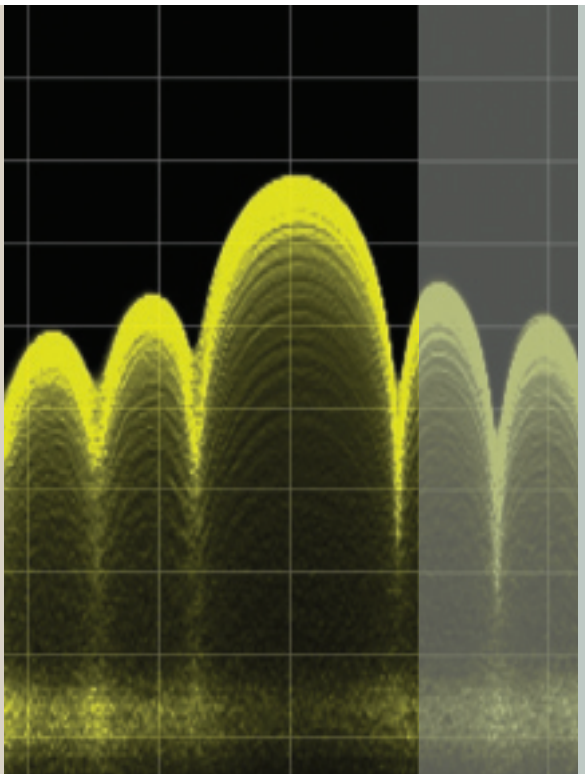
Application Note



Solving the Most Difficult RFID Testing Challenges

Introduction

Recent advances in submicron Complementary Metal Oxide Semiconductors (CMOS) promise to make RFID technology more ubiquitous. This can be seen in the increasing amount of embedded RFID, the founding of the Ubiquitous ID Center and T-Engine Forum, as well as the support of the GSM Association to embed Near Field Communication (NFC) capabilities into cellular phones. The lure of precision supply chain management, contactless point-of-sale (POS) transactions, anti-counterfeiting, and asset tracking/monitoring is fueling rapid deployment of the technology.

Tektronix®

The big challenges in RFID are optimizing performance, interoperability, integrating RFID into devices along with other technologies (i.e. Cellular, WLAN, Bluetooth, Zigbee, etc.) and fielding in the presence of interference.

This application note offers a systematic, detailed approach to analyzing the performance of an RFID system, and the environment in which it is deployed, using the features available in the Tektronix RSA3000B Series Real-Time Spectrum Analyzer (RTSA). While there are a variety of frequency bands and applications for RFID (as seen in Table 1), this application note will offer examples from the Ultra-High Frequency (UHF) band (300 MHz to 3 GHz) which utilizes radiative coupling. The challenges and solutions listed below often apply to inductive coupling systems (LF and VHF frequency bands) as well.

The 10 RFID analysis challenges addressed in this application note are:

1. Optimizing performance within assigned frequency bands
2. Evaluating dense mode reader/ interrogator performance
3. Verifying transmission duration
4. Triggering on a signal at a specific frequency and time
5. Document system performance
6. Correlating data in time, frequency, and modulation domains
7. Timing measurements
8. Demodulating hopping signals
9. Troubleshoot serial data connection
10. Troubleshoot embedded RFID transceiver

Application	Standard No.	Name
For Animals	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 13.56 MHz
	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 "Proximity" Card	ISO/IEC 14443-1	Physical Characteristics
	ISO/IEC 14443-2	Radio Frequency & Power
	ISO/IEC 14443-3	Initialization & Anti-collision
Identification "Vicinity" Card	ISO/IEC 14443-4	Transmission Protocol
	ISO/IEC 15693-1	Physical Characteristics
	ISO/IEC 15693-2	Air Interface & Initialization
	ISO/IEC 15693-3	Anti-collision & Protocol
Near Field Communication	ISO/IEC 18092	Near Field Communication Interface & Protocol

ISO: International Organization for Standardization **IEC:** International Electrotechnical Commission
TC: Technical Committee **SC:** Sub-Committee **WG:** Working Group **JTC:** Joint Technical Committee
TR: Technical Report **Proximity:** several mm - several 10 mm **Vicinity:** several 10 mm - 0.7 m

Table 1. RFID Standards.

	North America	Europe (302 208)	Singapore	Japan (pending)	Korea (new)	Australia	Argentina Brazil Peru	New Zealand	China
Bandsize (MHz)	902 - 928	866 - 868	866 - 869 923 - 925	950 - 956	908.5 - 914	918 - 926	902 - 928	864 - 929 spotty	840 - 845 920 - 925
Power	4 W EIRP	2 W ERP	0.5 W ERP 2 W in upper band	4 W ERP	2 W EIRP	4 W EIRP	4 W EIRP	0.5 - 4 W EIRP	2 W ERP 100 mW @ Band Edges
# of Channels	50	10	10	12	20	16	50	varied	20

Figure 1. Frequency spectrum allocated in various countries for RFID in the 800/900 MHz UHF ISM band.

RFID Challenge #1: Optimizing performance within assigned frequency bands

We begin our discussion with an overview of RFID parameters which are fundamental to all standards as well as non-standard (proprietary) implementations. For more details on RFID fundamentals, please refer to Tektronix Application Notes, RFID and NFC Measurements with the Real-Time Spectrum Analyzer (37W-19258) and Radio Frequency Identification (RFID) Overview (37W-18055) available at www.tek.com.

The first challenge addressed is that many RFID readers are designed to operate in a variety of countries. Figure 1 shows the frequency spectrum allocated in various countries for RFID in the UHF Industrial, Science, and Medical (ISM) band. As can be seen, the allocated spectrums can be as narrow as 2 MHz (Singapore and Europe) or as wide as 26 MHz (North America). Systems which operate in the 433.5 - 434.5 MHz band (such as ISO 18000-7 systems) are approved in every developed country with the exception of Japan and utilize Frequency Shift Keying (FSK) to minimize the amount of spectrum they occupy.

In those areas where only 2 MHz of spectrum is allowed, the data rate between readers and Tags will be much less in Europe and Singapore. Also, the spectral mask imposed by the EU and parts of Asia limits data transfer rates to 30% of those possible in North America (500 vs. 1500 reads/sec).

As an example, this may limit the speed of pallet loads on forklifts passing through dock doors. System throughput rates are an important consideration in the flow of asset tracking systems especially considering conveyor belt product spacing, speed, or groups (pallets) of products passing through a reader.

Also, as with any intentional radiator, the RFID transceiver must comply with local regulations regarding creating interference as well as be designed for optimum immunity to interference. There are essentially three approaches taken to implement this: Frequency Hopping (FH), Listen-Before-Talk (LBT), or synchronization (whereby frequency planning is used to limit the readers to certain channels such that they do not interfere with each other). Frequency hopping is utilized in the United States according to FCC 47 CFG Ch. 1 Part 15. LBT or synchronization is implemented in most European countries according to ETSI EN 302 208-1.

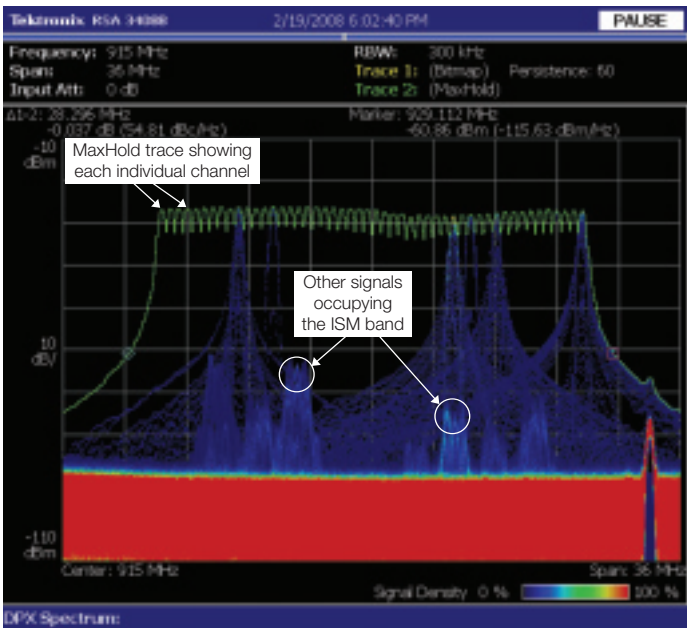


Figure 2. DPX display of the hopping signals from a reader which is designed to conform to ISO18000-6C for operation in North and South America (region 2). These signals last only ~5 ms and would take much longer to be captured on a Swept Spectrum Analyzer (SA) compared to the 48,000 spectrums/sec processing rate of DPX in the Tektronix Real-Time Spectrum Analyzer.

Solution #1: Using Live RF to discover the true RF environment

The first step in evaluating RFID system performance is to use the RSA3000B Digital Phosphor display known as DPX™, or Live RF, to evaluate what is happening in the frequency span of interest.

With DPX (Live RF) you can:

- See other RFID channels and systems used in the same band
- Discover other ISM band devices that might be present (two-way radios, cordless phones, Zigbee devices, etc.)
- Detect the potential for interference and system degradation

For the UHF band in North America, we would press the DPX button on the front panel of the RSA3408B, and then tune the RTSA to a 915 MHz center frequency and a 36 MHz span. This span allows for capturing the entire 26 MHz of interest as well as monitoring the modulation sideband behavior of both channel 1 (centered at 902.75 MHz) and channel 50 (centered at 927.25 MHz).

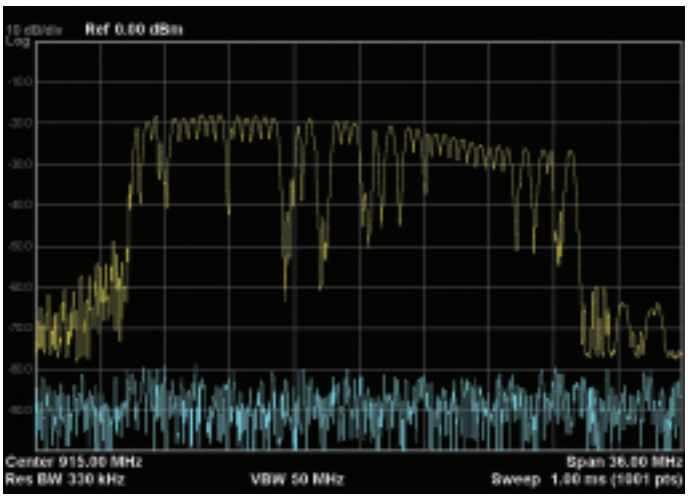


Figure 3. Same RFID reader as shown in Figure 2 after 30 seconds on a Swept Spectrum Analyzer.

In Figure 2, we see the DPX display on the RSA3408B. The display has the classic X and Y axis, where horizontal axis is frequency and the vertical axis is amplitude (in dBm). What is different are the update rate and the addition of color coding to indicate temporal, or time-based information. The color represents signal density, or how long a signal dwelled at that particular frequency and amplitude. The ability to display transient, or rapidly changing signals is also significantly increased compared to any other signal analyzer; for example, the RSA3408B DPX display is guaranteed to show signals which last only 31 µs or longer. For details on DPX, see the primer Fundamentals of DPX in Real-Time Spectrum Analyzers (37W-19638) available at www.tek.com.

After only 30 seconds of monitoring the output of the reader, a lot of information can be found. For one, we can see the RTSA has already captured all 50 of the channels, seen as peaks on the MaxHold trace (Green). Also, it is obvious that there are, in fact, a number of other signals occupying the frequency band; only DPX allows this fast view and ability to see signals which occupy the same frequency at different periods of time, even at different amplitudes. These lower level signals are not tags (we will see what the response of tags looks like in the DPX display) they are some other wireless devices operating in the ISM band and would not be viewable on a Swept Spectrum Analyzer (SA) display as shown in Figure 3, not matter what the claim of sweep rate.

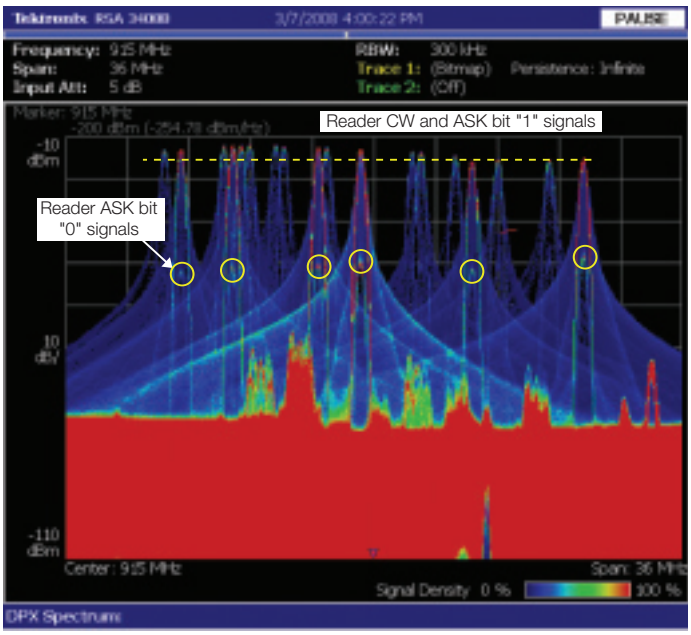


Figure 4. DPX display of RFID reader and tag interactions, note that tags are responding where there are no intefering signals.

The SA display will take considerably longer to show all of the 50 channels as each hop in this particular example is lasting approximately 5ms. The SA shown in Figure 3 would require signal duration of 11 ms for a 100% probability of displaying each frequency hop. This can be especially problematic for EPC GEN 2 readers when the system is operating at maximum read rate, that is, the reader is utilizing 'FM0' encoding and the reverse link (from the tag) Back Link Frequency (BLF) is at the maximum data rate of 640 kbps. In this mode, the read time can be as fast as 175 µs so it will take much longer for a swept analyzer to eventually see all the interactions. Eventually, the swept approach will show all the channels on the max hold display. What will never be seen are the interfering signals below, between the MaxHold trace and current trace. Let's examine why this is significant.

For testing purposes, a number of tags were placed into read range of an interrogator and monitored both with DPX and a PC which displayed successful reads. A correlation was made between when a tag response would appear on the PC and the spectral shape and frequency location as seen on the RSA3000B DPX display. Refer to Figure 4 and note that it is possible to see at which frequencies the reader is successfully interacting with the tags. This is seen by the fact that the signal increases in density (becomes more Red) as the

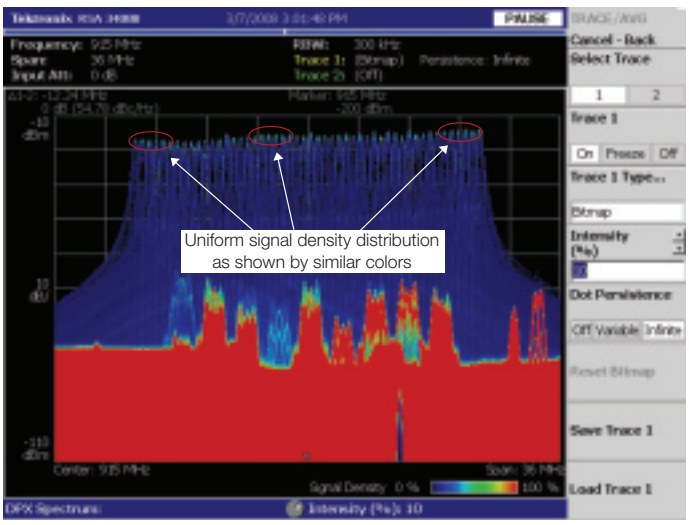


Figure 5. DPX display with infinite persistence after just a few seconds.

reader dwells longer to complete a tag interaction. The ASK low level signals from the reader can also be seen as a more narrow, lower-amplitude shape contained within the higher-amplitude reader CW and high amplitude ASK state signals. Note that all of the successful polling occurs at frequencies where there are no interferers, and the signal-to-noise ratio is greater. This clearly shows why the chances of a successful tag read increases in an environment with minimal interference.

When doing frequency planning to restrict each reader to a certain channel (or channels), DPX can be used to ensure that the modulation sidebands are not at such a level that would cause interference in those channels being used by co-located readers. Note that the reader and tag signals in the center of Figure 4 have wide spectral spreading and are dwelling for a longer period of time than in other channels; this is seen as the trace is darker due to the higher signal density. This could be a source of read failures in the adjacent channels, and action should be taken to ensure filtering in the readers is sufficient to have immunity to this interference.

The next thing to look for is frequency and amplitude distribution of the hopping signal. Ideally, the reader signal will be hopping in a pseudo-random pattern which spreads the signal density evenly across all 50 channels. Also, the amplitude of the reader signal should be the same as it hops across the allocated 26 MHz frequency band.

Now we will look for even frequency distribution by adjusting the Trace/Avg settings so that the intensity is reduced and Dot Persistence is set to *Infinite*. This will hold signals on the display and have them move from the Blue to Red spectrum as their signal density increases (e.g. as they spend longer time at that particular frequency and amplitude). The next step is to monitor the display and confirm that the channel signal density is changing in a uniform manner, which means the hopping algorithm is nicely distributing the hopping signal. If any one channel or individual channels display more signal density at a faster rate than the others, the hopping algorithm needs to be refined.

The challenge of optimizing performance within assigned frequency bands is even greater for RFID systems utilizing *active* tags, meaning they have an on-board power source (e.g. a battery) as opposed to tags which are *passive/active* and depend on the signal from the reader to charge their capacitive circuits. ISO18000-7 tags are always active and ISO18000-6C has an allowance for active tags (known as class 3 and 4). So, while high-powered active tags can be very helpful when operating in the presence of interference, the tags themselves are now intentional radiators and thus sources of interference. Reducing both the generation of, and the susceptibility to, interference is also of concern as radar, garage/gate door openers, amateur radio and remote keyless entry devices (in Europe) operate in or very near this frequency band.

The next area to look at with these same DPX display settings is the amplitude flatness or *frequency response* of the reader's transmitter when it is using a hopping algorithm.

Figure 6 is an example of an amplitude *drop-out* of around 10 dB in the area of 922 MHz. This problem is even worse because, using the DPX display, we can see there are also some lower level ISM signals which act as interferers. So the

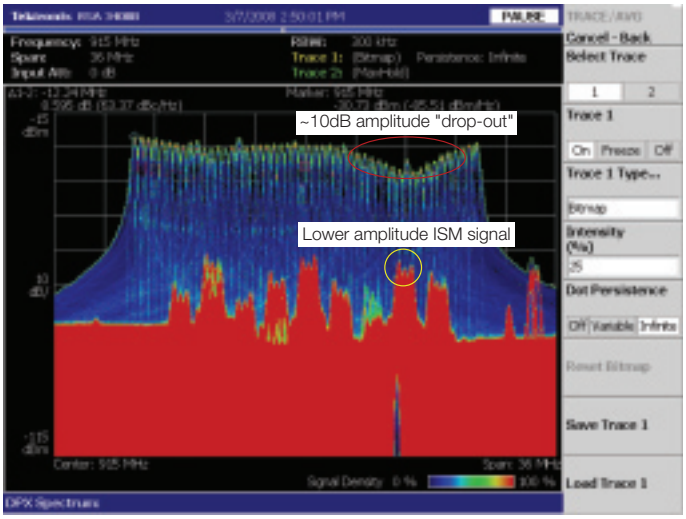


Figure 6. MaxHold in DPX display can show the frequency response of the channel operation in a particular band much faster than a swept approach.

signal-to-noise ratio is reduced from the 55 dB in other parts of the spectrum to only 25 dB or less in this frequency area. Action should be taken to flatten the frequency response of the reader's transmitter (most likely the output amplifier) or perhaps the antenna and to reduce or eliminate the source of interference.

The examples above were all using the frequency hopping approach. DPX is also extremely useful for providing an intuitive Live RF display of signal interaction when analyzing a *Listen-Before-Talk* (LBT) implementation. In LBT mode, the reader cannot begin to broadcast when a signal is present in that channel frequency and above a given amplitude. DPX would show if a reader did, in fact hop to that frequency and if it then vacated it or dwelled there. This would all be seen as a live update, there would be no need to trigger an acquisition and then perform post-capture analysis.

Challenge #2: Evaluating dense mode reader/interrogator performance and Challenge #3: Verifying transmission duration

So far we have discussed readers operating in a *Single Reader Environment*. In reality, many RFID systems will be implemented in a Multiple Reader or Dense Mode environment.

- Single Reader Environment: a single reader is operating in an environment
- Multiple Reader Environment: the number of simultaneously operating readers is less than the available number of channels
- Dense Reader Mode: the most challenging environment, whereby the number of readers is large compared to the number of channels (i.e. >10 readers in an environment with 10 channels available)

The term "operating environment" is defined as the zone within which the reader's RF signal is attenuated by less than 90 dBc (a radius of approximately 1 Km). Consequently, many readers will end up operating in a dense mode environment whether by design or due to neighboring RFID readers.

For example, in a shipping lane or warehouse application with fixed readers and accurate spectrum planning, there may be minimal interference from your neighbor within 1 Km; however, a mobile device using embedded RFID (i.e. NFC) should expect a dense reader mode environment due the lack of control over safe mitigation distances being maintained. In this case it becomes even more critical to discover what signals are present in the environment where the RFID system is being deployed and, especially in the cases of embedded/mobile RFID, understand the behavior of the reader and tags in the presence of interference.

To handle this environment, ISO18000-6C readers which have been certified for dense environments will often switch to Miller-Modulated Subcarrier (MMS) encoding. This elaborate encoding provides more transitions per bit and so is easier to decode in the presence of noise, but is slower for the same tag Backscatter Link Frequency (BLF). Three different MMS schemes are available, Miller-2, Miller-4 and Miller-8. The number specifies how many BLF periods define a data symbol. For example, using the slowest BLF of 40 kHz, the data rate for Miller-8 is the BLF/8 = 5 kbps. At such a slow rate, to transmit a 96-bit EPC and 16-bit error check will take 22.4 ms, corresponding to less than 45 tag reads per second (even fewer when all the overhead, such as the Forward Link commands, is included). Part 15 only allows for operation at a single frequency for up to 400 ms. So, regardless of read status, the interrogator must vacate the channel after this time and hop to a different frequency.

Readers and tags operating in conformance to ISO18000-7 take a different approach of utilizing longer RF transmissions with slower transfer rates, which allow the signal to be more immune to interference. This requires that the maximum transmission duration be increased to 60 seconds while maintaining a 10-second minimum silent period between transmissions. At such slow transfer rates, transferring the full 128 kilobytes of data needed to identify all the contents of a shipping container can take up to two minutes.

Solutions to #2 and #3: Arbitrary waveform generator, deep memory and continuous trigger

Simulating a Dense Mode environment to do pre-compliance for dense reader mode certification is possible using the Arbitrary Waveform Generator (AWG) from Tektronix. Either the AWG5000 Series or AWG7000 Series can be programmed to directly generate RFID signals across the HF and UHF bands and thus be used to simulate a variety of signals such as multiple readers or multiple tags with just one instrument. This reduces the time and cost of having to configure both a function generator and an RF signal generator.

Deep memory is often required of the analyzer to capture all of these interactions. Typically, the interations are delayed as the reader often tries multiple query iterations, and command the tags to reduce their link frequency (i.e. use MMS encoding) and to verify it is vacating the channel as required in a LBT implementation.

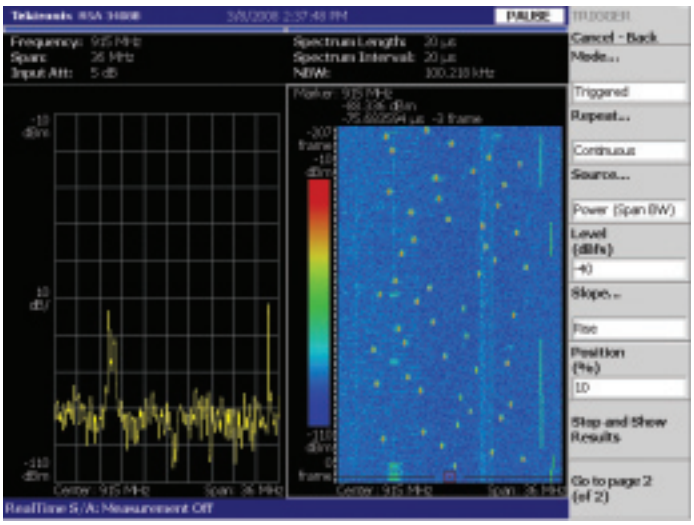


Figure 7. Set up for Continuous mode trigger and a spectrogram view of the resulting capture of multiple seamless acquisitions each time a trigger event occurs.

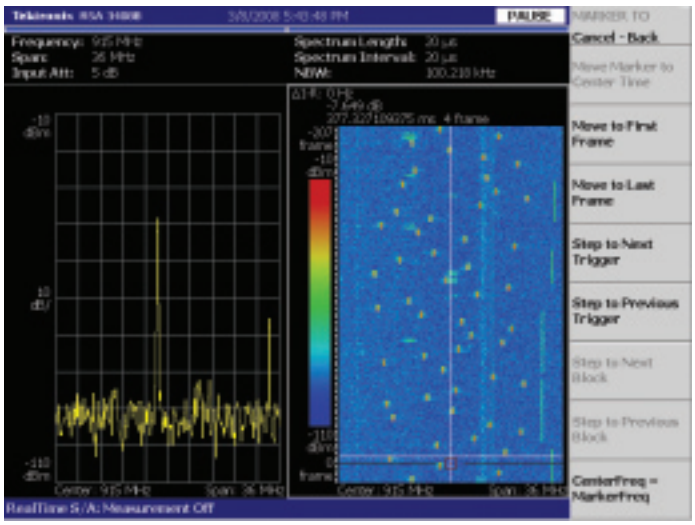


Figure 8. Measuring the ~377 ms hopping/burst interval (1-R) using reference marker and the ability to step the marker to each acquisition trigger point.

For verifying the 433 MHz band, a span of 500 kHz on the RSA3000B will offer up to 102.4 seconds of memory, more than enough to verify both the 60-second transmission and the 10-second silent period. The additional memory can be useful for the exception which allows for excluding the 10-second silent period in the case of data transmission error. So, a long memory capture can be made and, if more than a 60-second burst is seen, analysis can be performed to determine if a transmission error or interruption occurred.

Another way to view and analyze the hopping and bursting signals is to take advantage of the fact that the RSA3000B is not simply a *single-shot* acquisition engine. This is done by using the spectrogram display and changing the "Repeat" setting in the trigger menu to "Continuous" as shown in Figure 7. Continuous trigger allows not only for a seamless acquisition into memory whenever a trigger event occurs, but also for the trigger to re-arm and wait for future trigger events to store again seamlessly into memory. Using this mode of operation, a user can set up the RTSA for short acquisitions and then allow the instrument to trigger each time there is a frequency hop or the signal turns on/off (e.g. enters or leaves a silent period). Not only can multiple acquisitions be made but the time between these acquisitions can be measured directly. The white bars in the spectrogram view on the left side of the window in Figures 7 and 8 represent individual acquisitions; the top of these white bars are the trigger point. The marker menu allows a user to easily navigate within the spectrogram view by offering a way to move the marker from trigger point to trigger point and to either the first or last acquisition (frame). Simply set up a reference or delta marker, then move the marker to the next trigger and read out the time between hop/bursts as shown in Figure 8.

It may be desired to play back the acquisitions automatically while updating the spectrum display in a kind of video-like playback; this is possible on the RSA3000B using a macro known as Auto View. Pressing the MACRO front panel button will recall any installed macro program present on the instrument as seen in Figure 9. Auto View and the other RSA3000B macro programs can be downloaded from www.tek.com/rtsa, or ask your Tektronix sales representative about it.

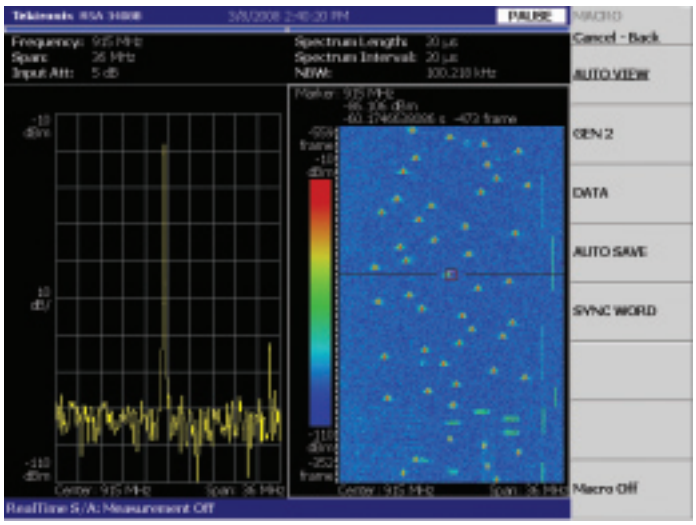


Figure 9. Pressing the MACRO front panel button displays all of the macro programs residing on the RSA3000B in the side bezel menu, including the Auto View macro.

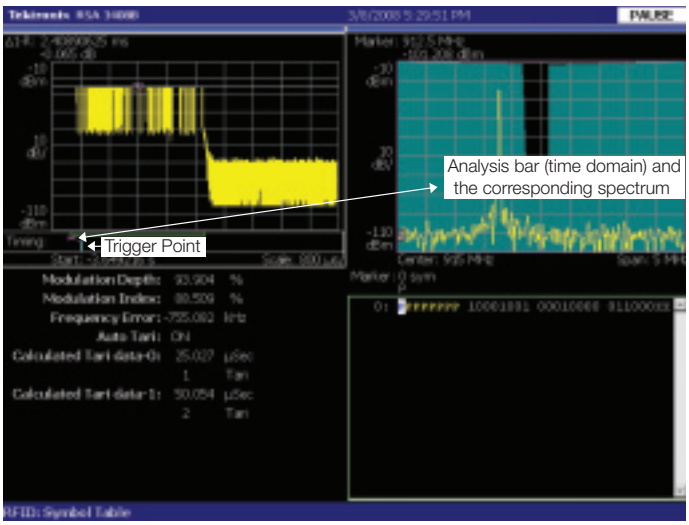


Figure 10. This figure shows the spectrum prior to the trigger point.

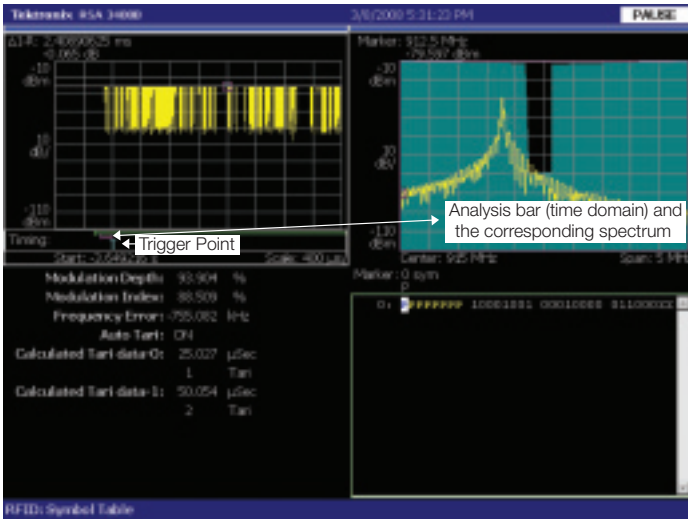


Figure 11. FFT of the time domain data at the trigger point shows the instrument triggered due to modulation sidebands violating the mask at that instant in time.

Challenge #4: Triggering on a signal at a specific frequency and time for further analysis

As shown in the earlier challenge sections, RFID signals often operate in presence of other signals. It can be a challenge to trigger only on your desired signal, especially if it is not the highest amplitude signal in the span you are monitoring. In many cases only the modulated portion of the reader signal, or only the tag response itself, is what you truly want to capture and analyze. And when that's the case, you aren't interested in the milliseconds or more of CW signal or polling before the tag responds.

Solution #4: Frequency mask trigger

Frequency Mask Trigger (FMT) allows for frequency selectivity when triggering on frequency domain signals. By simply defining a mask, a user can ignore other signals in the selected frequency span, even if they are of higher amplitude. For RFID applications this comes in handy for triggering only when a certain modulation sidebands are present (i.e. the reader is modulated or only when tags are responding).

Another use for FMT is using the synchronization and spectrum planning approach whereby readers are assigned certain channels to communicate, and filtering is used such that they do not interfere with one another. In these cases, it may be desired to only trigger on a reader operating at certain channels/frequencies.

Capturing a frequency domain event can be a challenge in some modes of RFID operation. For example, when ISO18000-6C tags are responding in the fastest mode (FMO encoding with the fastest link frequency of 640 kbps), then the read time is on the order of 175 µs. Fortunately, FMT is specified to trigger on signals as fast as 20 µs in a 36 MHz bandwidth on the RSA3408B.

The RSA3000B performs a Fast Fourier Transform (FFT) on the portion of the time domain data shown in the upper left window indicated by a magenta-colored bar and displays the resulting spectrum in the upper right. The “T” symbol is the trigger point. Figure 10 shows the spectrum prior to the trigger point. Figure 11 shows an FFT of the time domain data at the trigger point; the trigger event being the modulation side-bands violating the mask at that instant in time. In a 5 MHz span, as used in this example, the RSA3000B FMT has 100% trigger on all signals lasting >160 µs and offers up to 10.24 seconds of record length.

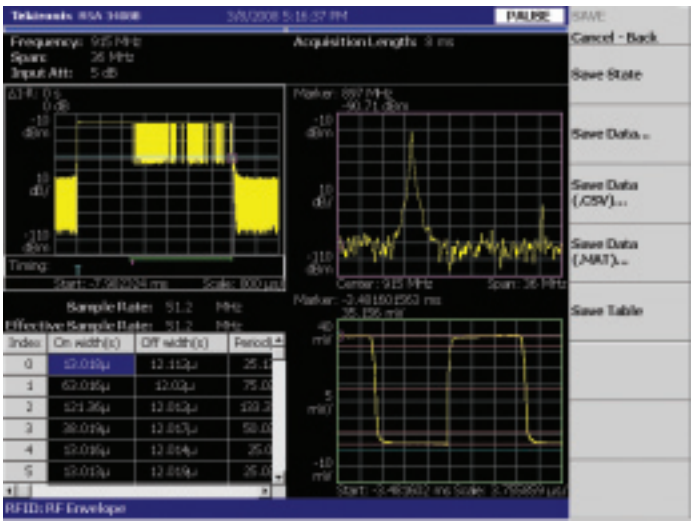


Figure 12. The functions of Save Instrument States, Save Data Formats, and Save Tables are all available on the RSA3000B.

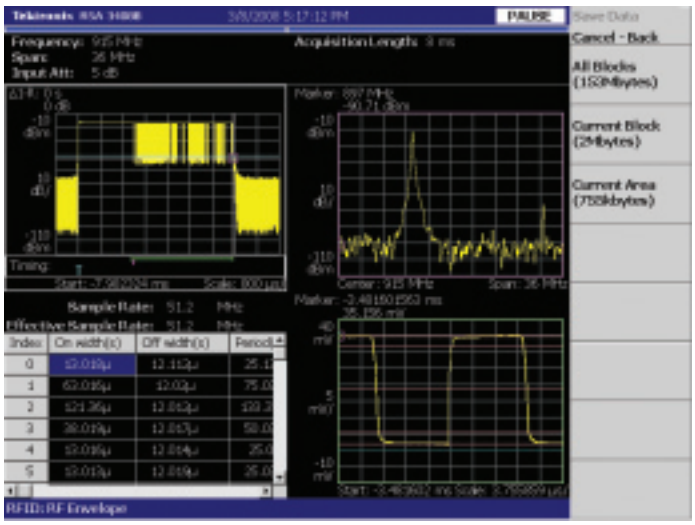


Figure 13. Save Data options on the RSA3000B.

Challenge #5: Document system performance

So far we have discussed using DPX to discover what is occurring in the spectrum of interest and get a clear idea of the reader/tag interactions. We then moved on to discussing triggering on the signal to capture a seamless acquisition. The next step is to save the data so that further analysis can be performed. The challenge here is that the file size and duration of the captured signal may quite large, but the area of interest may be only a small portion of the entire acquisition. The other part of this challenge is to save in a file format which makes it easy to import into other analysis tools or database software.

Solution #5: File formats and segmented save

The RSA3000B offers a variety of formats in which to save the data. As shown in Figure 12, a user can save in .MAT for easy import into MATLAB®, the IQ-versus-time can be saved as .CSV or the actual displayed table can be also be stored in CSV format. Screenshots can also be saved as .bmp for documentation purposes. RSAVu is the off-line version of the RSA3000B user interface; it can be installed as a stand-alone application in separate PCs and used for off-line documentation purposes or re-creation of measurements at a later date without having to recapture data.

Often a large acquisition is made but perhaps only a portion of the signal is what is desired to be stored for future reference. In this way, one does not have to scroll through a long acquisition to find that few milliseconds of desired signal. If multiple acquisitions were made (using the “continuous trigger” mode discussed earlier) then all of them can be saved using the “save all blocks” option. If only the acquisition currently being displayed is of interest, then the user selects “save current block.” The other option is to save only the portion that is being analyzed (the portion of the signal in the upper left of the display in Figure 13 that has a Green analysis bar underneath it).

Once the signal has been acquired, it is always a good idea to save it into memory before continuing on to the next step of analyzing the data.

Manual (Embedded/Proprietary)

Modulation types

- ASK, SSB-ASK, DSB-ASK, PR-ASK, OOK, FSK

Decoding formats

- Manchester, Miller(M_2), Miller(M_4), Miller(M_8), Modified Miller, FM0, PIE (Type A), PIE (Type C), NRZ

Figure 14. Supported modulation types and decoding formats available on the RSA3000B when the "Standard Type" parameter is set to "Manual."

Challenge #6: Correlating data in time, frequency, and modulation domains

Once we have a successful demodulation, we can begin to correlate the analysis in a way that helps to understand if the reader and tag are performing if expected, and if not, why not. Did an amplitude glitch cause a frequency error? If a particular bit is not decoding properly, is it because of an error in the FSK or ASK modulation? Being able to correlate data in various domains will help to answer these questions.

Solution #6: Time correlated, multi-domain analysis

Two features of the RSA3000B which will help with this are time-correlated markers, and the View: Define menu.

First the RTSA needs to be configured to analyze data from the reader and/or tag.

Once a user has selected the DEMOD mode of operation and has the acquired data loaded for analysis, the next step is to establish the signal parameters. This has been simplified in the "Meas Setup" screen. A user can select "Manual" if the system under test does not conform to an ISO standard. Or the user can select one of the 13 pre-configured standards so that the RTSA will set up parameters automatically according to which *Link* is selected (Interrogator or Tag). Figure 14 shows the currently available standards which are pre-configured, as well as the modulation and decoding options when manual mode is selected.

BLF (kHz)	Encoding	Date Rate (kbps)
40	FMO	40
	MMS-2	20
	MMS-4	10
	MMS-8	5
	FMO	256
256	MMS-2	128
	MMS-4	64
	MMS-8	32
640	FMO	640
	MMS-2	320

Figure 15. Data rates for reverse link (from the tag) according to the selected Backscatter Link Frequency (BLF) and encoding type.

After setting up the modulation and data coding parameters, the final parameter to enter is the bit rate (or Tari in the case of ISO18000-6C). In some cases the bit rate (or Tari) is unknown. This can be especially difficult in the case of ISO18000-6C where the bit rate from the tag can vary widely as seen in Figure 15. When this parameter is unknown, the user can simply toggle the "Auto" feature to "On."

Now the RSA3000B is configured to analyze the signal. The last step is to select a portion of the acquired signal for analysis. This is done either in the Acquisition/Analysis menu or using markers in the overview window (upper left).

Once the desired portion selected, use the front panel button labeled "Measure" and, on page 2, select "Symbol Table." Now the analysis can be performed by pressing the "Meas Setup" front panel button and selecting "analyze" from the side bezel menu. The reason for starting with a symbol table measurement is that it quickly allows a user to see if the bits were decoded as expected. This is especially true in the case of testing ISO standards where the preamble's data will be highlighted in yellow, a strong sign of a successful analysis.

User tip!

To use the marker option, simply double-click with the mouse to the left of the desired analysis area and then single click to the right. Next, use the "Marker to" front panel button (the one that says "Marker" and has an arrow under it) and select "Analysis Time = Marker Time" from the side bezel menu. A Green analysis bar will appear under the selected portion.

At this point the display will appear as seen in Figure 16: there will be an overview window (upper left), a spectrum view (upper right), the symbol table (lower right) and the modulation data (lower left).

In the case of ASK with backscattered tag responses, the difference between the interrogator and tags is quite obvious. The tags are much lower peak-to-peak amplitude variations, whereas the interrogator uses much deeper modulation and thus has greater amplitude variations.

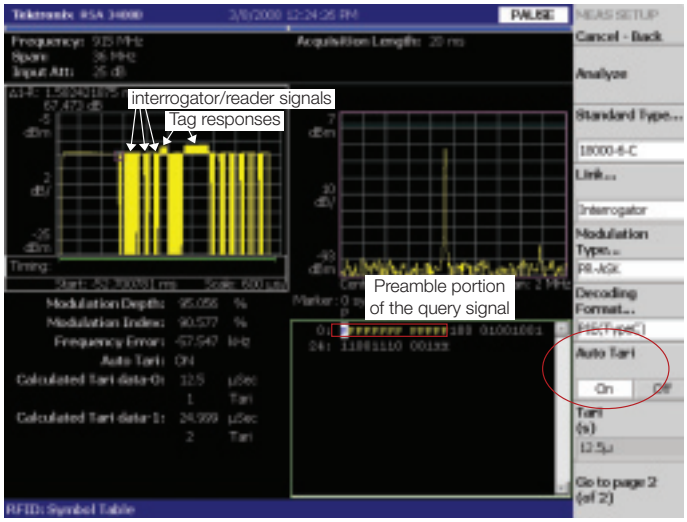


Figure 16. Auto "Tari" when testing ISO18000-6C (EPC GEN2). Note that 'P' indicates the preamble. For other portions of the interaction, it will be yellow 'S' for frame synch.

RFID Standards Measurements

Menu	Measurement	Standard					
		ISO 18000-4 Mode 1	ISO 18000-6 Type A, B & C	ISO 14443-2 Type A & B	ISO 18092 (424 k)	ISO 15693-2	ISO 18000-7
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		■	■	■	■	
FSK Pulse	On/Off Width						■
	Period/Duty						■
	On/Off Ripple						■
	Slope 1, 2, 3						■
Constellation	Modulation Depth	■	■	■	■	■	■
Eye Diagram	Modulation Index	■	■	■	■	■	■
Symbol Table	Frequency Error	■	■	■	■	■	■
	Bit Rate (Measured)	■	■	■	■	■	■
	Tari Length (0 & 1)	■	■	■	■	■	■
	Indicated Preamble	■	■	■	■	■	■
Marker	Turn Around Time	■	■	■	■	■	■

Table 2. RSA3000B offers automatic configuration and measurements on a variety of RFID standards.

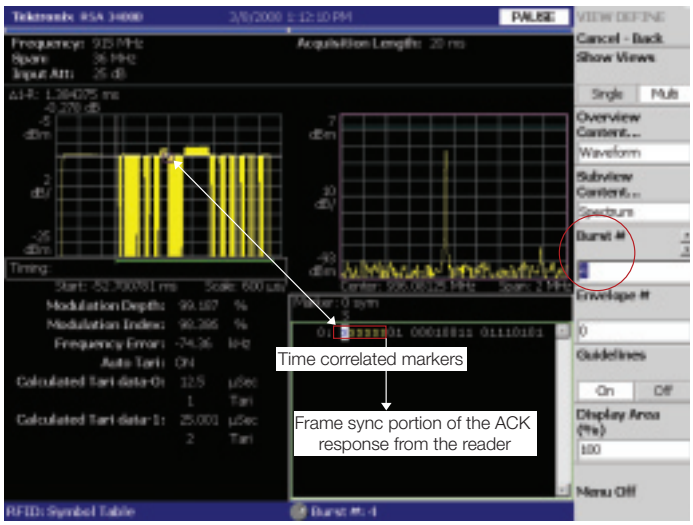


Figure 17. Burst is set to #4 which is the ACK response from the interrogator. Note that the marker (Red square) in the Overview window (upper left) is indicating what portion of the acquisition is being displayed.

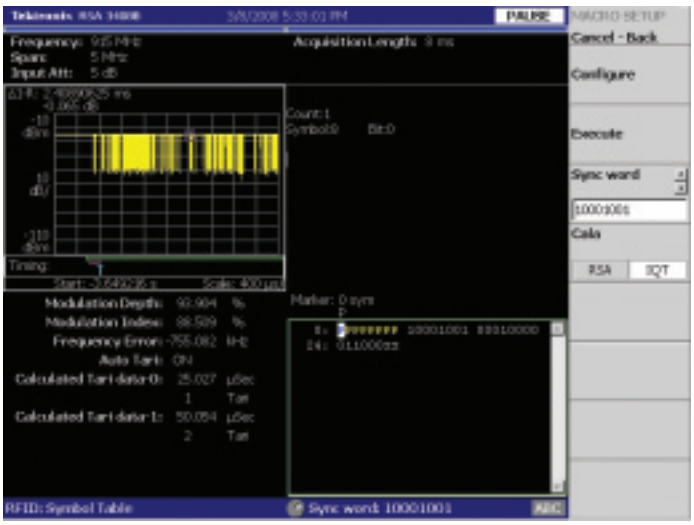


Figure 18. The Sync word macro automatically finds a string of data. Here it has found the byte '10001001' which occurs one time starting at symbol 8 (immediately following the preamble).

The "View: Define" menu allows a user to do two key things: navigate easily through the acquisition between frames (bursts), and to configure the display such that the desired parameters are viewed.

When the front panel button labeled "Define" is pressed, a side bezel menu appears as shown in Figure 17. The "Overview Content" and "Subview Content" allow for any one of a number of different displays to be selected while the "Burst #" and "Envelope #" allow for quickly navigating through the acquisition.

For example, to see if the correct ACK signal was returned from the interrogator to the tag on an ISO18000-6C system, simply rotate the Burst # and observe as the marker automatically moves to the beginning of the selected burst. Do this until the marker is at the burst immediately following the first response from the tag (which should contain the RN16); the symbol table (lower left of Figure 17) will automatically update with the decoded data. Here we see the expected response, the frame synch, followed by a 01 and the RN16.

The Sync Word macro allows a user to search the symbol table for a given data string (i.e. RN16, ACK, CRC bits, etc.) as shown in Figure 18. More details on this and all the other macros can be found in the documentation at www.tektronix.com/rfid

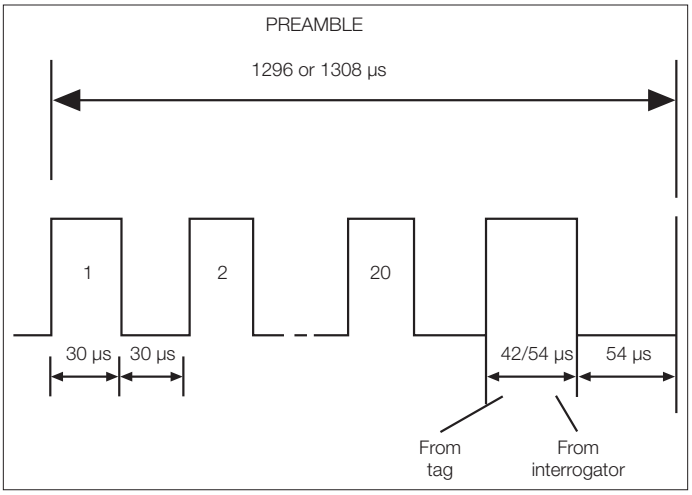


Figure 19. ISO18000-7 preamble.

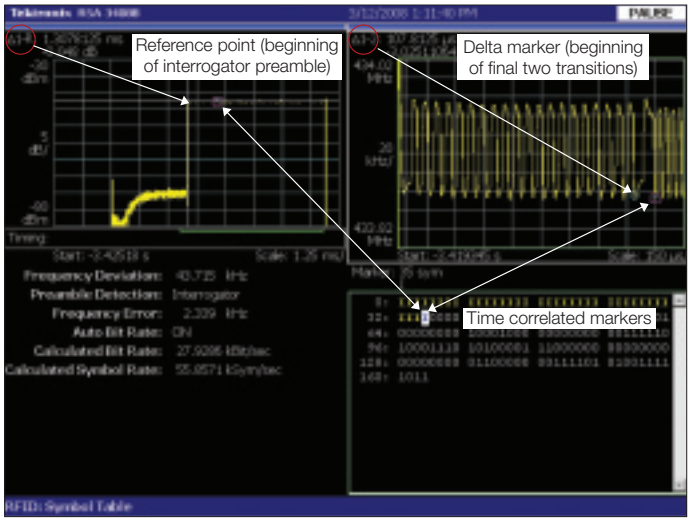


Figure 20. Verifying preamble of an ISO18000-7 Interrogator ('I') signal using time-correlated markers (special thanks to Savi Technology).

Challenge #7: Timing measurements

All of the data transmitted in RFID has a certain tolerance on the duration of the signal, be it a bit of data, a CW signal to power the tag, or response times between the reader and tag, also known as *turnaround time*. Turnaround time is measured as the interval between the last bit to transition from the interrogator to the first transition of the tag response. A long turnaround time can adversely affect the capacity and throughput of an RFID system.

Solution #7: Time correlated markers, automated timing measurements and GEN2 Macro (for ISO 18000-6C)

Let's look at some examples of analyzing/verify timing parameters using time-correlated markers, automated timing measurements, and GEN 2 macro. The first example is confirming the preamble timing on an ISO18000-7 signal.

According to the ISO 18000-7 document, "The preamble shall be comprised of twenty pulses of 60 µs period, 30 µs high and 30 µs low, followed by a final sync pulse which identifies the communication direction: 42 µs high, 54 µs low (tag to interrogator); or 54 µs high, 54 µs low (interrogator to tag)."

To verify these parameters, we isolate one of the bursts from the interrogator and demodulate the data.

Once the demodulation is performed, we see that the preamble appears as yellow 'I' (for Interrogator) and also that the display readout (lower left) identifies this signal as an interrogator; this is useful as the signals in this standard utilize Frequency Shift Keying (FSK) and are not as obvious to discern as the ASK used in many other RFID standards.

The RSA3000B offers timing resolution as fine as 20 ns to verify RFID timing parameters such as preamble length. To verify the length of the preamble, the reference marker is set in the overview window and a marker is moved along in the symbol table. As we do this, the marker also moves along in the overview window (upper left) which is displaying amplitude vs. time, and in the subview window (upper right) which is displaying frequency vs. time. So, at the end of the indicated preamble portion, we can read out directly from the marker in all windows which have the same horizontal axis (time) as they are all showing the exact same instant. Reading the delta time in the overview (Δ1-R) we see that the preamble lasted 1308 µs as dictated by the standard. We can also set up markers independently in each window. So in the subview window, a delta marker (Δ1-2) is also reading out the duration of the final two synch pulses for a total of ~108 µs, again, as dictated by the standard.

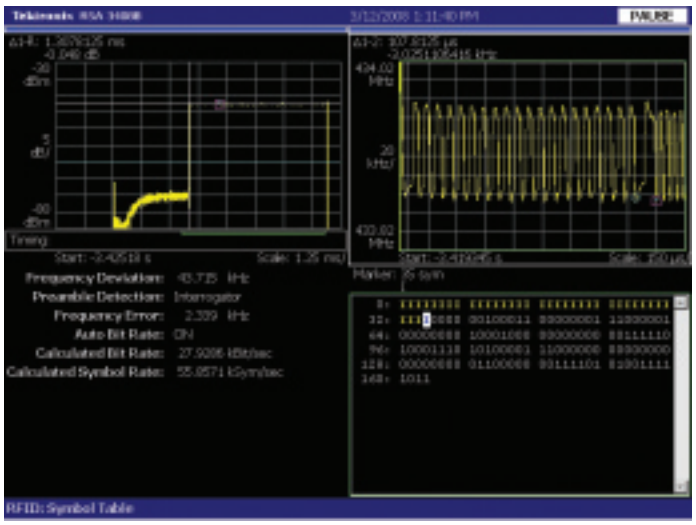


Figure 21. FSK Pulse parameter measurement screen.

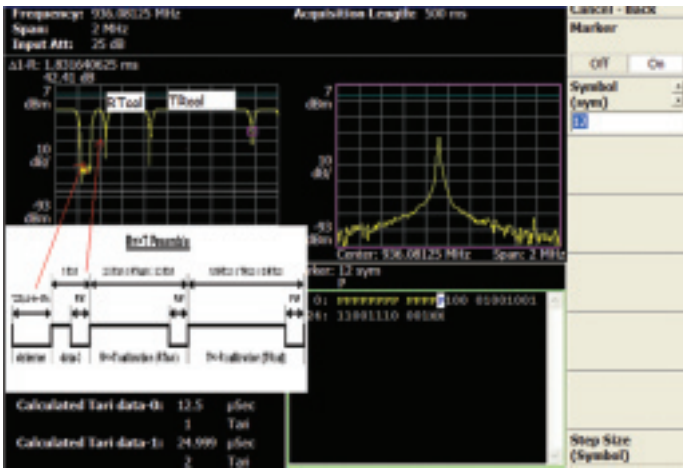


Figure 22. Critical timing parameters included in the preamble of an ISO18000-6C reader signal.

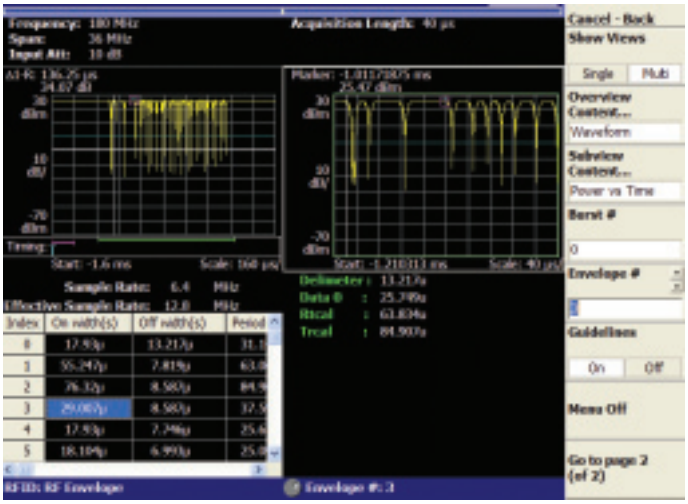


Figure 23. Automatic measurements of the RF envelope and preamble timing parameters: Delimiter, Data 0, RTcal and TRcal.

The *FSK Pulse* measurement mode is also useful for showing at a glance all the timing within the analysis period. As seen in Figure 21, the "On" and "Off" durations are ~30 µs following the final two transitions (Index 19 off, and Index 20 on) of ~54 µs. Also the *frequency rise time* can be analyzed, which is how long it took the device under test to transition from one frequency state to the next.

The second example is preamble timing and RF envelope measurements on an ISO18000-6C (EPC GEN2) signal. Preamble timing is critical because it sets the decision points for all future communication. If this timing is outside of acceptable limits, then all further signaling will not be properly decoded by the reader.

The four especially critical timing parameters in an ISO18000-6C signal are: Delimiter, Data 0 (Tari), RTcal and TRcal as shown in Figure 22. These parameters can be read by using the marker approach previously described, or by using the *RF Envelope* measurement. However, the easiest approach is to use a macro which automatically imports the results from the RF Envelope measurement, then calculates and displays these parameters as shown in Figure 23.

In addition to preamble timing, the standard has specifications for each of the following RF envelope parameters: ripple on, ripple off, pulse width on, pulse width off, and duty cycle. The ripple specification is designed to minimize the effects of noise or ringing from the tag's backscatter modulation method. If the noise and ringing effects are excessive, the Interrogator's ability to detect all the information contained in the tag's response is compromised. The pulse width specification allows sufficient time for the Interrogator to detect and decode data from the tag. The duty cycle defines the length of time the interrogator can transmit power. All of these measurements are made and displayed in the RF envelope table shown in Figure 23.

Challenge #8: Demodulating hopping signals when not captured at center of span

Signals at a frequency which are offset from the center frequency set on the analyzer are not possible to demodulate using mode spectrum analyzer and vector signal analyzers software analysis. So, if you set up a 5 MHz span and 915 MHz center frequency and the signal you capture happens to be at 908.75 MHz, you would still like to be able to demodulate it, right?

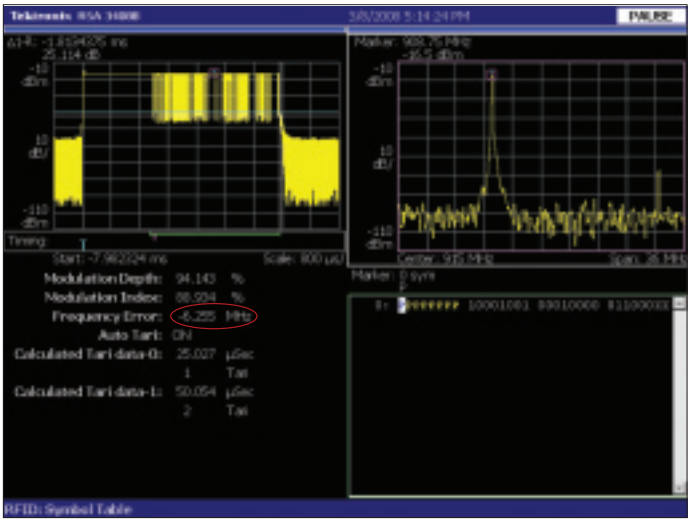


Figure 24. Demod off-center frequency when capturing hopping signals (6.25 MHz off CF in this case).

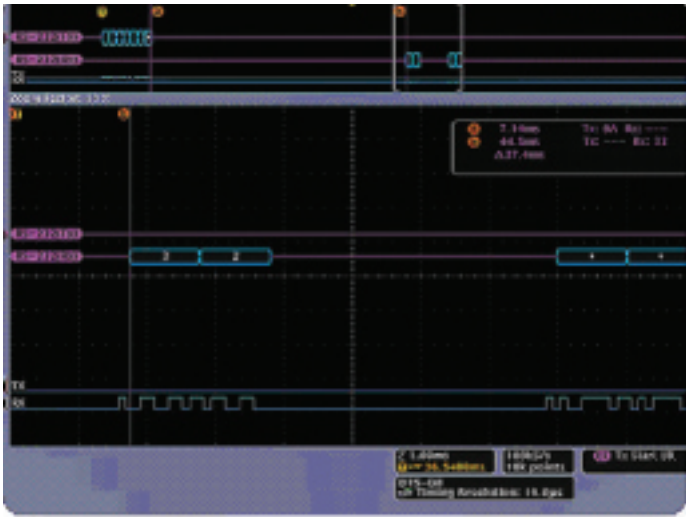


Figure 25. RS-232 triggering and decoding on the DPO4000.

Solution #8: RSA3000B ability to demodulate anywhere in the capture bandwidth

"A picture is worth a thousand words" and Figure 24 says it all: the RSA3000B can demodulate a signal anywhere in the capture bandwidth, so there's no need to worry if the acquisition of the hopping signal is not right at (or very close to) the center frequency you set on the analyzer. There is no need to waste time adjusting the analyzer to analyze the signal. Just select the area of analysis in the overview window and select "Analyze" to get all the measurements available on the RSA3000B, no matter where in the span the signal occurred and without having to recapture the data of the hopping signal.

Challenge #9: Troubleshooting the serial data connection

Data needs to get from the RF interface to a peripheral (i.e. PC or recorder) using some serial interface; typically this is implemented as a RS-232/422/485, SPI, or I^2C.

RS-232 asynchronous receiver module can be a problem spot. Ideally, you would like to see the data shifting every (serial) clock cycle and holding for a while after. Then, look at the data terminal ready (DTR) output, and confirm it is being asserted. Having DTR asserted at the right time is the number one issue in throughput from the reader to the PC.

Solution #9: DPO/MSO 4000 Series Oscilloscopes

The MSO4000 Series of Mixed Signal Oscilloscope adds 16 integrated digital channels to serve the needs of embedded system designers. In the RS-232 example mentioned above, one would connect the logic probes on the MSO4000 to RX data (or SOUT) which would indicate when the RFID chip is receiving data from the card. Using the digital analysis is also useful for making sure that the values in the buffer are what you expect them to be, as well as to check on the values of intermediate signals like the counter. The following modules will help with this. Simply use the one that matches the data connection you are using.

The DPO4COMP – Computer Serial Triggering and Analysis Module enables triggering on packet level information on RS-232/422/485/UART buses as well as analytical tools such as digital views of the signal, bus views, packet decoding, search tools and packet decode tables with timestamp information. The DPOEMDB Embedded Serial Trigger and Analysis Module enables triggering on packet level information on I^2C and SPI buses as well as analytical tools such as digital views of the signal, bus views, packet decoding, search tools and packet decode tables with timestamp information.

For more information see the Tektronix application note: Debugging Low-Speed Serial Buses in Embedded System Designs (48W-19040) available at www.tek.com.

- DPX uncovers the problem
  - Signal appears to spend time offset from final carrier frequency during a hop
- Frequency Mask Trigger captures the problem
  - Capture just the data around the hop, every time
- Measure the problem
  - Signal source analysis capability measures setting time, frequency excursion

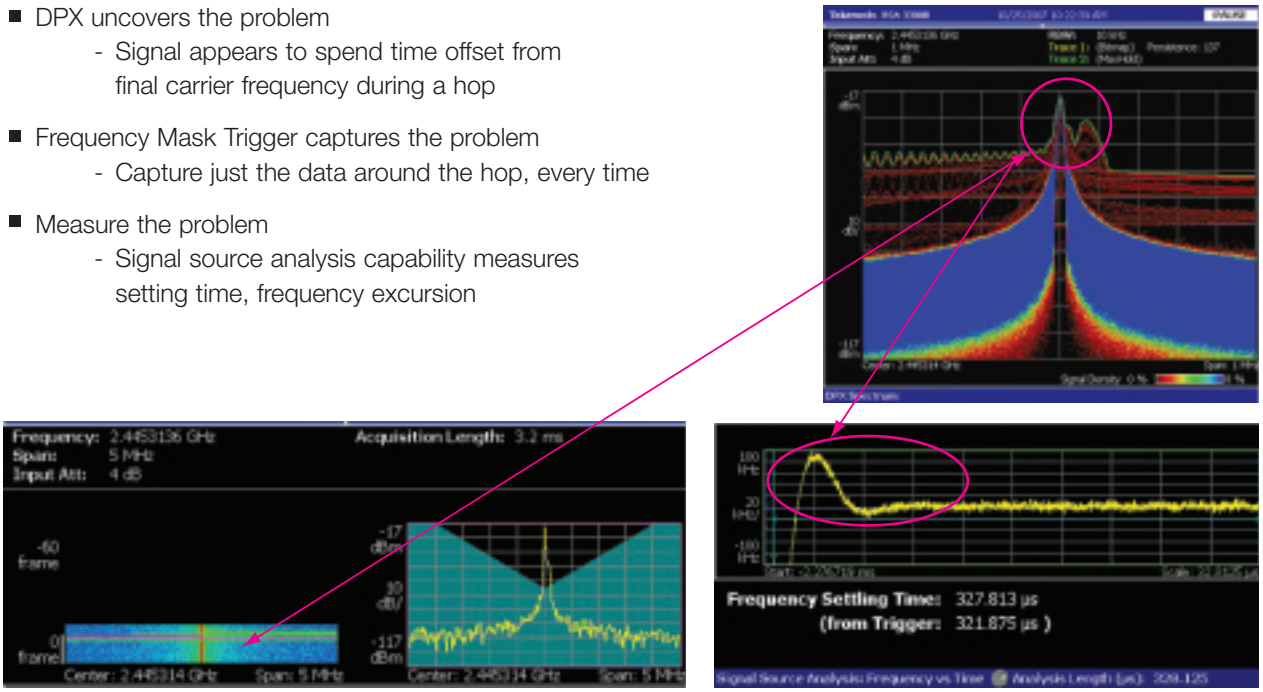


Figure 26. Process for evaluating PLL behavior using DPX, FMT and Signal Source Analysis.

Challenge #10: Troubleshooting the embedded design RFID transceiver

Embedded design was touched on in Challenge #9 but only in regards to serial data connections. Embedded design extends far beyond this application; there are critical digital and analog components at every stage of the RFID transceiver. For example, the Phase Locked Loop (PLL) can experience significant drift over when transmitting a long string of bytes. A *sample and hold* technique is sometimes utilized in the PLL to address this. Another example is that bit clock/sample clock phase coherency can be an issue, especially important when implementing a phase-reversed ASK (PR-ASK) modulation approach. One solution to ensure coherency is to use the Timer/Counter 0 as Carrier divider. This allows a falling edge of demodulated data (usually the first edge) to reset the counter and allows the sample clock to be in synch with the bit clock.

Earlier we discussed using the RSA3000B to discover if and when an RFID reader is violating the spectral emission masks set by the FCC or ETSI requirements. The solution for this is often implemented in baseband filtering and pulse shaping.

Solution #10: Utilize a Mixed Signal Oscilloscope (MSO) and the differential basband inputs on the RSA3000B

Three examples of an embedded design challenge were raised: PLL stability/drift, bit clock/sample clock phase coherency, and baseband filtering/pulse-shaping; these are only a few of the number of challenges that the RFID embedded design engineer faces every day. It's far beyond the scope of this application note to touch on them all, so let's discuss the ones mentioned to provide an overview of a solution which can be applied to a number of challenges.

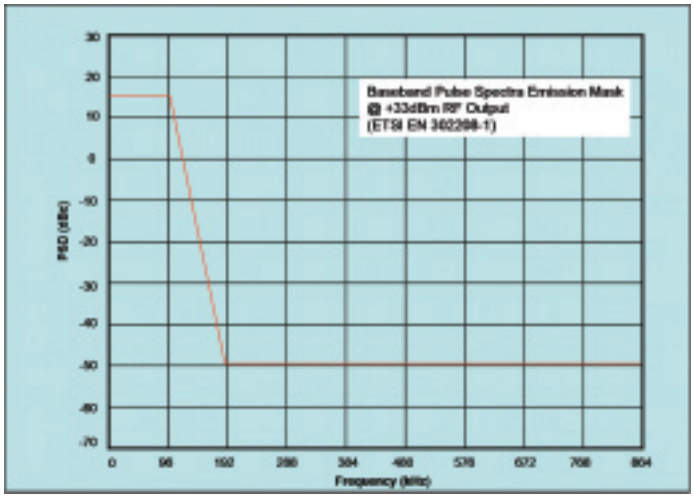


Figure 27. Baseband PR-ASK pulse spectra.

For the PLL example, the signal analysis mode on the RSA3000B can be utilized to perform phase noise and jitter analysis as well as making automatic settling time measurements. PLL behavior may be evaluated at RF frequencies or in the analog baseband utilizing the RSA3000B differential baseband inputs (I+, I-, Q+, Q-).

In the sample-and-hold solution listed above, the MSO could be configured to trigger on any hold violations. The trigger output signal from the MSO could be connected to the trigger input on the RTSA and allow for correlating any setup/sample/hold violations implemented in DSP to the result in the RF signal. The RSA3000B also offers a trigger output so that this could be performed in the opposite configuration with any frequency hopping violations (discovered using the Frequency Mask Trigger) on the RTSA triggers an acquisition of the DSP signaling.

The same triggering arrangement could be arranged for verifying bit clock/sample clock phase coherency, whereby the timer/counter is monitored using the MSO and each frame from the reader triggers it and the RTSA (tying together the triggers and 10 MHz time bases). Any violations could be seen as an 'x' in the symbol table measurement on the RSA3000B and this could be correlated to see if it were due to bit/ample clock errors. Especially telling would be an instance where the data bits are accurate initially and then start to become unstable (displayed as an unexpected 'x' in the symbol table), or reverse completely to the opposite bit (e.g. a '1' where a '0' is expected or vice versa).

Many RFID IQ modulators use a low pass filter between the digital-to-analog converter (DAC) and the modulator input to attenuate the sampling images from the DAC. Step one in verifying baseband filtering is to verify the corner frequency, as it will often vary depending on the sampling frequency of the DAC. This can be done with either a scope or using the baseband inputs on the RSA3000B, which offer extremely good dynamic range and frequency measurements from DC (0 Hz) to 40 MHz. This dynamic range is especially useful for the second step, which is to ensure that any pulse shaping utilized meets the demanding ETSI EN302208-1 spectral mask. The mask requires that baseband pulse spectra be attenuated as shown in Figure 27.

This 65 dB of dynamic range is achieved using the 14-bit A/D found in the RSA3000B. If necessary, it is possible to use probes connected to the RTSA using the Real-Time Spectrum Analyzer TekConnect® Probe Adapter (RTPA2A).

This pulse shaping is typically achieved digitally using a FIR filter in the DSP which drives the DAC. The MSO4000 can be used to monitor up to 16 digital channels to ensure the DSP signaling is correct. If more digital capability is required, a logic analyzer such as the TLA5000 Series should be used.

Conclusion

The Tektronix RSA3000B Real-Time Spectrum Analyzer delivers unique solutions and advantages for designers working with RFID signals of all kinds. Only the RSA3000B Series offers frequency selective triggering, deep memory storage, multiple acquisition capability, and analysis features to help designers understand the full range of RFID interrogator and transponder behavior. Along with Tektronix Arbitrary Waveform Generator and Oscilloscope offerings, the RTSA offers a comprehensive solution that can stay current with emerging trends in RFID design.

Contact Tektronix:

ASEAN / Australasia (65) 6356 3900
Austria +41 52 675 3777
Balkans, Israel, South Africa and other ISE Countries +41 52 675 3777
Belgium 07 81 60166
Brazil & South America (11) 40669400
Canada 1 (800) 661-5625
Central East Europe, Ukraine and the Baltics +41 52 675 3777
Central Europe & Greece +41 52 675 3777
Denmark +45 80 88 1401
Finland +41 52 675 3777
France +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) 5424700
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) 6917-5000
Russia & CIS +7 (495) 7484900
South Africa +27 11 206 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

Updated 12 November 2007

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**

05/08 EA/PDF 37W-19258-1

Tektronix®