

Advanced RFID Measurements: Basic Theory to Protocol Conformance Test

Overview

As RFID adoption continues to grow, the need to validate tags for interoperability with products from other vendors and for conformance with the specified protocol is increasing. Today's market also drives the mounting pressure to improve tag performance. RFID system designers face a significant test challenge when attempting to meet the needs of this emerging market. Fortunately, the demand for RFID technology has spawned both significant industry growth and innovation. In fact, scientists in the research and commercial environments have often chosen National Instruments measurement tools to characterize both tag and reader performance.

Introduction

This application note explains both the basic functionality of RFID systems and the measurements that are commonly made. It explores some of the key technical design and implementation challenges RFID design and test engineers face. In addition, it provides insight into how customers have used measurement systems based on PC-based modular instruments in researching and developing RFID products.

While many of the principles discussed are broadly applicable to all RFID standards, this article mainly focuses on the ISO 18000-6C (Class 1, Gen 2) specification [1]. This standard addresses UHF RFID in the bands from 860 to 960 MHz, and is commonly used in applications ranging from supply chain to baggage tracking in airports. This application note has five sections:

1. RFID theory of operation
2. Introduction to tag testing methodology
3. Tag and antenna characterization
4. System protocol and conformance test
5. RFID products and third parties

Each section provides theoretical background and practical measurement tips and techniques. Use this document to gain comprehensive knowledge about RFID measurement systems and a more detailed understanding of the ISO1800-6C specification. While several unique architectures for RFID measurement systems are examined, the discussion primarily focuses on results from the VISN-100 RFID tester, illustrated in Figure 1.

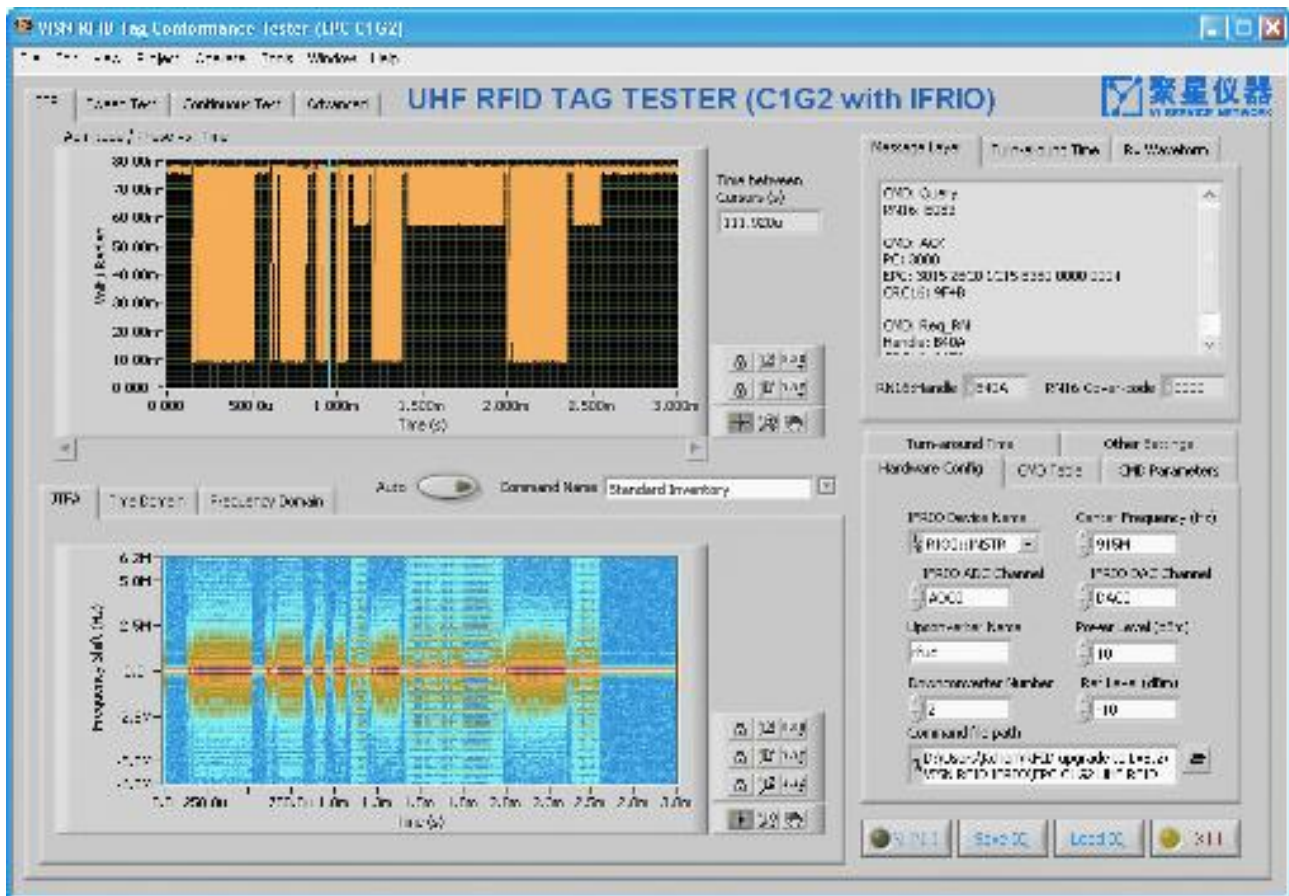


Figure 1. Screenshot of the VISION-100 RFID Measurement System

The heart of this measurement system is the NI PCI-5640R IF transceiver, which uses NI LabVIEW FPGA Module code to fully emulate either a tag or reader. The VISION-100 RFID measurement system is the preferred solution for RFID testing because it provides both PHY layer and protocol layer measurements in an out-of-the-box package. In addition, because this system is purely software-defined, it is also user-configurable for custom measurements and analysis.

Part 1: RFID Theory of Operation

RFID tags come in a broad range of shapes and sizes depending on the frequency range and antenna design. As a general rule, the decision to use one tag over another depends on several factors including physical environment, required read range, and even the physical properties of the material that you are tagging. For an idea of how RFID frequency bands can affect read ranges, see Table 1

	Frequency	Range	Example Standard
LF	125 kHz	Less than a foot	ISO 18000-6A
HF	13.56 MHz	Up to 3 ft	ISO 18000-3

UHF	850 to 950 MHz	30+ ft	ISO 18000-6C
Microwave	2.4 to 2.45 GHz	100+ ft	ISO 18000-4

Table 1. Comparison of the Typical RFID Read Range According to Frequency Band (Passive Tags)

While Table 1 compares the read range of passive tags, note that there are actually three RFID tag types: active, passive, and semiactive. Because active and semiactive tags use an onboard power source to power the tag response, they are typically capable of much longer read ranges. Passive tags, on the other hand, are actually powered by electromagnetic energy from an interrogator's command. This technique significantly lowers the cost of the tag, but it also limits the read range and creates significant – but interesting – design challenges. For example, RFID tags specified by the ISO18000-6C standard are passive tags.

Tag-to-Reader Interaction: The Inventory Round

An RFID system consists of a tag reader (also called the interrogator) and a tag. All communication between the tag and reader occurs completely through a wireless link that is sometimes called an air interface. Through a sequence of commands sent and received between both devices (called the inventory round), an RFID reader can identify the electronic product code (EPC) of an RFID tag. For passive tags, the basic idea is that the interrogator initiates an interrogation round with a query command. The query command essentially “wakes up” the tag, which responds with the appropriate information. Figure 2 shows a basic block diagram of the tag/reader system.

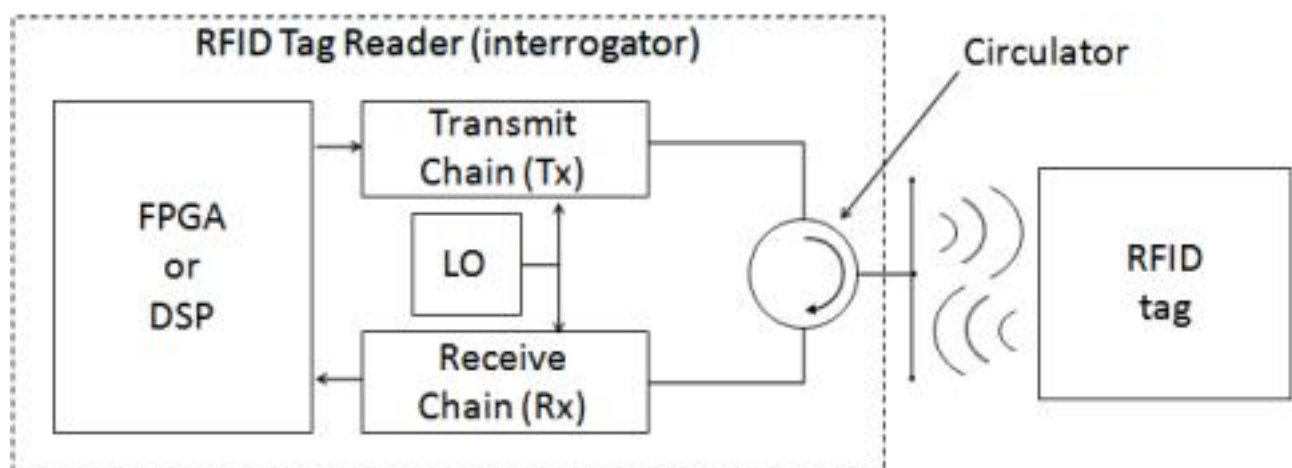


Figure 2. Block Diagram of a Typical RFID Tag/Reader System

Note from Figure 2 that many RFID readers and measurement systems actually use a three-port RF component called a circulator that gives both transmit and receive front ends the ability to use the same antenna. Note that with many RFID, standards, timing information between transmit and receive commands

is defined by strict guidelines. In fact, a sort of “handshaking” is required between the tag and reader to complete an interrogation round. This actually creates a unique test challenge because the instrumentation must be capable of the same behavior. On an interrogator, an embedded processor is required to decode and generate commands within a tight timing interval. As discussed in a later section, this design is quite similar to field-programmable gate array (FPGA)-enabled RFID measurement systems, which use similar embedded processing to fully emulate either a tag or a reader.

UHF Antenna Characteristics

One of the most elusive goals of RFID design is the challenge of extending a tag’s read range. At UHF frequencies, this challenge is particularly daunting because a tag’s electromagnetic properties (which determine performance) can be substantially affected by properties of the material on which the tag is applied. In general, two of the most important factors that affect a tag’s read range include efficiency of the antenna and impedance matching between an antenna and chip (or inlay) [2][3][4][6]. For reference, observe the basic design of a UHF RFID tag, shown in Figure 3.

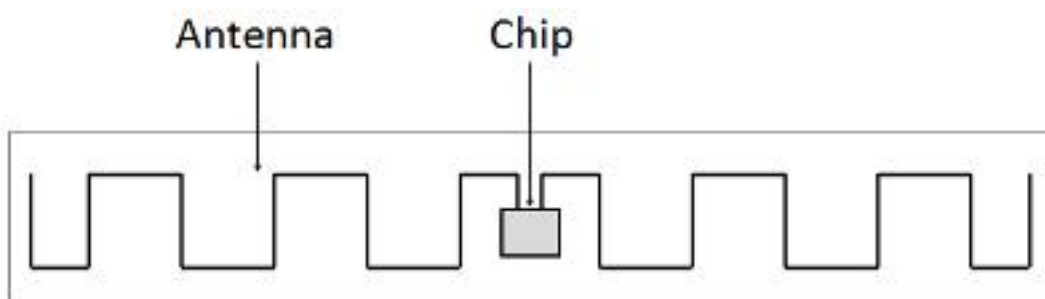


Figure 3. Basic Design of a UHF RFID Tag

The specific tag design shown in Figure 3 is known as the meandering trace design [2]. In some cases, you can tune the resonant frequency of this particular design simply by clipping the trace length [6].

One interesting characteristic of RFID antennas is that they often have impedance that is highly reactive. When a reactive substance is stimulated with an electromagnetic wave, a tag actually reradiates the same electromagnetic wave back at its source. This characteristic of the antenna is actually helpful in RFID systems because it provides the tag with a straightforward mechanism to send an electromagnetic wave to the source without the need of an onboard synthesizer. This method is called backscattering.

Antenna design of RFID tags has already been the subject of significant research. More specifically, this research has examined techniques to tune antennas for operation over a broad frequency range [3]. This document does not describe the design trade-offs that must be made to maximize a tag’s read range. Instead, it examines the measurement techniques that you can use to characterize various aspects of a tag’s performance.

Backscattering

The principle of backscattering is one of the most intriguing technologies in the RFID theory of operation. Because of this technique, a tag is able to respond to interrogator commands without the aid of an external power source. It is perhaps easiest to understand this technique by stepping through each stage of reader-to-tag (R->T) and tag-to-reader (T->R) communications.

Step 1: Interrogator (R) Sends a Command to the Tag (T)

The first step of the interrogation round is an interrogator-to-tag (R->T) transmission. The digital message data is typically encoded according to one of several common schemes including Manchester (ISO 14443) and pulse-interval encoding (PIE) (ISO 18000-6C). The encoded message is then modulated with one of several variants of the amplitude shift keying (ASK) modulation scheme. For example, with the EPC Class 1, Gen 2 (ISO 18000-6C) standard, readers can use any of the double-sideband ASK (DSB-ASK), single-sideband ASK (SSB-ASK), and phase-reversal ASK (PR-ASK) options. Of these three options, note that PR-ASK is one of the most interesting. This scheme uses a combination of 180 deg phase transitions every symbol and a 100 percent modulation depth to provide the lowest C/N requirement for error-free communications.

Step 2: Command Decoding

Once the interrogator transmits a command, the electromagnetic wave propagates in free space toward the tag. When the wave reaches the tag, the tag's antenna is excited and the RF power is converted to DC power through a voltage rectifier. This DC voltage is then able to power the control logic (often employed with a state machine) on the chip, which demodulates the waveform and determines the appropriate next command. A functional block diagram of the chip is illustrated in Figure 4.

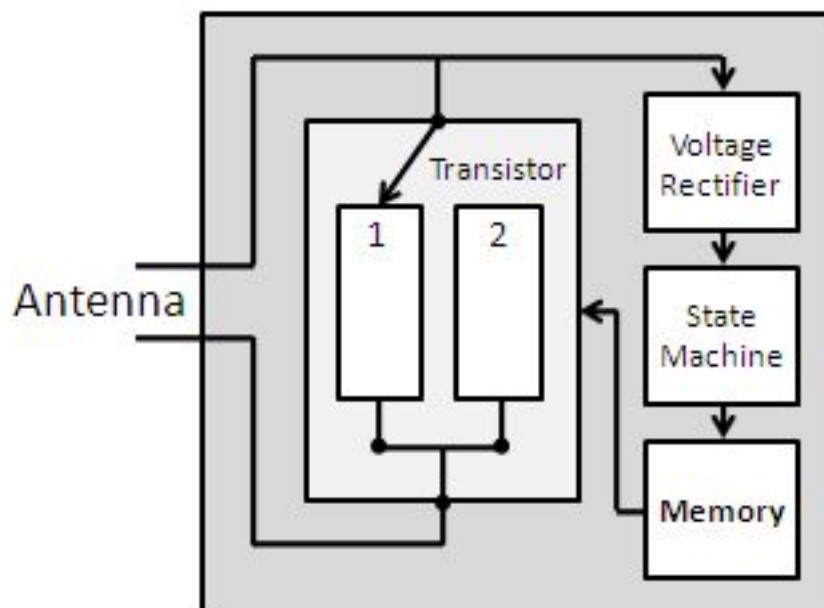


Figure 4. A Functional Block Diagram of an RFID ASIC (inlay)

The chip is also called the “inlay,” and it can be broken down into several functional blocks. The voltage rectifier converts an electromagnetic wave to DC power. The control logic/state machine determines the next command to be sent to the reader. Finally, the transistor enables modulation of the reradiated electromagnetic wave.

Step 3: Reradiation of Electromagnetic Wave

One of the most fascinating aspects of passive RFID tags is the method of remodulating an interrogator command through backscattering. Because RFID tags are designed to have a reactive (capacitive) impedance, any incoming electromagnetic wave is actually reflected (reradiated) by an antenna to its source. Thus, when the interrogator transmits an electromagnetic wave to a tag, the wave is reflected by the tag back toward the transmitter. Because of this characteristic, a tag is able to encode a message by modulating the reradiated electromagnetic wave. Actual modulation of this wave occurs as a transistor on the inlay rapidly switches between two discrete impedance states. Because each impedance state has both a resistive and capacitive characteristic (real and imaginary impedance), the tag actually performs both phase and amplitude modulation of the reradiated signal. Thus, the interrogator receives a signal characterized by phase and amplitude modulation of the original R->T transmission. Note that backscattering has motivated significant research into the optimal tag radar cross section (RCS) characteristics. This is discussed in detail in Part 3.

Understanding the RFID theory of operation and backscattering is critical to understanding the concerns and considerations in tag design. As an example, the nature of the tag's dual phase and amplitude modulation scheme produces interesting reader design decisions. While a reader can demodulate a tag response with a simple ASK demodulation algorithm, read range can be improved by analyzing the phase changes as well. This technique requires transmit and receive portions of an interrogator to share the same local oscillator (LO).

Part 2: RFID Test Instrumentation

Both RFID tags and readers have unique test requirements, which creates a significant test challenge for today's engineers. In fact, design validation of today's RFID tags requires special attention to both conformance and interoperability testing. As an example, the ISO 18000-6C (Class 1, Gen 2) standard allows for significant variation between readers. Some of the specifications that are flexible include allowable data rates, modulation schemes, and even RF envelope characteristics. Thus, reader emulation is often required for design validation to ensure that a tag is functional across many permutations of the standard.

In general, you can divide tag validation into two basic types: (1) physical (PHY) layer measurement and analysis, and (2) conformance and protocol validation. While you can perform many PHY layer measurements with software-defined instrumentation and appropriate measurement algorithms, full reader emulation is required for conformance and interoperability testing. In general, NI recommends a system capable of full reader emulation because it can address all measurement needs. However, based on the specific testing needs mentioned above, there are several instrument configurations that you can use for

RFID testing. This next section explains how to architect each type of measurement system and the trade-offs between them.

RFID “Sniffer” Architecture

The most basic RFID tag test system uses a vector signal analyzer to “sniff” the air interface between an interrogator and a tag. This system, illustrated in Figure 5, uses a reference “gold” reader or RFID simulator to initiate an interrogation round with the tag. Meanwhile, the RF vector signal analyzer is used to record and analyze both tag and reader transmissions over an RF air interface.

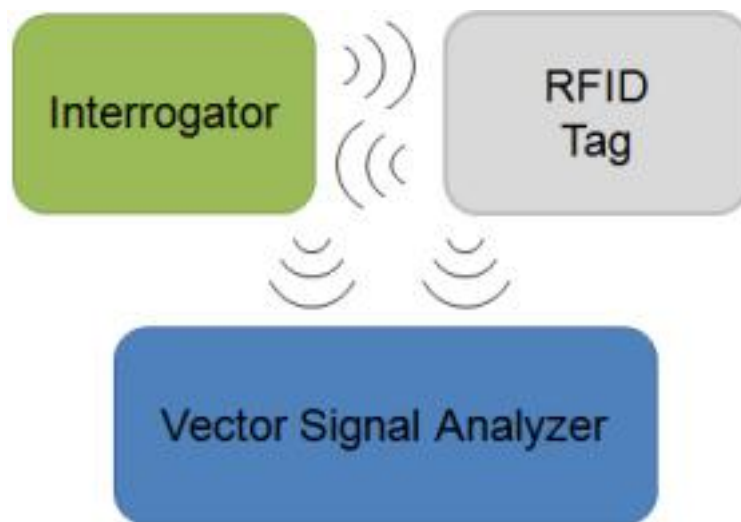


Figure 5. Illustration of a Generic RFID Test Strategy

In this test scenario, the vector signal analyzer is configured with an RF power trigger to capture all transmissions between the interrogator and tag. Many modern vector signal analyzers, such as the NI PXI-5661, offer the capability to perform frequency-domain triggering. Using the measurement configuration described above, RF transmissions are analyzed in both the time and frequency domains for full analysis of tag-to-interrogator transmissions. While you can use this technique to perform basic PHY layer characterization of either the tag or the reader, you cannot use it for interoperability or conformance testing. In fact, characterizing a tag with this method would require a large number of “gold” readers to emulate the full breadth of the RFID standard.

Stimulus-Response Architecture

A second implementation of an RFID test system is the simple stimulus-response architecture. In this configuration, the “gold” interrogator is replaced with a vector signal generator. The generator is able to generate a single “query” command while simultaneously sending a digital marker trigger to a vector signal analyzer. Upon receiving the trigger, the vector signal analyzer captures the RF signal for further

analysis. Note that this implementation is common because measurements are easily automated and can be made with significant predictability [4][7][8][9].

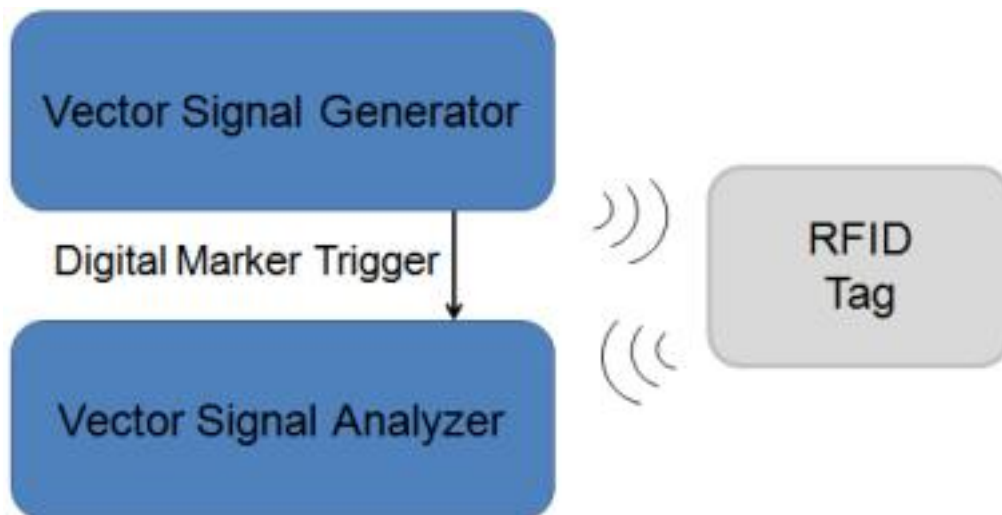


Figure 6. Host-Based Processing RFID Test System

Using the stimulus-response method, you can perform conformance testing in much the same way as in the “sniffer” architecture. However, the stimulus-response method has one additional benefit – it can emulate a wide variety of interrogator-to-tag commands. Because each command is created in software, use of a vector signal generator gives you the ability to modify PHY layer characteristics such as data rate and center frequency. The disadvantage of the stimulus-response method is that you can use it only to emulate the first command of an interrogation round, so you cannot use it for protocol conformance. For protocol conformance test, real-time tag response for a complete interrogation round is critical. This type of measurement system is described in the next section.

Real-Time Interrogator Emulation

The final and most sophisticated approach to tag or reader testing is the complete emulation of either a tag or reader. In this scenario, the RF instrumentation is able to send and receive commands in much the same way that an actual tag or reader does. As a result, you can use the instrumentation to conduct both PHY layer measurements and perform complete protocol validation.

Protocol testing includes analysis such as state machine validation and link timing measurements. While it is often possible to do this by creating a custom interrogator, the easiest approach is to use an out-of-the-box RFID tester that uses FPGA-enabled instrumentation. With FPGA-enabled instrumentation, a real-time baseband processing engine ensures that the system can decode and retransmit commands within several microseconds. The VISA-100 is one example of an FPGA-enabled instrumentation system.

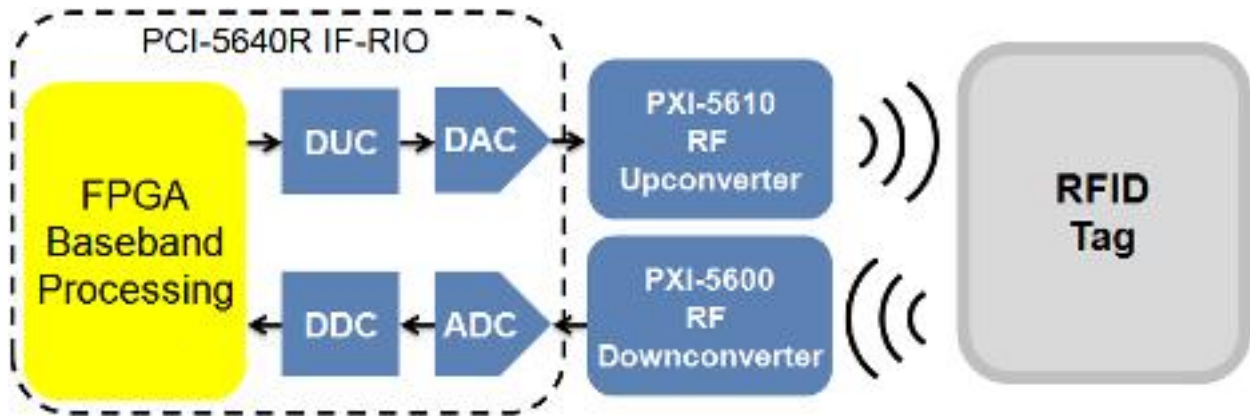


Figure 7. Use the PCI-5640R for real-time baseband processing.

As Figure 7 illustrates, the RFID modulation and demodulation algorithms are implemented in FPGA hardware to ensure that the instrumentation can fully emulate a tag or reader. In the case shown above, the algorithms are coded in the NI LabVIEW FPGA graphical programming language. Once compiled as VHDL, all measurement algorithms can be executed in real time on the dedicated hardware platform. The key component of the system in Figure 7 is the PCI-5640R IF transceiver [9].

Part 3: Tag and Antenna Characterization

One of the perpetual challenges of RFID tag design is the requirement to maximize tag read range across a broad range of frequencies or on a broad range of deployed objects. Overall, tag read range is determined by several factors including antenna gain, effective area, and impedance matching between the inlay (chip) and the antenna. In some cases, many of these characteristics are also affected by the substrate on which the tag is applied. Thus, various organizations, including the University of Pittsburgh RFID Center of Excellence and Oden Technologies, serve the RFID community by providing a range of consulting services [8][10][11]. In this scenario, a firm wanting to use RFID technology asks a consultant to help determine factors such as ideal frequency usage and best tag placement for a particular application.

To understand the challenges of tag read range performance, first take a look at theoretical tag performance. To start with, you can express the total power collected by a tag's antenna in free space according to the following equation.

$$P_a = \left(\frac{P_t G_t}{4\pi r^2} \right) \left(\frac{\lambda^2}{4\pi} \right) G_{tag}$$

Equation 1. This equation shows antenna power affected by antenna gain, wavelength, and distance [2].

As Equation 1 illustrates, the power available at an antenna, P_a , is a function of various factors including the

power and gain (efficiency) of the transmitter antenna (P_t and G_t), the distance from the transmitter (r), electromagnetic wavelength (λ), and gain (efficiency) of the RFID tag's antenna (G_{tag}). The obvious conclusion from Equation 1 is that to improve read range (r) without increasing transmit power, you must improve the gain of the RFID antenna. As a result, characterization of RFID tags often involves significant characterization of the antenna over a wide range of frequencies [4][5][7].

Tag and Inlay Impedance Design Decisions

On the RFID tag reader side, reradiated power is also important. In general, more efficient reradiation of electromagnetic waves translates to easier dynamic range requirements on the RFID reader. Note that reradiated power is also influenced by factors such as antenna gain and tag-antenna impedance matching. This is illustrated in the equations below, which express reradiated power as a function of several factors:

$$P_{re-radiated} = \left(\frac{4R_a^2}{|Z_a + Z_c|^2} \right) P_a G_{tag}$$

$$K = \frac{4R_a^2}{|Z_a + Z_c|^2}$$

Equations 2 and 3. These equations show antenna power affected by antenna gain, wavelength, and distance [4].

As you can observe from Equation 3, reradiated power is highly dependent on the impedance matching between the inlay and the tag's antenna. In Equation 3, Z_a represents the impedance of the antenna and Z_c represents the impedance of the chip (inlay). From this equation, you can see that when the impedance of the antenna is zero (short circuit), the tag reradiates four times as much power as a matched antenna. On the other hand, when the antenna impedance is highly reactive (capacitive), a complex conjugate loaded antenna actually reradiates more power than an antenna with zero impedance [4]. While this paper does not explore these trade-offs in-depth, it is worth noting that design decisions such as choice of antenna and inlay impedance/reactance can have a significant impact on tag performance. To examine these trade-offs in-depth, read [Theory and Measurement of Backscattering from RFID Tags](#) by Nikitin and Rao [4]. In their article, they not only detail the trade-offs between various combinations of antenna and inlay impedance but also characterize tag performance across the frequency range. You can find a description of the measurement system in the case study [Using National Instruments Software and Hardware to Develop and Test RFID Tags](#) by Pavel V. Nikitin of Intermec Technologies Inc. [12].

Relationship between Read Range and Antenna Gain

You can improve read range by improving the efficiency of the RFID tag's antenna, but other factors can affect read range as well. Thus, maximizing read range has been the subject of much research. To investigate this subject, first evaluate a theoretical calculation of read range, which is illustrated in Equation 4.

$$Range_{max} = d \sqrt{\frac{EIRP}{P_{tag_min} G_{tag}}}$$

Equation 4. This equation shows read range as a function of distance and equivalent isotropic radiated power (EIRP) [3].

In addition, the theoretical read range can be described in greater detail according to the equivalent power and gains from each of the antennas involved in the transmission. In greater detail, you can represent the range with the following equation:

$$Range_{max} = \frac{\lambda}{4\pi} \sqrt{\frac{P_{tag} G_{tag_min} G_{receiv_tag_min} \tau}{P_{tag_min}}}$$

Equation 5. This equation shows read range as a function of distance, power, and gain [4].

In Equation 5, the Tau (τ) is the same K factor from Equation 3. Note that while you can theoretically estimate the read range as a function of wavelength (λ) and various power and gain coefficients, practical measurements for read range are more difficult. In fact, tag and chip impedance are only two of several factors that affect read range [2][3][4].

One motivation for RFID consulting services is that a deployed tag's substrate can often substantially affect read range [8][10][11]. In other words, a tag tuned to a frequency of 915 MHz might have a read range of 4 m on one object and a read range of 3 m on another object, even if the interrogator's transmission in both scenarios has the same EIRP. The reason for this behavior is that the read range is greatly determined by the impedance of the tag's antenna and chip (as noted in the Tau, τ , factor of Equation 5). Unfortunately, the impedance of the tag's antenna can be affected by the substrate on which it is applied. Because impedance is one determining factor of the resonant frequency of an RFID tag, changes in impedance can drastically affect the read range. Thus, practical use of RFID systems often requires substantial testing to ensure that the tag produces the desired read ranges when applied to the various mediums.

Because the read range of an RFID system is highly dependent on the impedance of the tag, chip, and substrate, RFID system designers often employ one of several techniques to tune a specific tag so that it is optimized according to substrate and frequency. Rao, Nikitin, and Lam explore the technique of tuning a tag by clipping the ends of the antenna. You can use other techniques as well. Some tag manufacturers

intentionally design RFID UHF (915 MHz) tags with a resonate frequency that is well over 100 MHz higher than the operational frequency. In other instances, researchers have explored techniques that can be used by a tag or reader to dynamically retune the resonate frequency of a tag.

Characterization of Power versus Frequency

This application note covers the mechanisms used to optimize read range, but it is important to emphasize that a wide range of factors can influence a tag's performance over a broad range of frequencies. For this reason, one of the most common measurements used in tag characterization is basic power versus frequency analysis. You can achieve simple measurements of a tag's power versus frequency with either a vector signal generator/vector signal analyzer combination or with a complete RFID emulation measurement system. In this configuration, both the RF generator and analyzer are swept through a range of frequencies. At each step, the power of the tag response is measured at each discrete frequency.

Part 4: Protocol and Conformance Test

While you can use extremely basic physical (PHY) layer measurements to characterize the RF performance of an RFID tag or reader, additional validation is often required for conformance test. In this method of testing, tag or reader commands are demodulated and the returned bitstream is evaluated. In general, you should perform both protocol and conformance testing with a combined RFID measurement and emulation system. This system, which uses an FPGA to perform real-time baseband processing, is able to concurrently emulate a tag reader while performing PHY layer measurements. This discussion of protocol and conformance test is divided into three sections:

- PHY layer conformance test
- Demodulation of backscatter
- Emulation-based protocol testing

PHY Layer Conformance Test

You can test both standard conformance and multivendor interoperability by emulating various interrogator-to-tag parameters. The ISO 18000-6C (Class 1, Gen 2) is extremely flexible in the range of modulated signals that an RFID tag is expected to decode. For example, Section 6.3.1.2 of the EPC Class 1, Gen 2 air interface specifications permit interrogators to use either double-sideband ASK (DSB-ASK), single-sideband ASK (SSB-ASK), or phase-reversal ASK (PR-ASK) modulation schemes. In addition, this section specifies that a tag should operate over a variable Type-A reference interval (Tari). This interval, which defines the duration of "Zero" symbol, can range from 6.25 to 25 μ s [1]. Finally, Section 6.3.1.2 also provides specific guidelines for minimum and maximum values for parameters such as RF envelope ripple, modulation depth, and many others. As a result of the standard's flexibility, tag validation and verification require tags to be tested over a wide range of stimulus conditions. Two of the most common parameters that

a tag must be tested for are the data rate and RF envelope of the interrogator-to-tag transmission.

RF Envelope Parameters

As shown in Figure 8, the various parameters of the RF envelop for ASK and PR-ASK reader-to-tag transmissions are strictly defined in the ISO 18000-6 Type C standard.

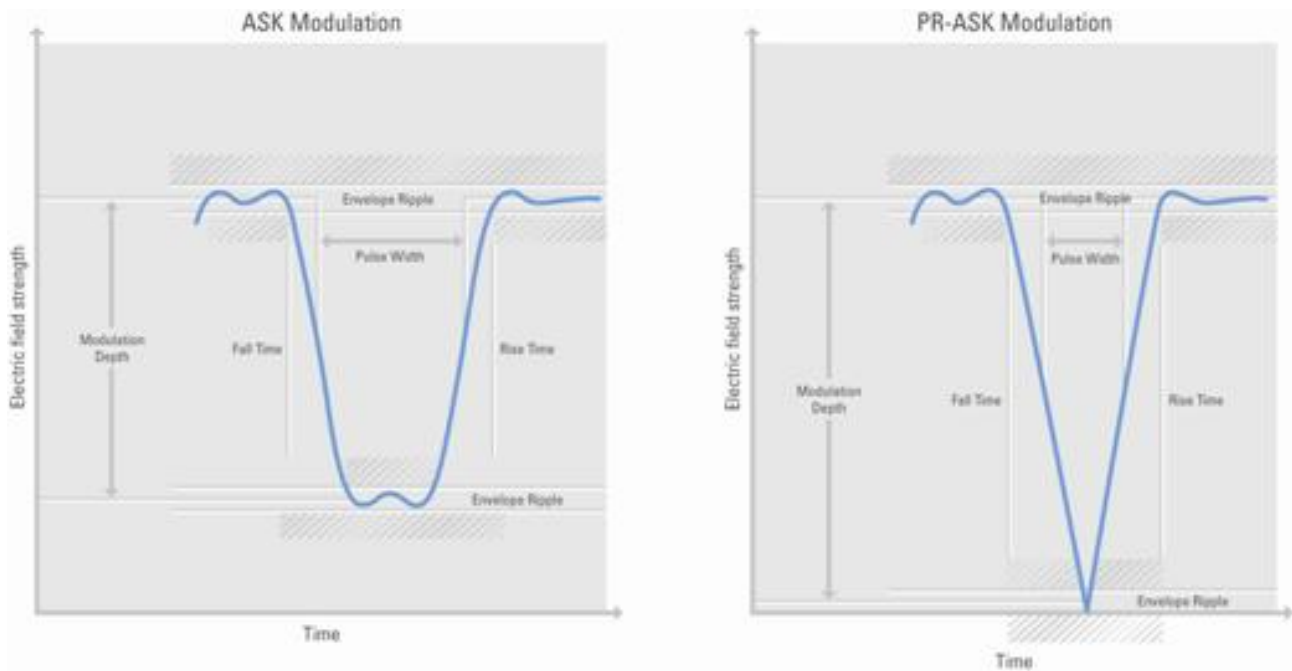


Figure 8. Specified Requirements for ASK Modulation in ISO 18000-6 Type C

According to Section 6.3.1.2 of the EPC Class 1, Gen 2 air interface specifications, the RF envelope of transmitter-to-tag transmission should adhere to the following characteristics:

Parameter	Minimum	Nominal	Maximum	Units
Modulation Depth	80	90	100	%
RF Envelope Rise Time	0	-	0.33 T_{ari}	μS
RF Envelope Fall Time	0	-	0.33 T_{ari}	μS
RF Pulse Width	MAX (0.265 T_{ari} , 2)	-	0.525 T_{ari}	μS

Table 2. RF Envelope Parameters of Interrogator-to-Tag Transmission [1]

To ensure that a tag is conformant, it must be tested through each permutation of the standard. One way to accomplish this is with a software-defined approach to command generation. By simulating parameters such as modulation depth and RF pulse width in software, you can validate that the tag is responsive to a broad range of conditions. In addition, because you can achieve this in an automated manner, you can quickly

make sure that the tag conforms with the standard.

Demodulation of Backscattered Baseband

To validate that the command response from a tag or reader is correct, you first need to demodulate the RF carrier. This section primarily focuses on the demodulation of T->R transmissions. With turnkey RFID solutions, such as the VISION-100 RFID tester, demodulation of commands is performed automatically by the software. Thus, this section is an academic exercise designed to promote a greater understanding for why tag radar cross section (RCS) is important.

As you see in the following sections, the combination of both phase and amplitude modulation in RFID tags requires designers to make trade-offs between the chosen impedance stances of the tag.

Demodulation of T->R transmissions is unique because of the backscattering demodulation technique. With this technique, an antenna collects an electromagnetic wave and then reflects it back toward the transmitter. As the electromagnetic wave is reflected toward the antenna, a transistor is switched rapidly between one of two impedance states. Because each impedance state has both a complex and imaginary characteristic, the resulting RF signal shows changes in both phase and amplitude. Thus, backscattered information from an RFID tag uses a modulation scheme that is a combination of phase-shift keying (PSK) and amplitude shift keying (ASK). To illustrate this, compare a typical constellation plot (Smith chart) of a backscattered RFID wave with that of ASK and PSK modulated waveforms.

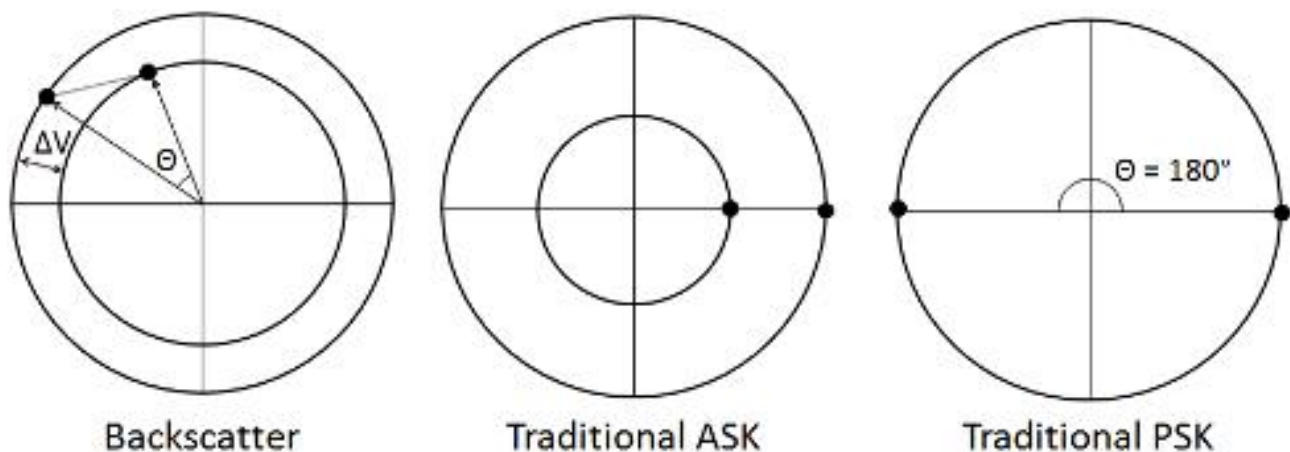


Figure 9. These illustrations show Smith charts of backscattered, ASK, and PSK waveforms.

Because the modulation type for RFID T->R communications is slightly nontraditional, software-defined instrumentation gives you the ability to implement custom demodulation algorithms to correctly decode the data.

Demodulation of the T->R transmission is actually something of a cross between ASK and PSK demodulation. At a high level, you can examine an algorithm for the demodulation of backscattering in Figure

10.

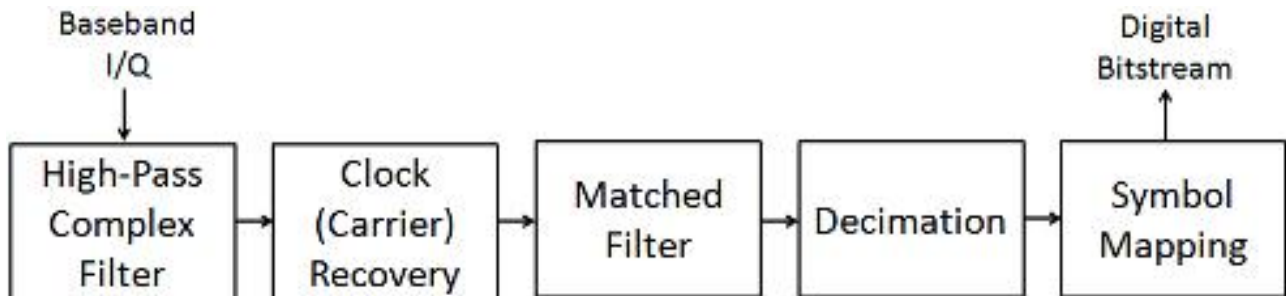


Figure 10. Demodulating Backscattered RFID

Note that the algorithm in Figure 10 is a modified version of a traditional PSK demodulator.

Step 1: Highpass Filter

The first step in demodulating backscattered data is to pass the baseband waveform through a highpass filter. By applying the highpass filter, any DC offset is removed, enabling the baseband waveform to be demodulated with a traditional PSK demodulator algorithm. Removal of the DC offset can be observed in Figure 11, and the resulting baseband waveform is shown to be centered around the origin of a Smith chart.

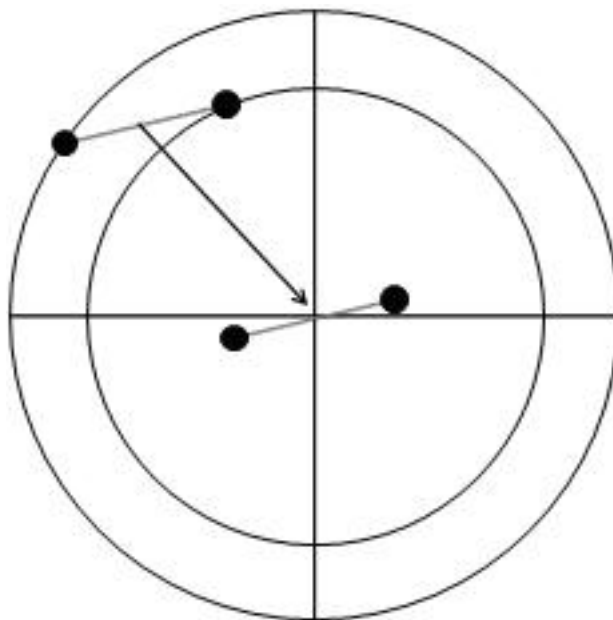


Figure 11. Role of Highpass Filter in Backscatter Demodulation

As you can see in Figure 11, filtered baseband matches the symbol map of binary phase shift keying (BPSK) and can be demodulated with a traditional PSK demodulation algorithm.

Step 2: Clock Recovery

Clock recovery is the second step in the demodulation of a backscattered carrier. This step is actually the first of the traditional PSK algorithm. In this phase, the baseband waveform is essentially resampled so that each symbol location aligns precisely with a baseband sample. Clock recovery, sometimes called a maximum likelihood algorithm, is often combined with the application of a matched filter.

Note that because both the transmit and receive chains of an interrogator share the same LO, it is typically not necessary to remove carrier frequency offset. Because the tag simply remodulates the carrier of the interrogator, both the interrogator-to-tag and tag-to-interrogator transmissions occur at precisely the same RF frequency. Thus, the only carrier offset present occurs as a result of the Doppler effect from a mobile tag. In most scenarios, this effect is not significant enough to greatly affect the signal demodulation.

Step 3: Decimation to Symbol Rate

Once each sample is aligned to ideal symbol locations, you can obtain the final symbols by decimating the waveform to the symbol rate. As a result of decimation, each sample of the resulting waveform has samples that correspond to two distinct states.

Step 4: Symbol Mapping

A digital bit is assigned to each sample based on its corresponding phase and amplitude. This is illustrated in Figure 12, which shows how each symbol is mapped to binary information.

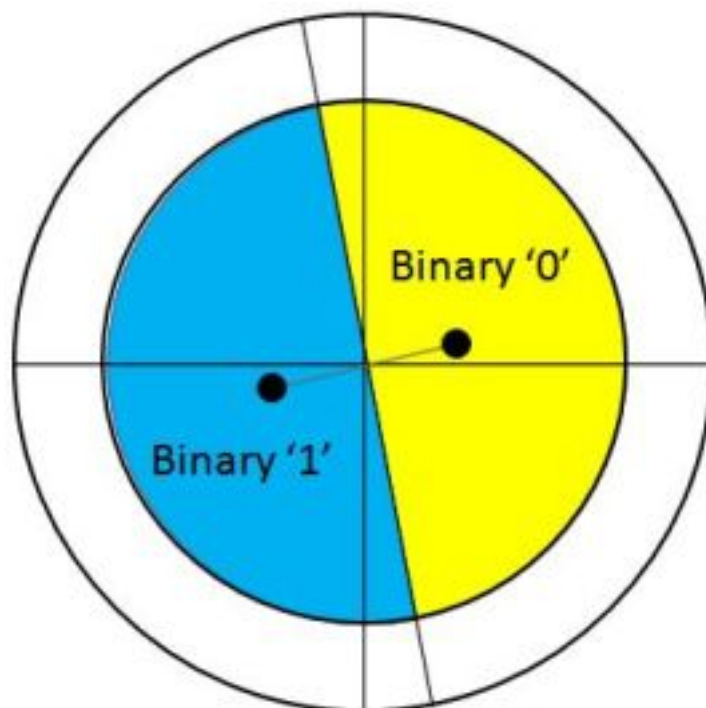


Figure 12. Graphical Representation of Symbol Mapping

Mathematically, symbol mapping is performed simply by comparing the phase of each complex symbol to a particular threshold. As you can see in Figure 12, symbols with a phase value between 100 and 280 deg are

assigned a digital value of 1, while all others have the digital value of 0. Once you map symbols to their corresponding binary values, you can use the appropriate channel decoding algorithm to return the raw message data from the encoded bitstream.

As a result of demodulating the tag-to-reader transmission, you can directly translate the resulting RF signal into a digital bitstream. This translation is a critical aspect of RFID protocol testing because it involves verification that the appropriate packets have been transmitted by the tag.

Protocol Testing with Reader Emulation

The combination of flexibility within RFID standards and the requirement for multivendor interoperability makes protocol testing an important stage of product development. For example, the ISO 18000-6 type C protocol gives both tags and readers the ability to operate with a broad range of variability. The standard enables an interrogator to send data at a variety of symbol rates. In addition, the same standard also requires the tag to respond to various interrogator commands within an allotted time period that is dependent on the original command. Finally, several RFID standards specify both optional and required commands that the tag and reader must support. For the purposes of this discussion, protocol testing is the process of validating that the tag is functionally compliant with the protocol being used. In the following discussion, all protocol testing has been completed with respect to the ISO 18000-6C standard. Though each standard has its unique nuances, the widespread adoption of this standard fuels the discussion below.

Note that on the instrumentation side, protocol testing requires that your RFID measurement system be capable of full reader or tag emulation. While you also can use a stimulus-response instrumentation system to measure basic PHY layer characteristics, protocol testing requires you to simulate an entire interrogation round between the reader and tag. Thus, it is crucial that your measurement system is capable of fully emulating a functional tag reader. In most cases, a “golden” tag reader is insufficient for this task because it cannot be programmed with the same flexibility as an instrumentation system. In addition, the use of a golden reader approach lacks the RF measurement capability of a vector signal analyzer.

The ideal approach to protocol testing is with a combined emulation and measurement system, such as the VISA-100 RFID tester from VI Service Network. As briefly discussed in the section on instrumentation systems, this product is based on the PCI-5640R RF transceiver. The transceiver features both IF input and IF output channels, which are connected to external upconverter (NI PXI-5610) and downconverter (NI PXI-5600) modules. One unique characteristic of this product is that both input and output channels are directly connected to a LabVIEW FPGA target. The FPGA conducts all baseband processing and, through real-time execution, is able to fully emulate and demodulate commands to and from an RFID tag. A block diagram of this is illustrated in Figure 13.

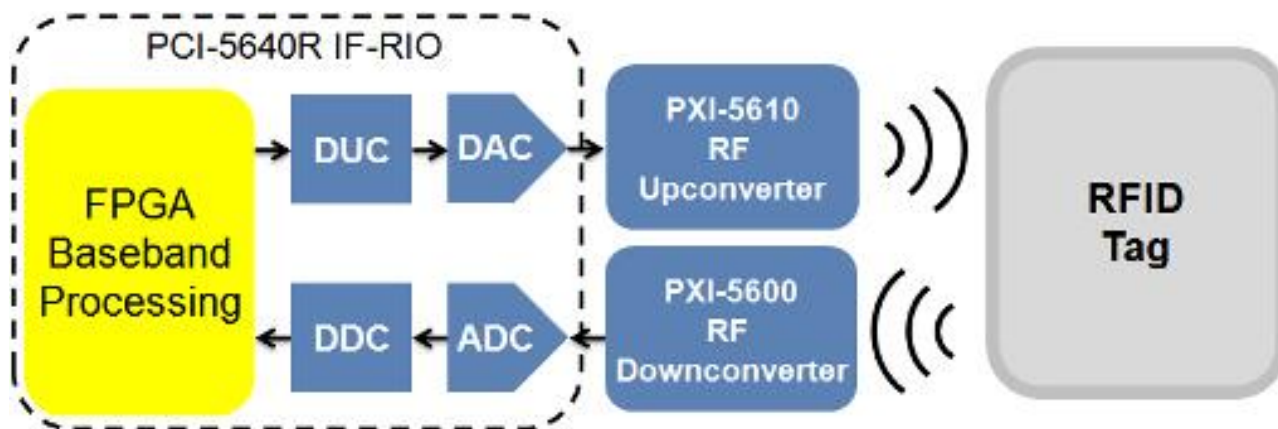


Figure 13. Use the PCI-5640R for real-time baseband processing.

With the baseband processing engine shown in Figure 13, the RFID measurement system is capable of simultaneously emulating an RFID interrogator and characterizing the tag's response. The following section describes how you can use this system for three unique protocol functional tests: data rate validation, link timing validation, and command set validation.

Data Rate Validation

According to ISO 18000-6C, specifications for a tag must be designed so that it can communicate with interrogators operating at a range of data rates. In addition, it specifies that RFID readers must use the same data rate for the duration of the interrogation round.

In the interrogator-to-tag transmission, interrogators use PIE to make demodulation easier within the tag. The basic premise of PIE is that different pulse intervals are used to represent a "0" and "1." This is illustrated in Figure 14.

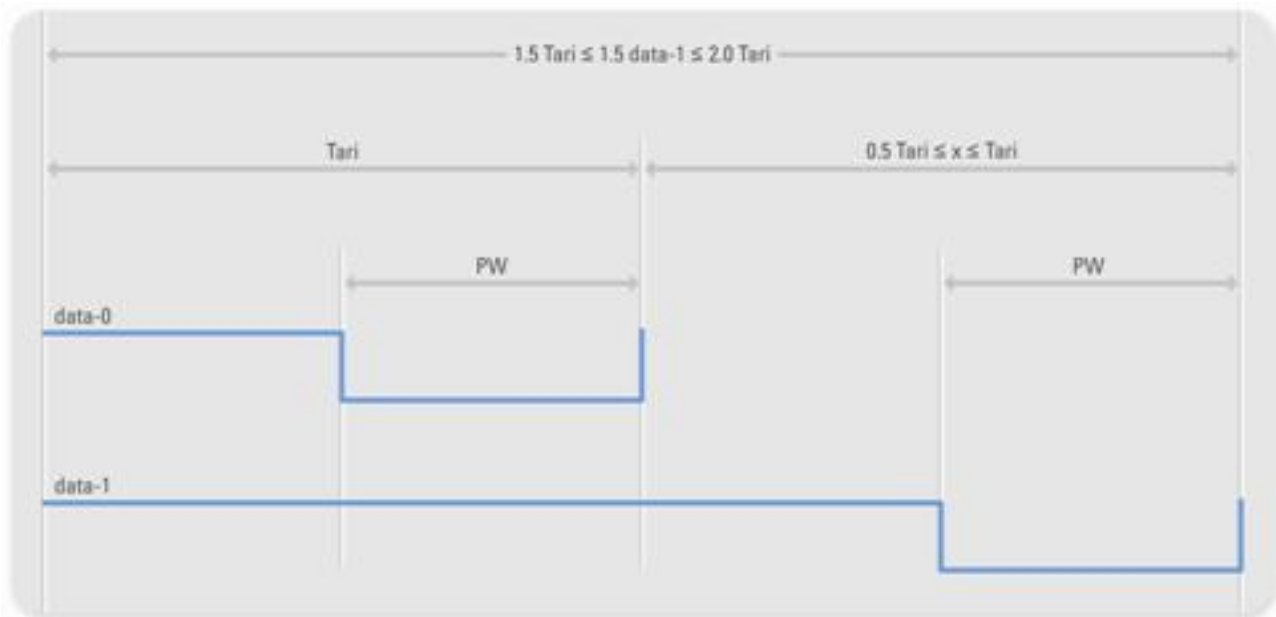


Figure 14. ISO 18000-6 Type C Timing Diagram

As shown in Figure 14, PIE uses variable pulse lengths to transmit digital information. Note that the data rate is often specified by the time interval required to transmit a zero bit when using PIE. As mentioned earlier, this value is known as the T_{ari} , or type A reference interval.

According to the ISO 18000-6C standard, tags are required to respond to commands whenever the T_{ari} value is between 6.25 and 25 μs [1]. Thus, multivendor interoperability testing requires that you validate a tag's performance across all potential data rates. In a typical test sequence, you can emulate multiple interrogators by performing a stimulus-response measurement for a range of T_{ari} values between 6.25 and 25 μs . For each T_{ari} step, you can both functionally validate that response and measure the PHY layer characteristics of the tag's response.

Link Timing Validation

One series of measurements that requires full emulation of the RFID interrogator is validation of the link timing characteristics. As specified by the ISO 18000-6C standard, the link timing specifications govern the maximum and minimum response times of a tag to a reader – and vice versa. To perform this measurement, it is important to simulate a complete interrogation round between the reader and tag. In this case, a simple stimulus-response measurement is insufficient because it is possible for the link timing to vary from one command to the next. Thus, to validate that the link timing is within spec for all communications between the tag and reader, it is important to simulate an entire interrogation round. An example of this is illustrated in Figure 15.

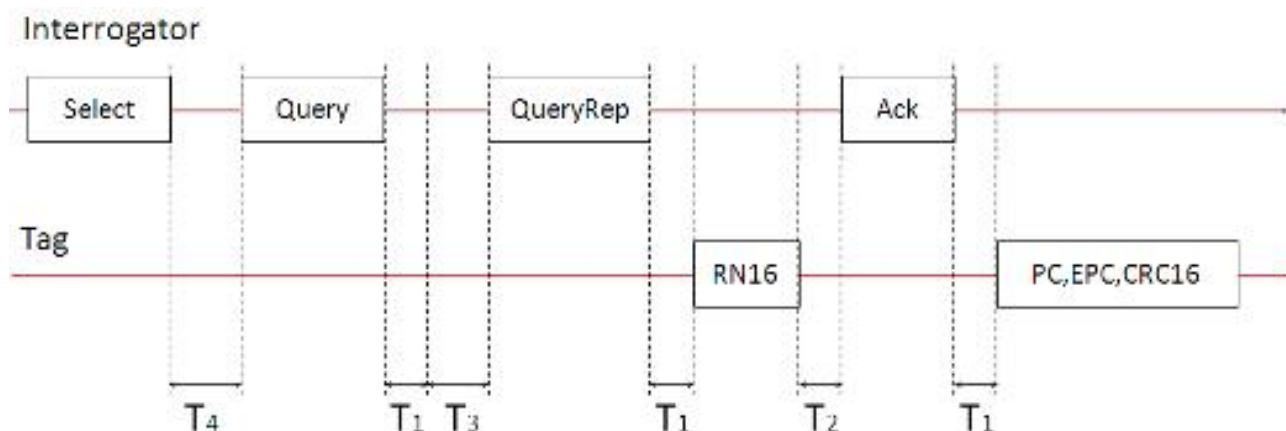


Figure 15. Link Timing Parameters for ISO 18000-6C

Figure 15 shows that an interrogation round results in a series of commands being exchanged between the interrogator and tag. In addition, these commands are exchanged in a handshake manner. In other words, when the tag responds to the interrogator, it is essential for the interrogator to issue its command within the specified limits of the T_2 link timing parameter.

For example, consider a scenario in which a tag takes longer to issue an RN16 command than it does to issue a PC + EPC + CRC16 command sequence. As illustrated in Figure 15, the interrogator first issues a Query or QueryRep command. Upon receiving the command, the tag responds with an RN16 command in accordance with the T_1 link timing specifications. Based on the exchange of these two commands, it is essential that the interrogator respond with an ACK command within the given T_2 specification to ensure that the tag responds with the PC + EPC + CRC16 command sequence. Thus, to verify that the tag responds to all commands within the allotted T_1 time period for all commands, you must simulate a complete inventory round.

In addition to simply measuring the link timing characteristics of an interrogation round, you can simulate how a tag responds to variable link timing. Using a software-defined emulation approach, you can configure your RFID test system to use custom T_2 and T_4 link timing values for each interrogator-to-tag transmission. By sweeping these parameters through the range of values specified by the ISO 18000-6C standard, you are able to verify that the tag conforms to the protocol.

You must consider four link timing parameters when testing either tags or readers. These parameters, T_1 , T_2 , T_3 , and T_4 , are determined primarily by the data rate used for transmission. Limit and description details for each link timing parameter are included in Table 3.

	Minimum	Nominal	Maximum	Description
T_1	$\text{MAX}(\text{RTcal}, 10T_{\text{pri}}) \times (1 - \text{FT}) - 2\mu\text{S}$	$\text{MAX}(\text{RTcal}, 10T_{\text{pri}})$	$\text{MAX}(\text{RTcal}, 10T_{\text{pri}}) \times (1 + \text{FT}) + 2\mu\text{S}$	Measure of time from interrogator transmission to tag response
T_2	$3.0T_{\text{pr}}$		$20.0T_{\text{pr}}$	Measure of time from tag response to interrogator transmission
T_3	$0.0T_{\text{pr}}$			Time an interrogator must wait, after T_1 , before issuing another command
T_4	2.0 RTcal			Minimum allowable time between interrogator commands

Table 3. Link Timing Requirements as Specified by ISO 18000-6C [1]

Note that in Table 3, you can define RTcal as the duration of a data-0 symbol plus the duration of a data-1 symbol in an interrogator-to-tag transmission. In addition, T_{pri} is the equivalent of $1/\text{BLF}$, where BLF is the backscatter link frequency.

Tag Command and State Machine Validation

A final aspect of protocol testing is tag command and state machine validation. According to the ISO 18000-6C standard, RFID tags are designed to respond to predefined commands with predefined responses. As observed in the earlier section, an RFID tag responds to the Query command with a RN16 command response. In addition, the tag enters the Reply state, which defines how the tag responds to the next command. In all, the ISO 18000-6C standard includes seven tag states [1] [8]. These states are Ready, Arbitrate, Reply, Acknowledged, Secured, and Killed. You can take a quick look at the state transition of the tag during a simple inventory round, as shown in Table 4.

Reader-to-Tag	Tag-to-Reader	Tag State
Query	-	Arbitrate
-	RN16	Reply
ACK	-	Reply
-	PC + EPC + CRC16	Acknowledged
Req_RN	-	Acknowledged
-	Handle + CRC16	Secured

Table 4. An RFID tag transitions through several states during a standard inventory round.

As Table 4 suggests, a protocol-conformant tag responds with a command that is dependent on its state. Because all states and potential tag responses are defined by the RFID standard, it is important to validate that the tag reacts as expected to a broad range of conditions. In this scenario, the RFID test system must be capable of the full emulation of the interrogator. In the case of the VISN-100 RFID tester, the instrumentation not only demodulates the tag response but also returns the complete command information – including the binary information contained in the tag response. By analyzing the raw bitstream returned from the tag, you can troubleshoot the tag during the design validation phase of product development.

To understand this in greater detail, consider a subset of a tag's state machine information in Figure 16.

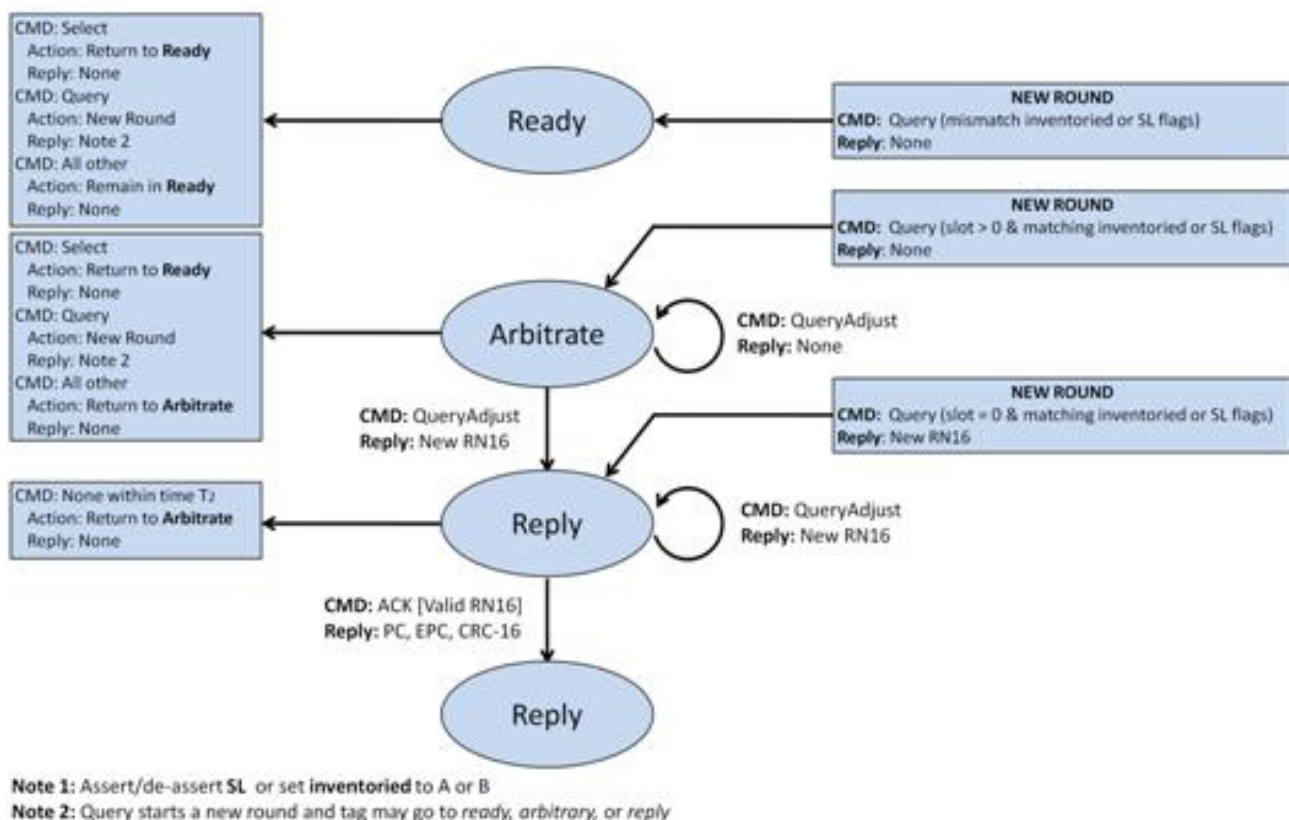


Figure 16. Partial Implementation of ISO 18000-6C Protocol [1][8]

Because Figure 16 is somewhat complex, consider the case where the tag is in the Ready state. While the tag is in this state, a Query command from the interrogator causes the tag to move into the Arbitrate state. From there, a QueryAdjust command yields a new RN16 response from the tag and moves to the Reply state. One interesting characteristic about the Reply state that you can observe from the state diagram is that the interrogator must respond within the specified T₂ link timing to stay in the Reply state. In fact, as the diagram illustrates, the tag moves back into the Arbitrate state if the interrogator does not issue the next command within the appropriate window of time.

As the exercise above illustrates, protocol testing can often be complex. In addition, it requires a

measurement system that is capable of reader emulation to complete the entire communication cycle. In this scenario, one of the primary benefits of the VISN-100 RFID tester is that you can configure it to respond with a wide range of commands to emulate the functionality of interrogators from a variety of manufacturers.

One growing requirement for protocol validation has resulted from the need for tag security. According to the Class 1, Gen 2 specifications [1], the security features that give an interrogator the ability to lock or kill a tag are optional. Because of this, researchers at the University of Pittsburgh RFID Center of Excellence have approached this problem by automatically configuring the command set of each tag [8]. They developed an RFID compiler that automatically generates controller code for a microprocessor or hardware device based on a high-level description of the command set that the user desires to support. While this paper does not examine this research, you can find more information in the article, "The Unwinding of a Protocol," by Dontharaju, Tung, Jones, Mats, Panuski, Cain, and Mickle.

Protocol testing is an important part of RFID tag and reader validation because you need it to verify protocol conformance. But perhaps the greater need is to verify interoperability between tags and readers of different vendors. As you have observed, the ISO 18000-6C specification allows for significant variability in characteristics such as data rate (Tari), link timing, and even command set. Thus, tag or reader emulation is an important aspect of product validation because it gives you the ability to simulate a full range of conditions that a product might encounter in the deployment environment.

Part 5: RFID Test Vendors and Third Parties

You can implement RFID test systems in a variety of ways to meet your test needs. Several National Instruments customers have implemented the PHY layer-specific RFID protocols on their own using a standard PXI RF vector signal analyzer and RF vector signal generator, but you can accomplish the same task with an out-of-the box solution. National Instruments recommends the NI-VISN-100 RFID Tester from VI Service Network.

NI-VISN-100 RFID Tester

The NI-VISN-100 RFID Tester is a comprehensive conformance test solution for RFID tags and readers. Because it implements the RFID protocol stack within the FPGA of the PCI-5640R IF transceiver, it is capable of full RFID tag and reader emulation. The tester is based on National Instruments vector RF modules, including the PXI-5610 2.7 GHz RF upconverter and the PXI-5600 2.7 GHz RF downconverter. Brief specifications are included in the next section, but you can find more information on the product in the article ["VI Service Network Offers RFID Tester."](#)

Product Specifications

- 250 kHz to 2.7 GHz frequency range
- 20 MHz real-time bandwidth
- -130 dBm/Hz noise density

- High-stability OCXO timebase
- +15 dBm maximum output power

Measurements/Features

- Frequency accuracy, frequency drift
- Power in band, OBW, ACPR
- Frequency and power sweeping
- Power on/off time, settling time
- Transmission ripple, pulse width, duty cycle, modulation depth
- Tari, delimiter, preamble
- Link timing, turnaround time
- Data rate, coding test
- Anticollision test, protocol state transition

RFID Standards Supported

- ISO 14443 Type A&B
- ISO 15693
- ISO 18000-3 Mode 1&2
- ISO 18000-6 Type A&B&C
- EPC HF Class 1
- EPC Class 1 Generation 2
- Customized Standard
- Future RFID Standard

Third Parties and Distributors

The NI-VISN-100 RFID Tester is offered worldwide through the distributors listed below:

Greater China: VI Service Network

About VI Service Network: www.vi-china.com.cn

VI Service Network is an independent instrumentation engineering service company that serves the growing instrumentation needs in China and elsewhere. It has expertise in cellular phone and related radio frequency testing, sound and vibration testing, and vision and motion integration. Dr. Hui Shao, a former NI Shanghai RD manager, started VI Service Network.

Contact Information: hui.shao@vi-china.com.cn

Europe: CISC Semiconductor Design and Consulting

About CISC: www.cisc.at

CISC Semiconductor Design and Consulting GmbH is a design and consulting service company for industries developing embedded microelectronic systems with extremely short time-to-market cycles. Their core competencies are system design, modeling, simulation, verification, and optimization of heterogeneous embedded microelectronic systems with a particular focus on automotive and RFID systems.

Japan: Peritec

About Peritec: www.peritec.co.jp/

Peritec specializes in system integration and general consulting for LabVIEW and other National Instruments products. Their specialties include manufacturing test and RFID measurements.

Contact Information: Peritec@peritec.co.jp

United States: Nexjen Systems

About Nexjen: www.nexjen.com

Nexjen Systems is a division of Jenkins Electric, a century-old supplier of industrial electrical test equipment and repair services. Nexjen continues this test solution tradition by focusing on today's need for test, measurement, and automation solutions. Nexjen is a full service integrator that provides clients nonproprietary and modular robust solutions using open architecture.

Contact Information: sales@nexjen.com

Korea: Infinity Wireless

Taiwan: T&C Technologies

Conclusion

The unique challenges of RFID tag testing have led to a wide variety of testing methodologies. From simple configuration of a vector signal analyzer as a packet “sniffer” to full interrogator emulation, the increasing complexity of test instrumentation offers more measurement capabilities. Thus, when performing RFID tag validation and verification, you must carefully consider the measurements you want to conduct to select the appropriate measurement hardware. For comprehensive testing that involves both PHY layer measurements and protocol validation, National Instruments recommends the NI-VISN-100 RFID Tester.

References

- [1] EPCTM Radio-Frequency Identification Protocols Class-1 Generation-2 RFID Protocol for Communications at 860 MHz – 960 MHz Version 1.10, EPCglobal Inc, 2006.
- [2] Dobkin, Daniel M. "The RF in RFID," Elsevier Inc., 2008.
- [3] Ng, Mun Leng. Leong, Kin Seong. Cole, Peter H. Analysis of Constraints in Small UHF RFID Tag Design, 2005.
- [4] Nikitin, P. V. and K. V. S. Rao, Theory and measurement of backscattering from RFID tags, IEEE Antennas and Propagation Magazine, vol. 48, no. 6, pp. 212-218, December 2006.
- [5] Nikitin, P. V., K. V. S. Rao, and R.D. Martinez, "Differential RCS of RFID tag," Electronics Letters, April 12, 2007, Vol. 43, No. 8.
- [6] Nikitin, P. V., K. V. S. Rao, and S. Lazar, "An overview of near field UHF RFID," IEEE RFID 2007 Conference, March 2007.
- [7] Rao, K. V. Seshagiri, Pavel V. Nikitin, and Sander F. Lam. "Antenna Design for UHF RFID Tags: A Review and a Practical Application." IEEE Transactions on Antennas and Propagation, VOL. 53, NO. 12, December 2005.
- [8] S. Dontharaju, S. Tung, A. K. Jones, L. Mats, J. Panuski, J. T. Cain, and M. H. Mickle, "The Unwinding of a Protocol," IEEE Applications & Practice, RFID Series, Vol. 1, No. 1, pp. 4 - 10, April 2007.
- [9] Jones, A. K., Dontharaju, S., Mats, L., Cain, J. T., and Mickle, M. H., "Exploring RFID Prototyping in the Virtual Laboratory," MSE Conference, 2007.
- [10] Sweeney, Patrick J. RFID for Dummies, pp.119-138. Wiley Publishing Inc, 2005.
- [11] Mickle, Marlin H. "Establishment of the University of Pittsburgh RFID Center of Excellence," IEEE Applications and Practice Magazine, April 2007.
- [12] Nikitin, Pavel V., [Using National Instruments Software and Hardware to Develop and Test RFID Tags](#), 2008.

Appendix A: Terms and Definitions

Term	Definition
Air Interface	Referring to the RF link (electromagnetic) between an interrogator and tag
ASK	Amplitude shift keying (modulation scheme)
BLF	Backscatter-link frequency ($BLF = 1 / T_{pri}$)
CRC16	16-bit cyclic redundancy check
dBm	Power in decibels relative to 1 mW
DR	Divide ratio

DSB-ASK	Double-sideband amplitude shift keying (modulation scheme)
EPC	Electronic product code
FHSS	Frequency-hopping spread spectrum
Inventory Round	A session between interrogator and tag initiated by the interrogator with a Query command and ended with a Query or Select command
PIE	Pulse interval encoding
PR-ASK	Phase-reversal amplitude shift keying (modulation scheme)
PSK	Phase Shift Keying (modulation scheme)
PHY Layer	Physical layer - refers to RF, modulation, and encoding characteristics
RN16	16-bit random or pseudorandom number
RTcal	Duration of data-0 plus duration of data-1 in interrogator-to-tag transmission
SS-ASK	Single-sideband amplitude shift keying (modulation scheme)
T _{ri}	Duration of a data-0 symbol in interrogator-to-tag signaling
TAT	Turnaround-time (general link timing term for T ₁ , T ₂ , T ₃ , and T ₄)
T ₁	Time for interrogator transmission to tag response
T ₂	Time from tag response to interrogator transmission
T ₃	Time an interrogator waits, after T ₁ , before it transmits another command
T ₄	Minimum time between interrogator commands
T _f	RF signal envelope fall time
T _{pri}	Backscatter-link pulse-repetition interval (T _{pri} = 1/BLF)
TRcal	TRcal = (DR/BLF) – refers to tag-to-interrogator calibration symbol