots of channels are available for RFID applications. In North America, 50 channels are available in the 902 to 928 MHz frequency range, enough for the Gen2 standard to employ Frequency Hop Spread Spectrum (FHSS) capability. However in Europe only 10 channels are available in the 866-869 MHz band. Frequency congestion in Japan's 952-954 MHz band has many Japanese producers opting to work at 2.4 GHz with the ISO 18000-4 standard instead.

In numerous countries, the regulatory laws are changing to catch up with the unique data link characteristics of the passive RFID tag. Most spectral regulators prohibit CW transmissions from devices unless it is for a short-term test. Passive tags require a CW signal to modulate. Even though passive tags don't have a typical transmitter in them, they still produce a modulated signal from their backscattering. However, regulatory laws are not written for modulating devices without a transmitter.

Worldwide RFID standards often simply state that "An interrogator's choice of operational frequency will be determined by local radio regulations and by the local radio-frequency environment," leaving it to the manufacturer to comply with a vast array of local emission requirements in the regions where they expect to sell their product. Thus a variety of spectral emission tests, which may not be explicitly contained in the RFID standard for the interrogator, become requirements.

The broadband nature of the passive RFID tag also presents some challenges for dense (multiple) reader sites. Since the interrogator sets the system's frequency of operation and the tag is a broadband device that responds to any interrogator the antenna can receive, with multiple interrogators the tag has limited ability to respond to a specific reader. Passive tags may try to respond to all readers that are interrogating them. Synchronization techniques of multiple readers can be used to improve a dense multiple reader installation's throughput.



▶ **Figure 6.** *ASK modulation depth, rise time and fall time are typically specified to ensure readers can properly power tags and interpret data symbols.*

RFID systems usually employ modulation techniques and coding schemes that are simple to produce. For example, ISO 18000 Type C (also known as EPC Gen2, Class 1) calls for Double Side Band-Amplitude Shift Keying (DSB-ASK), Single Side Band-ASK (SSB-ASK) and Phase Reversal-ASK (PR-ASK).

Amplitude shift keyed digital modulations are spectrally inefficient, requiring substantial RF bandwidth for a given data rate. Bandwidth efficiencies of 0.20 bits per Hertz of RF bandwidth are not uncommon for DSB-ASK.

One approach to improving bandwidth efficiency is to use SSB-ASK. This is particularly important in European countries where bandwidth restrictions may preclude DSB-ASK.

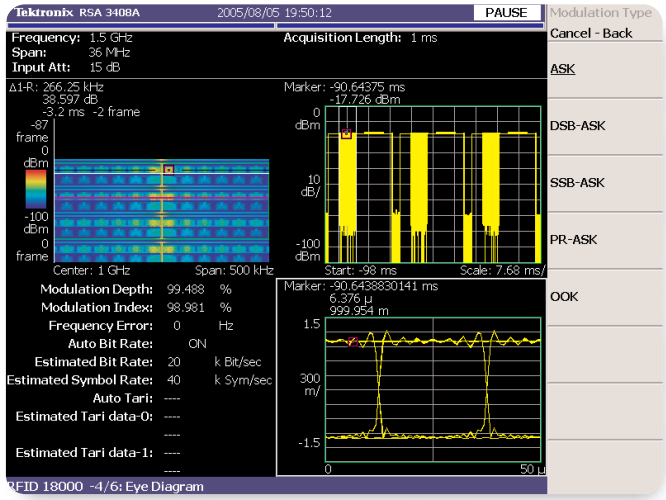
The power efficiency of DSB-ASK and SSB-ASK is dependent on the modulation index. With a modulation index of one, or On and Off Keying (OOK) of the carrier, the lowest Carrier to Noise (C/N) required to achieve a given Bit Error Rate (BER) is obtained for DSB-ASK and SSB-ASK. Unfortunately, this also provides the least amount of RF power transport on the downlink to supply the tag with energy.

Ideally, the off time of the carrier should be minimized so that the tag doesn't run out of power. The carrier to noise requirements should also be minimized to maximize ID read range. For many modulations, these are conflicting goals.

One such modulation that can minimize the carrier to noise requirement in a narrowband while maximizing the power transport to the tag is PR-ASK. Similar to a Phase Shift Keyed (PSK) signal, PR-ASK changes phase 180° each time a symbol is sent. PR-ASK also creates an amplitude modulation depth of 100% or a modulation index of one as the phase vector of the old symbol and the new symbol cross and briefly sum to a zero magnitude. This provides an easily detected clock signal as the amplitude briefly goes to zero, but minimizes the time the carrier power is off, so power transport to the passive tag is optimized. PR-ASK has carrier to noise and bandwidth requirements more closely matching PSK than DSB-ASK, making it attractive for narrowband and longer-range applications.

DSB-ASK is the least bandwidth efficient modulation, but the easiest to produce by On and Off Keying (OOK) of the carrier signal. ASK modulation specifications often have a modulation depth as well as rise and fall time requirements. The rise and fall time is typically related to the bandwidth filtering while the modulation depth is set by the attenuation difference between the keying states.

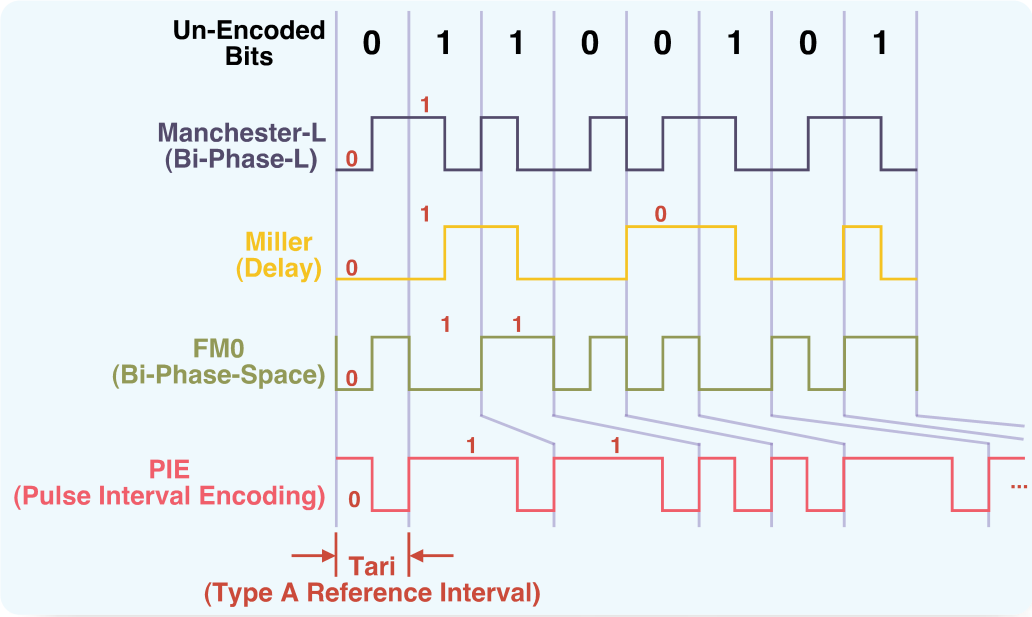
Before modulation, the data must be encoded into a serial information stream. There are many types of bit encoding schemes available, each with unique advantages in their base-band spectral properties, complexity to encode/decode and difficulty to clock into memory.



▶ **Figure 7.** *The real-time spectrum analyzer can easily measure modulation depth or index for popular RFID modulations. In this screen capture, symbol eye-patterns are viewed with the spectrogram and power versus time displays.*

Passive RFID tags place unique requirements on the coding schemes used. The impracticality of precision timing sources on board the passive tag, challenging bandwidth requirements and the need for maximum RF power transport to energize the tag, make data encoding critical for many RFID applications.

Manchester (Bi-Phase-L) and Pulse Interval Encoding (PIE) are popular for interrogator to tag (R=>T) communications. An important characteristic of these coding schemes is that they are based on transitions and are self-clocking, greatly reducing the complexity of the synchronization circuitry required in the power-starved tag.



▶ **Figure 8.** *RFID systems use a variety of PCM bit coding schemes. Important considerations are synchronization complexity in the tag as well as low frequency DC spectral energy for backscattering.*

PIE encoding is based on a given minimum pulse duration or interval such as 20 Ìs. This period is called a 'Tari,' and is named after the ISO 18000-6 Type A Reference Interval (Tari). One and zero bits as well as special symbols like Start Of Frame (SOF) and End Of Frame (EOF) are composed of differing numbers of tari periods. This makes the transmission length for a given number of bits variable. Since PIE encoding is self-clocking the variable length has little effect.

The Tari length is also the minimum pulse width for the modulated signal, an important factor in determining the bandwidth of the transmitted signal. The shorter the Tari length, the greater the bandwidth requirement will be for the signal. More recent standards such as the ISO 18000-6, Type C allow for several Tari lengths (6.25, 12 & 25 Ìs) to accommodate differing regulatory spectral emission requirements worldwide.

Another important property for RFID Pulse Code Modulation (PCM) coding schemes is their DC spectral component. Backscattering tags modulate a carrier signal. The carrier signal is then filtered out as a baseband DC level back in the tag reader, leaving only the much weaker uplink modulation from the tag. Coding schemes in the tag require the uplink to the reader to have little or no DC energy to conflict with the carrier signal.

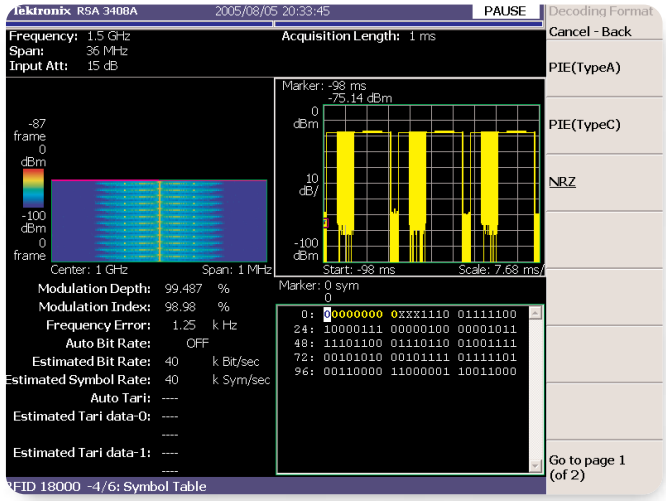
Miller and FM0 encoding share this property of little or no DC energy in their spectrums. ISO 18000-6 Type C further enhances the Miller encoding by offering different sub-carrier rates. One, two, four and eight times the sub-carrier frequency enable adjustment of the modulation encoding to optimize read range, speed or bandwidth.

Most signal analyzers used for troubleshooting ASK modulations have no ability to decode these analog PCM waveforms into symbols or bits. The real-time spectrum analyzer with its RFID software option supports the decoding of analog RFID waveforms into the bits they represent. This can be particularly helpful for diagnosing issues with circuits or the environment the RFID system is installed in.

Amplitude-based modulations used in many RFID systems are susceptible to rapid signal fading conditions. Moving forklifts with pallets full of tags traveling by readers located in between metal trucks and warehouse structures, can undergo devastating multi-path conditions. Rapid Rayleigh fading or shadowing can be indistinguishable from amplitude modulation, causing bit errors.

The RTSA's ability to see both the analog waveform in the power versus time display as well as the symbols interpreted from the waveform help the engineer gain insight into why a given symbol is incorrect. Analyzers without this ability require the engineer to manually decode waveforms that can be 96 or more bits long.

With both analog waveform and decoded symbols, the process of determining the effect of noise or interference on the communicated data is greatly simplified. Often during diagnostic testing, received waveforms have substantial noise and interference on them. In many cases it can be difficult to tell just what effect the signal impairments are likely to have on the data. With the analyzer decoding the symbols the data payload can be examined on a test instrument known to be accurate. This allows the RFID engineer to easily sort out insignificant impairments from those that create serious data errors.



▶ **Figure 9.** *The RTSA's RFID analysis software features symbol decoding for popular interrogator and tag PCM encoding schemes.*

Another RFID consideration occurs when an interrogator queries the tags near it, as more than one tag may be in a position to respond. Some form of anti-collision protocol is required to enable reading of all the tags in the interrogator's field of view. There are two basic types of anti-collision protocols, deterministic and probabilistic. Popular RFID protocols are the deterministic binary tree and the probabilistic ALOHA and slotted ALOHA approaches.

The binary tree method searches for tag IDs that fit a specific binary number. For example, all tags that begin with the binary 1 respond, then all tags with a second digit of 0, until each tag is addressed and recorded. If a collision occurs, additional digits are added to the search for that part of the decision tree. Binary tree protocols can be slow to search the entire tree for tag IDs.

The probabilistic ALOHA protocol (developed at the University of Hawaii) allows the tag to send its message and if the message doesn't get through, it simply tries again later until it does. The slotted ALOHA approach uses synchronization between all the tags, so communications packets are not interrupted mid-stream in the transmission. Slotted ALOHA is about 30% efficient with the use of the available bandwidth while straight ALOHA is only about 18% efficient. The ALOHA protocols are relatively quick in sorting through large numbers of tags.

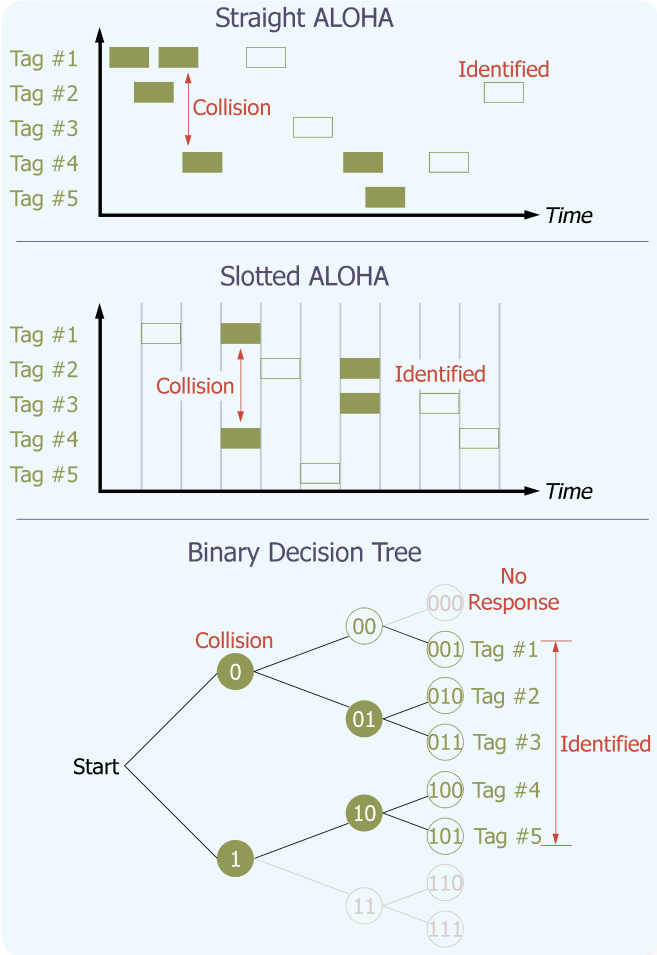
Additional efficiency gains are possible by using Listen Before Talk (LBT) schemes. With LBT, the interrogator listens to the channel to make sure it is clear and doesn't interrupt a transmission already in progress.

Standards like the ISO 18000-6 have evolved through a variety of protocols. Initially ISO 18000-6 Type A used the ALOHA protocol. Then, with the adoption of ISO 18000-6 Type B, the binary tree protocol was used. Most recently, ISO 18000-6 Type C now calls for the slotted ALOHA protocol, giving it faster throughput.

The Gen2 standard also unifies several previous UHF standards and provides the flexibility to enhance performance while meeting the rigors of worldwide deployment.

The Gen2 standard offers 4 different communications speeds, allowing each installation to take better advantage of the maximum throughput offered in the communications channel for each installation, while accommodating differing national regulatory limitations.

The 'Q' protocol containing the slotted ALOHA scheme has been further optimized from earlier standards to more robustly read tags that are marginally accessible in the reader's RF field of view. Protocol interchanges have been shortened in duration to make sure tags receive



▶ **Figure 10.** *Popular protocols that arbitrate collisions between simultaneous transmissions back from multiple tags include ALOHA, slotted ALOHA and the Binary Decision Tree.*

enough RF energy that they don't run out of power during the interchange. A special parameter 'Q' has been set up to control the likelihood a tag will respond to the reader. Gen2 tags also have the ability to be put to sleep after being read, minimizing collisions to speed the reading of the remaining tags.

The ISO 18000-6 Type C standard also addresses the disparity between downlink and uplink power levels in dense reader deployments. Multiple readers deployed in close proximity can easily interfere with each other. The downlink power level generated in the power amplifier can be as high as +37 dBm in the United States, allowing passive tags to receive a usable level greater than -15 dBm of transported RF power at about 4 meters. The backscattered uplink from the tag can be as low as -63 dBm, far below the interrogator's downlink power level. In dense deployments other tag readers can easily drown out the weak backscattered signals.

In the United States where bandwidth is more plentiful, frequency hop spread spectrum techniques enable many readers to function in close proximity.

In Japan and European countries, UHF bandwidth is scarce, so ISO 18000-6 Type C specification helps alleviate the congestion by allowing multiple readers to synchronize their interrogations. Schemes like 'listen before talk' to avoid channels already in use or the use of one of four different sub-carrier encoding rates (FM0, Miller M=2, M=4 & M=8) to vary the channel widths improves the reader's ability to work in congested, noisy or interference-prone environments. The latest specifications have also improved security and extensibility to future standards.

Now that we have reviewed RFID technology, issues and standards, let's look at some important test considerations.

RFID Testing Overview

RFID systems, particularly those with backscattering passive tags, present some unique challenges for test and diagnostics.

Timing measurements are of particular concern, as system readers can be required to read the ID data from many tags very quickly without error.

Most RFID systems use transient Time Division Duplexing (TDD) schemes, where the interrogator and tags take turns communicating on the same channel. To read many ID tags within a very short period of time with a serial TDD multiplexing scheme, the standards call for very precise timing. Timing measurements on the data interchange thus present a unique RFID challenge.

The transient RFID signals often contain spectrally inefficient modulations using special PCM symbol encoding and decoding. Troubleshooting the homodyne interrogators or tags that receive these unusual signals requires special signal analyzer capabilities.

Traditionally, swept tuned spectrum analyzers, vector signal analyzers and oscilloscopes have been used for wireless data link development. The limitations of these instruments make their application to modern RFID product development and production inefficient at best.

The spectrum analyzer has historically been the tool of choice to characterize the RF spectral output of a transmitter to ensure compliance with regulatory emission restrictions. The traditional swept tuned spectrum analyzer was developed primarily for the analysis of continuous signals, not the intermittent RF transients associated with modern RFID products. This can lead to a variety of measurement issues, particularly the accurate capture and characterization of transient RF signals.

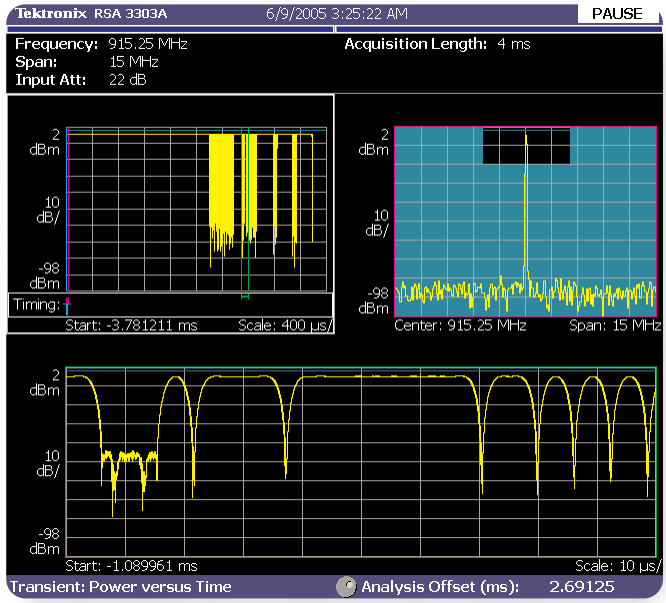
Similarly, the vector signal analyzer possesses little ability to capture transient RF signals, also being initially developed for CW signals. Though most vector signal analyzers have extensive demodulation ability for popular spectrally efficient modulations, current offerings have virtually nothing to support the spectrally inefficient RFID modulations and their special PCM decoding requirements. This makes the current generation of vector signal analyzers of little value to the RFID engineer.

The oscilloscope has long been a valuable tool for analysis of base-band signals. In recent years some oscilloscopes have extended their sampling speed to very high microwave frequencies. They are, however, still sub optimal tools for UHF or higher frequency measurements on RFID systems. Relative to the modern real-time spectrum analyzer the fast oscilloscope has substantially less measurement dynamic range and lacks modulation and decoding capability.

The real-time spectrum analyzer solves the limitations of the traditional measurement tools to provide a substantially more efficient test and diagnostic experience for the RFID engineer.

Pulsed tag reads and writes require an RF analyzer optimized for transient signals. The Tektronix real-time spectrum analyzer product family excels at characterizing transient signals with its unique real-time architecture and time correlated displays.

The RTSA has the digital processing speed necessary to transform the input signal from time domain samples into the frequency domain with a real-time Fast Fourier Transform (FFT) prior to capturing a recording of data. This enables the RTSA to compare spectral amplitudes



▶ **Figure 11.** *The RTSA's Frequency Mask Trigger and deep memory can capture complete interrogator/tag interactions. Setting a narrow mask around the desired carrier allows the RTSA to ignore nearby intermittent signals that are larger in amplitude and make IF level triggering useless.*

to a frequency mask set by the user in real-time. The RTSA can then trigger a capture on a spectral event of interest for subsequent detailed off-line analysis.

This is an important capability for RFID applications as it allows the engineer to begin a capture of the entire transient interrogator and tag interaction starting with the initial spectral burst. Furthermore, the Tektronix patented Frequency Mask Trigger (FMT) enables reliable capture of interrogator and tag interactions in complex real-world spectral environments where other signals might actually be larger in amplitude.

The RSA3408A has sufficient memory capability combined with its precision triggering ability to capture the entire exchange between reader and tag. System interactions can then be quickly diagnosed with a complete data record.

The real-time spectrum analyzer's extensive use of time correlated multi-domain analysis enables the user to display multiple measurement domains with precise time correlated markers between displays. For example, a marker can be placed on a symbol bit that is in error and the instrument will correlate this marker with the instant corresponding to the power versus time display or spectrogram.

Time correlated analysis domains greatly enhance diagnostic insight and reliability by providing positive confirmation of the anomaly responsible for an event in different displays.

In addition to the RTSA's outstanding ability to trigger and capture transient RFID signals, it offers the test and measurement industry's first RFID analysis package. This gives the RSA3408A the capability to demodulate, decode and measure the special signals used in many RFID applications.

The modern RSA3408A can provide a far faster and more efficient diagnostic and characterization experience than traditional test equipment for RFID applications. To illustrate the utility of the RTSA, next we examine some common RFID measurements…

RFID Measurements

The RFID engineer faces a variety of design challenges to bring a product to market. First, the product must meet local frequency regulations to emit energy into the spectrum. Next, the interrogator and tag interaction must reliably work together. To accomplish this, both the interrogator and tag must comply with the appropriate industry standard. Finally, to be competitive, the RFID system's performance must be optimized to appeal to a particular market segment. This could mean maximizing the number of transactions per second, operating in a dense reader environment or stretching the reader's ability to communicate over longer distances.

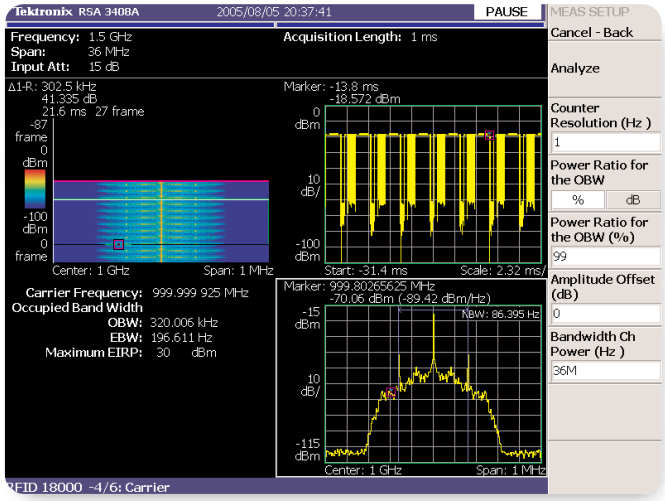
To show how the RTSA and the RFID analysis software are becoming an indispensable part of RFID testing, we begin with the key measurements necessary to characterize spectral emissions for government regulatory compliance.

Adherence to Government Regulations

Government regulations require that transmitted signals be controlled in power, frequency and bandwidth. These regulations prevent harmful interference and ensure each transmitter is a spectrally good neighbor to other users of the band. The RSA3408A with its RFID software can easily measure the spectral parameters government regulators insist upon.

Power measurements of pulsed signals can be challenging for many spectrum analyzers. The RTSA's transient signal optimization makes measurement of the power in a pulsed RFID packet transmission simple. The FFT analysis presents a complete spectral frame for any given period of time during the packet transmission. This eliminates the need to synchronize tuning sweeps with packet bursts, suffered by older swept tuned spectrum analyzers. Also, unlike traditional spectrum analyzers, where correction factors are needed to compensate for Successive Log Video Amplifier (SLVA) peak detection circuits, the RTSA uses a true RMS detection approach that accurately reads power for most regulatory measurements.

Another important spectral emission measurement is the carrier frequency of the signal. There are two ways this measurement can be expressed: actual absolute carrier frequency or carrier frequency error from a given assigned channel frequency. The RTSA will display carrier frequency error when demodulating a signal. In spectrum analysis mode, the absolute carrier frequency can be displayed by selecting the measurement button, followed by the carrier frequency soft key.



▶ **Figure 12.** *Key regulatory spectral measurements can be made quickly by displaying the spectrum and choosing the OBW/EBW measurements. Carrier Frequency, OBW/EBW and EIRP, assuming an omni-directional antenna, are also given.*

One notable advantage of the demodulated carrier frequency measurement is it doesn't require the signal to be positioned at the center of the span. This can be very useful for frequency hopping signals.

Similarly, the Occupied BandWidth (OBW) measurement or the Emission BandWidth (EBW) can be obtained in two ways. In the demodulation mode the RTSA displays the OBW and EBW as well as the carrier frequency and transmission power levels. The bandwidth measurements are also available in the real-time spectrum analyzer mode under the measurement key.

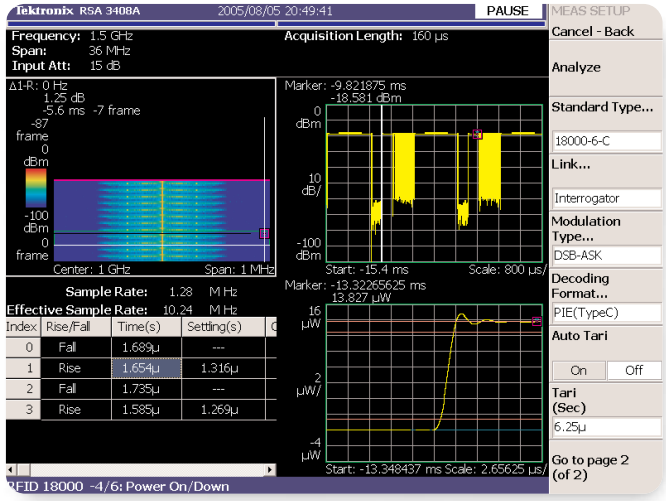
Using these preprogrammed automatic measurements essential regulatory data can be quickly and accurately obtained. This eliminates the drudgery of attempting to coax a traditional spectrum analyzer into making measurements on a transient RFID signal. The RTSA recognizes the modulation and provides the answer at the push of a button.

Meeting Industry Standards

Reliable interrogator and tag interaction requires conformance to industry standards such as the ISO 18000-6 Type C specifications. This adds many tests beyond those essential to meet government spectral emissions requirements. RF conformance tests are critical to assure reliable interoperability amongst tags and readers.

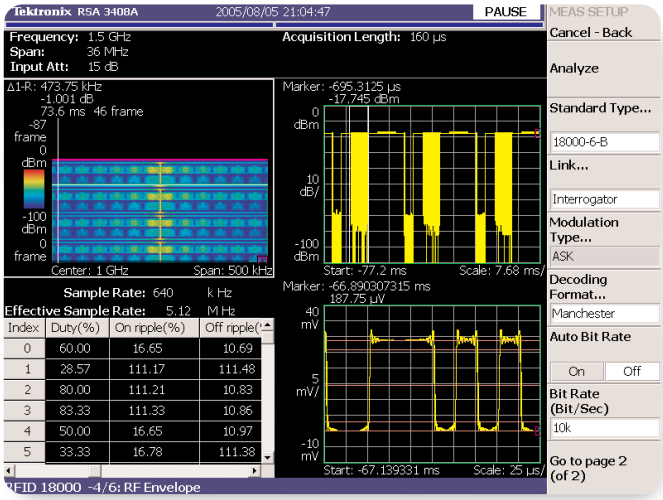
The RSA3408A's RFID software contains key measurements needed for the ISO 18000-4 Mode 1 and ISO 18000-6 Type A, B and C standards. Preprogrammed measurements on the RTSA eliminate most of the setup time required to check out these signal formats.

For example, one important measurement for ISO 18000-6 Type C is the power on and power down time. The rise time of carrier energy must be turned on promptly to ensure the tag collects enough energy to function properly. The signal must also settle out to a stable level. At the end of the transmission the fall time of the signal burst must be quick enough to avoid disrupting other transmissions.



▶ **Figure 13.** *Power on and down measurements for query session can be tested at the touch of a button with the RTSA to determine compliance with the industry standards.*

In the demodulation mode with the appropriate RFID standard and Type selected, depress the analyzer's soft key and choose Power On/Down. The RTSA will then automatically measure power on rise time, power off fall time, power settling time, overshoot and undershoot. For a more detailed perspective, the RTSA also displays the waveform characteristics in the measurement window.

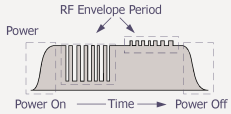


▶ **Figure 14.** *The RFID measurement software measures essential compliance specifications like on and off ripple, duty cycle and pulse widths for the RF envelope.*

Communications between interrogator and tag are accomplished with ASK signal bursts during the power on period. These signal bursts make up the RF envelope and are important for interoperability. The modulation pulse envelope contains characteristics necessary to assure compatibility between reader and tag. The RTSA's RFID software automatically measures RF envelope specifications like on width, off width, duty cycle, on ripple, off ripple and the slopes of the RF envelope edges.

The RSA3408A can characterize a variety of modulation envelopes including DSB-ASK, SSB-ASK and PR-ASK. To simplify keeping track of protocol transmissions, the RFID software labels individual bursts with an index number. The analyzer further subdivides bursts into envelope numbers to show individual symbol parameters in the detail display.

Option 21 RFID Standard Measurements



Menu	Measurement	Standard: ISO18000-4, Mode1	ISO18000-6, Type A	ISO18000-6, Type B	ISO18000-6, Type C
Carrier	Carrier Frequency	✔	✔	✔	✔
	OBW/EBW	✔	✔	✔	✔
	Ave. Power for Pwr. On	✔	✔	✔	✔
Spurious	Spurious	✔	✔	✔	✔
ACPR	ACPR	✔	✔	✔	✔
Power On/Down	Transmission Power	✔	✔	✔	✔
	Rise & Fall Time	✔	✔	✔	✔
	Settling Time	✔	✔	✔	✔
	Over/Under Shoot	✔	✔	✔	✔
	Off Level	✔	✔	✔	✔
RF Envelope	On/Off Width	✔	✔	✔	✔
	Duty Cycle (%)	✔	✔	✔	✔
	On/Off Ripple	✔	✔	✔	✔
	Rise Time	✔	✔	✔	✔
	Fall Time	✔	✔	✔	✔
Constellation	Modulation Depth	✔	✔	✔	✔
Eye Diagram	Modulation Index	✔	✔	✔	✔
Symbol Table	Frequency Error	✔	✔	✔	✔
	Bit Rate (Measured)	✔	✔	✔	✔
	Tari Length (0 & 1)	✔	✔	✔	✔
	Indicate Preamble	✔	✔	✔	✔
Marker	Turn Around Time	✔	✔	✔	✔

▶ **Table 3.** *Option 21 includes many preset measurements that can greatly reduce instrument setup time improving efficiency when working with internationally recognized standards.*

Testing Proprietary Communication Schemes

Many RFID and NFC devices use proprietary communications schemes that are optimized for specific market applications. The RTSA offers a variety of flexible modulation measurements that enable testing of the proprietary system with manually configured measurements.

The instrument allows a user to define the modulation type, decoding format and data rate. The frequency can be set to test systems including the Low Frequency (LF) band (125 kHz – 135 kHz), High Frequency (HF) band (13.56 MHz), Ultra High Frequency (UHF) band (868 – 928 MHz), and even S band microwave (2.45 GHz).

For example, a user can manually set the RTSA to test compliance of the NFC devices that adhere to ISO 18092, as well as testing interoperability with devices conforming to ISO 14443, Type A and Type B. The user simply sets the RTSA's frequency to 13.56 MHz, modulation type to ASK or BPSK (Type B card/target) decoding format to Modified Miller, Manchester or NRZ and the data rate to 106, 212, or 424 Kb/s.

The extensive general-purpose modulation measurement capability of the RSA3408A supports many modulation types with data rates as high as 51.2 Mbps. Additionally several bit decoding schemes are supported, making it an ideal tool for the proprietary RFID or NFC system.

Modulation		***Decoding***
ASK	GFSK	Manchester
DSB-ASK	BPSK	Miller
SSB-ASK	QPSK	Miller (M-2, M-4 & M-8)
PR-ASK	1/4 πQPSK	Modified Miller
OOK	OQPSK	FM0
FSK	8PSK	PIE (Type A or C)
GMSK	16 – 256 QAM	NRZ-L

▶ **Table 4.** *The RTSA supports a wide variety of proprietary RFID or NFC applications with extensive modulation and decoding options that are configurable. Decoding options vary based on the modulation type, with popular combinations supported on the RTSA.*

Gaining a Competitive Edge

Once the basic specifications are met, it is important to optimize some of the RFID product's features to gain a competitive advantage in a particular market segment. The RTSA can be extremely valuable in maximizing system performance while at the same time minimizing the engineering commitment necessary to achieve the desired goal.

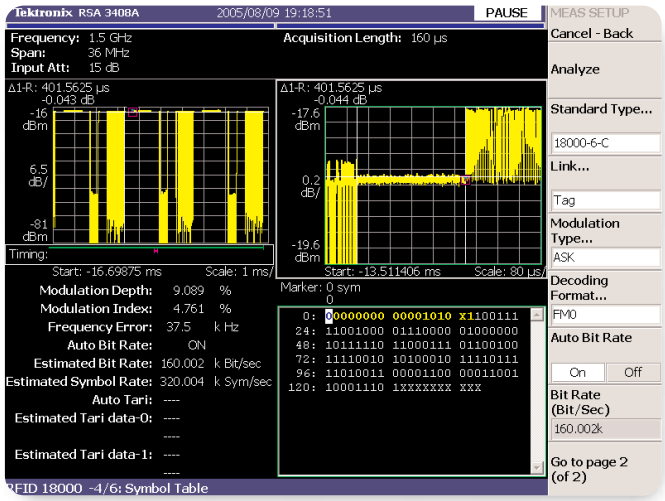
One such example is optimizing the number of tag reads possible in a given amount of time. This can increase the overall system capacity, making it more appealing to lucrative high volume applications. An important element in maximizing capacity is minimizing the Turn Around Time (TAT) for each tag reply. Available RF power, path fading and altered symbol rates can lengthen the time it takes for the tag to reply to the interrogator's query. The slower the reply, the longer it will take to read many tags.

The ability to quickly measure the turn around time for a half duplex system is essential to optimizing performance. The RTSA makes it easy to measure the TAT.

First, the entire query between the interrogator and a tag is captured into the analyzer. In the demodulation mode with symbol table chosen, under the view define window, the user sets the RTSA to a power versus time display in the sub window. Next, using the view select and scale keys, the sub window is zoomed into the portion of the waveform where the tag is backscattering.

Convention dictates that the period between the end of one downlink transmission (R=>T) to the beginning of the next downlink transmission is the turn around time or TAT for a half duplex system. Thus by placing a marker at the end of the tag interrogation and a second delta marker at the end of the backscattering or beginning of the next interrogator data transmission, a precise measurement of turn around time can be made. Maintaining the shortest TAT for the widest range of downlink conditions helps maximize the system's throughput.

The RTSA also has the ability to demodulate the symbols or bits associated with the tag query. The user merely selects the appropriate RFID standard, modulation type and decoding format. The analyzer can automatically detect and display the link's bit rate. To further enhance the engineer's productivity, the recovered data symbols are color-coded based on function. The RTSA automatically recognizes the preamble and colors those symbols yellow. This makes the actual data payload easily recognizable for comparison to the known values.



▶ **Figure 15.** *The turn around time of the RFID link can be easily measured with the RTSA's markers. In this screen capture the data symbols or bits returned from the tag's backscattering are decoded. Preamble symbols are automatically shown in yellow.*

Optimizing communications often requires extensive diagnostic work to correct problems that might be robbing the system of performance. Many traditional signal analyzers cannot easily provide the diagnostic insight necessary to troubleshoot complex RFID systems. Without the RTSA's state of the art frequency mask triggering capability to reliably capture important spectrums, comprehensive ASK demodulation and specialized RFID symbol decoding, engineering productivity on the bench can slow to a unacceptable pace. This is a recipe for disaster in the fast moving RFID industry.

The real-time spectrum analyzer's time correlated multi-domain displays mean that multiple displays can be viewed at once with time correlation between markers in each display. Time correlated multi-domain displays are particularly useful for troubleshooting and diagnostic work.

A marker placed on an anomaly in a spectrogram will correlate to a marker on the exact symbol that corresponds to the event. Time correlated displays take the guesswork out of diagnostic analysis and greatly improve the reliability of problem insight. The engineer doesn't have to assume a power versus time glitch is causing a data error, because the time correlated markers verify the two events occurred simultaneously.

These capabilities make the RSA3408A uniquely suited to solving today's RFID problems. Unlike older analyzer types, like the swept tuned spectrum analyzer or vector signal analyzer designed for an entirely different era of communications equipment, the modern RTSA provides a solution to rapidly getting an RFID system up and working at a competitive pace.

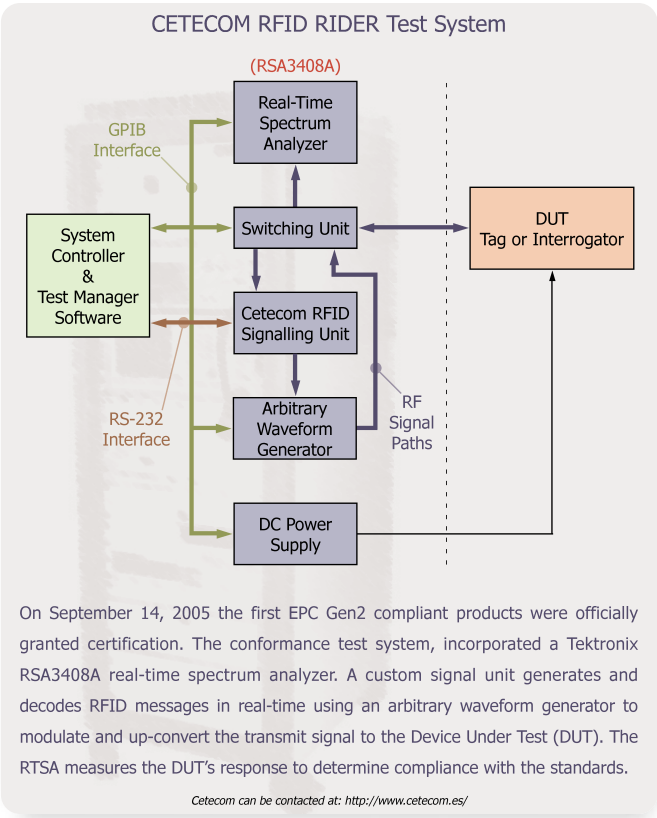
Once the RFID system is performing correctly, the next step is often preparing it for compliance certification before market introduction. In the next section we look at how the RTSA is applied to pre-compliance testing to ensure a successful certification experience.

Pre-Compliance Testing with the RTSA

Many industry standards require compliance certification in order to display the trademark that assures performance compatibility. Such stamps of approval are very important to prospective customers, providing some independent assurance the system will function correctly with a variety of readers and tags from different vendors.

Compliance testing is much like any impartial objective test. Come prepared and it is an exciting rewarding experience. Come ill prepared and it probably won't be much fun. Unfortunately, in the fast moving RFID industry, the greatest cost of being ill prepared for compliance certification is usually the opportunity cost in getting the product to market. Failing a compliance certification test and having to reschedule another test can mean many weeks of lost revenue from a late product introduction.

The time to market and lost sales revenue can be very dependent on proper preparation for passing the compliance test. Many companies realize this fact and invest in substantial pre-compliance testing to help ensure a quick pass on the first try. It is much less costly to discover a problem before the design leaves the company, than to discover a problem at the compliance certification laboratory. With efficient pre-compliance test equipment, a few extra days of testing can save weeks of lost revenue.

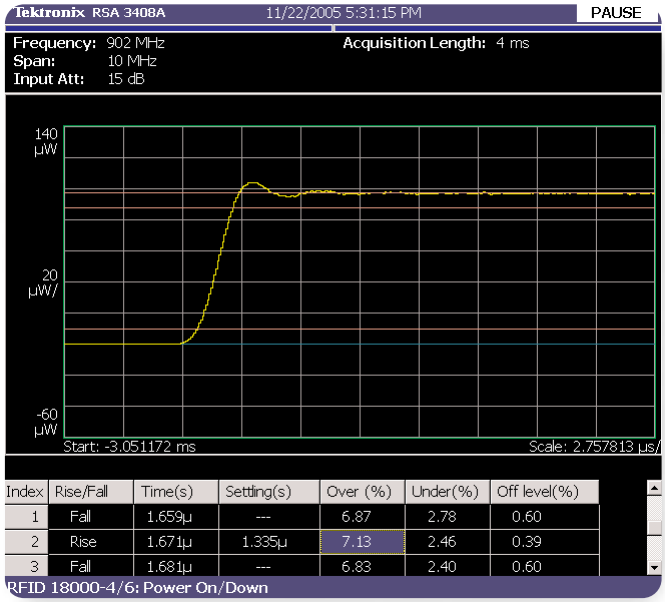


On September 14, 2005 the first EPC Gen2 compliant products were officially granted certification. The conformance test system, incorporated a Tektronix RSA3408A real-time spectrum analyzer. A custom signal unit generates and decodes RFID messages in real-time using an arbitrary waveform generator to modulate and up-convert the transmit signal to the Device Under Test (DUT). The RTSA measures the DUT's response to determine compliance with the standards.

Cetecom can be contacted at: http://www.cetecom.es/

A certified test laboratory usually carries out compliance testing with a custom automatic testing system. Compliance testing is frequently much more exhaustive than the typical bench development testing. The time required for most engineers to exhaustively test their designs may not make sense if the measurements are arduously slow to make. This is where the RSA3408A can offer the engineer an outstanding pre-compliance testing advantage.

The RSA3408A's unique RFID measurement software allows rapid characterization of many critical industry specification requirements. The built- in tabular data display enables the engineer to search for compliance



▶ **Figure 16.** *Pre-compliance measurements like settling time can help ensure interrogators pass the official compliance test the first time.*

issues quickly. With traditional test equipment the labor required to make many of the measurements is so great only a few spot checks are logistically possible. The high speed that measurements can be taken with the RSA3408A allows the engineer to approximate the exhaustive compliance test much more closely.

As we have seen, many of the important RF measurements have the convenience of one-button setups with the RTSA's RFID measurement software. The ability to quickly recheck a host of specifications reduces the possibility of a surprise failure during the actual compliance test.

For example, careful pre-compliance measurements under a variety of conditions testing the interrogator's data burst power on, power down and RF envelope ripple can help avoid issues during certification.

Using the RSA3408A as a pre-compliance measurement tool will likely eliminate the possibility of measurement algorithm errors between pre-compliance and compliance measurement equipment. The RSA3408A's leadership in delivering the test industry's first dedicated RFID measurement suite has given it rapid adoption by a wide range of RFID experts, including the compliance test laboratories. There is a very good chance that one's RFID product will successfully undergo compliance certification with the RSA3408A making many of the measurements.

If an issue does arise during the compliance test, having the easily portable single box RTSA available provides a means to quickly troubleshoot circuits. Once a compliance failure condition is known, the RTSA's multi-domain time correlated analysis capability delivers the insight necessary to trace the failure to its root cause. The RSA3408A can help the engineer rescue the compliance effort by rapidly identifying the issues. This can prevent the lengthy setbacks that can occur with outdated and inefficient test equipment.

Conclusion

The RFID industry encompasses a broad array of technologies and applications, many of which differ from the typical communications link. The latest international RFID standards call for sophisticated FHSS signals with transient half duplex RF bursts composed of ASK modulations with unusual encoding and robust anti-collision protocols. To mitigate the need for elaborate measurement setups and simplify the user interface for easy diagnostic insight, Tektronix has introduced the RSA3408A real-time spectrum analyzer with RFID analysis software.

With the first comprehensive RFID analysis software package, the real-time spectrum analyzer supports a variety of popular international RFID standards. This capability greatly speeds development diagnostics, pre-compliance testing and production checkout. Furthermore, the RFID analysis package fully supports time correlated multi-domain measurements, improving the reliability of troubleshooting assessments.

Measurements standards requiring demodulation of DSB-ASK, SSB-ASK and PR-ASK, as well as the necessary symbol decoding for each of the supported formats, now have one button measurement convenience on the RSA3408A. This greatly enhances engineering productivity while shortening the time to market. The RTSA also helps engineers perform RFID measurements that either cannot be made or require elaborate, time-consuming test setups on traditional swept spectrum analyzers or vector signal analyzers.

Whether debugging a development issue, meeting government spectral regulations or preparing the product for certification with a battery of pre-compliance testing, the RTSA is uniquely suited for analyzing RFID signals generated by interrogators and tags.

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

Our most up-to-date product information is available at: **www.tektronix.com**

12/05 FLG/WOW 37W-19258-0

Tektronix
Enabling Innovation