RIGOL

ZigBee Signal Analysis Application Note

ANW01100-1220-0046

1. Document description

1. Content in this guide

The purpose of this application guide is to describe the following:

- Describe the basic physical layer concepts and typical testing requirements of the ZigBee / IEEE 802.15.4 protocol
- Describe the features and operation of the ZigBee analysis software option with the RSA6000/RSA800 series real-time spectrum analyzers
- Describes the method of using ZigBee analysis software for typical test items such as modulated quality, EVM, spectrum characteristics, frequency offset, etc.
- Describe the instrumentation and configuration requirements required to complete the above tests
- Describes the safety precautions for the use of the instrument and RF accessories

2. Applicable instrument and software version

Category	**Product information**
Spectrum analyzers	RSA6000/RSA800 Series Real-Time Spectrum Analyzers
Analysis software options	ZigBee Signal Analysis Software Options (VSA· ZIGBEE)
Downloader software version	Refer to the software installation package release notes
Instrument firmware version	Refer to the firmware release notes in the corresponding product manual

3. Scope of applicable standards and agreements

The test methods and measurements in this guide refer to the following standards and protocols:

Standards/Protocols	**Description**
IEEE 802.15.4-2015	The ZigBee physical layer and MAC layer core specifications define the frequency band, channel, modulation, frame structure, etc.
ZigBee Specification (ZigBee Alliance)	Network layer and application layer protocol specifications based on IEEE 802.15.4
IEEE 802.15.4 O-QPSK PHY	2.4 GHz Frequency Band Physical Layer Modulation Specification (O-QPSK + Half-Sine Pulse Shaping)

2. Safety precautions

1. Instrument usage precautions

Input Power Limit: The instrument's RF IN port is extremely sensitive. Never input more than the maximum continuous RF power (typically +30 dBm, i.e. 1 W) and the maximum DC voltage (typically 50 VDC) indicated by the screen print on the front panel of the instrument. An out-of-limits signal can cause permanent burn-out of the RF front-end attenuator or mixer.

Reliable grounding: Always make sure that the instrument power cord is properly connected to an AC power outlet with a protective earth cord before measuring. A good grounding is not only a safety guarantee against electrical shock, but also a prerequisite for reducing floor noise and ensuring measurement accuracy for small signals, such as signals with demodulated thresholds down to 2 dB.

Venting Heat: The instrument generates heat during intensive real-time or VSA vector demodulation operations. Make sure that the cooling vents on both sides and at the rear of the instrument are unobstructed and that the test table is well ventilated.

2. Notes on the use of RF accessories

Connector Inspection and Cleaning: Before connecting any RF cable, attenuator, or impedance converter, visually inspect the connector bore and external threads for wear, distortion, or metal debris. It is recommended that the fittings be cleaned regularly with anhydrous alcohol and a special cotton swab.

Using a torque wrench: Do not use excessive force when tightening the type N or type SMA RF connectors. Standard torque wrenches such as SMA connectors are recommended with 0.9 N · m or 8 lbs-in torque to ensure stable electrical contact and extend connector life.

Cable bend radius: High-quality high frequency coaxial cables are weak, do not bend or twist cables excessively when routing and connecting (follow the minimum bend radius specified by the cable manufacturer) to avoid damaging the internal insulation. Causes impedance mismatch and worsening of the standing wave ratio (VSWR).

3. DUT Connection Considerations

Electrostatic protection (ESD): ZigBee chips and instruments have RF interfaces that are extremely vulnerable to electrostatic discharge (ESD). The operator must wear an anti-static wrist strap and ensure that a grounded anti-static bench mat is installed on the test bench before connecting DUT.

Avoid live plugging: When connecting or disconnecting the RF cable from DUT to the instrument, always turn off or power off the RF Transmission Control program of DUT. "Hot Plug" is strictly prohibited while DUT is transmitting a high-power signal to prevent instantaneous surges from damaging the front of the instrument.

DC block matches impedance:

1. If your ZigBee module RF output port has a DC bias voltage, be sure to series a DC Block in the link with an appropriate frequency range.
2. Identify the output impedance characteristics of DUT. For non-standard 50Ω impedance (e.g. 75Ω design on some antenna ends), always use a special impedance matching pad to convert to avoid heavy signal reflections.

3. ZigBee Signal and Test Basics

The purpose of this chapter is to provide the user with the theoretical basis for ZigBee signal analysis. By introducing the IEEE 802.15.4 standard, band distribution, modulation, frame structure, and core test metrics, To help users better understand the various measurements and analysis results of the RIGOL RSA6000 series of spectrum analyzers in ZigBee testing, providing theoretical guidance for actual R&D debugging and production line testing.

1. ZigBee / IEEE 802.15.4 Technical Overview

ZigBee is a low-power LAN protocol based on the IEEE 802.15.4 standard. In the standard OSI network model, the IEEE 802.15.4 specification defines the physical layer (PHY) and the media access control layer (MAC).

Key features of ZigBee technology include low power consumption, low cost, low data rates, and support for large network nodes (supporting star, tree, and mesh topologies). In the physical layer testing of RF instruments, we focus on the analysis and validation of RF characteristics and baseband modulation quality of their transmitters.

2. The ZigBee band is divided into channels

The IEEE 802.15.4 physical layer defines three major unlicensed industrial, scientific, and medical (ISM) bands. Channel division and transmission rates vary by frequency band:

- 2.4 GHz Band (Worldwide): This is the most widely used band available today and is the default and focus of the RSA6000 for analytics. The frequency band offers 16 channels (channel numbers 11 to 26) with a frequency range of 2405 MHz to 2480 MHz and a 5 MHz spacing between adjacent channel centers. The maximum data rate is 250 kbps.
    - Center frequency is calculated as $F_c = 2405 + 5 \times (k - 11) \text{MHz}$, where k is the channel number ($11 \le k \le 26$).
- 915 MHz band (Americas region): Provides 10 channels (channels 1 through 10) with 2 MHz spacing and a maximum speed of 40 kbps.
- 868 MHz band (European region): Provides 1 channel (Channel 0) at a maximum rate of 20 kbps.

3. O-QPSK modulation and half-sine pulse shaping

In the core 2.4 GHz band ZigBee/IEEE 802.15.4 uses direct sequence spread spectrum (DSSS) technology and offset orthogonal phase shift keying (O-QPSK, Offset-QPSK) modulation.

- Spread Spectrum Process: The physical layer maps every 4-bit data symbol (Symbol) to a 32-chip pseudo-random code (PN code) sequence with a Chip Rate constant of 2 Mcps.
- O-QPSK Modulation: Unlike traditional QPSK, O-QPSK staggered half of the symbology period in time (i.e. half code slice time $T_c / 2$) for the bitstream of the same phase (I) and orthogonal (Q) branch. This time shift prevents the signal trace from passing directly through the origin in the constellation graph, effectively reducing the fluctuation of the signal envelope.
- Half-Sine Pulse Shaping: Standard specifies that I/Q baseband signals pass through a half-sine pulse shape filter. Combined with the offset characteristics of O-QPSK, the shaped signal has an almost constant envelope (similar to MSK modulation). This design allows ZigBee transmitters to use high-efficiency nonlinear power amplifiers (PA) without causing significant spectrum expansion (Regrowth), which is well suited to the design needs of IoT devices with very low power consumption.

Measurement Tip: The initial IQ alignment format supported by the RSA6000

For the current release of the RSA6000 demodulation algorithm, The system has strict initial phase alignment requirements for captured or imported O-QPSK baseband IQ data sequences: At the initial sampling point of the signal payload, the I-way data must start at the highest point (peak) of the half-sine pulse. At the same time, the Q-way data must start from the start point of the half-sine pulse (past zero point).

In the ideal normalization state, the value of the sample point of the starting complex base band should satisfy I=1.0000, Q=0.0000 (i.e., 1.0000+0.0000i). If the initial I/Q timing alignment of the burst sent by the device under test does not match this format (for example, I/Q path reversal or timing offset), it may cause the instrument to trigger a synchronization failure or an abnormally high EVM / Offset EVM measurement

4. Introduction to the ZigBee frame structure

At the Physical layer, ZigBee's data transmission is burst (Burst) in the form of a Physical Layer Protocol Data Unit (PPDU). Understanding the frame structure is essential for accurate burst search and synchronization with the RSA6000. A standard PPDU frame consists of three main parts:

1. Synchronization Header (SHR):
    1. Preamble: Typically a 32-bit full '0' sequence for automatic gain control (AGC) and symbol synchronization on the receiving side.
    2. Frame Start Separator (SFD): A length of 8-bit (fixed to 0xA7), which marks the beginning of valid data. The RSA6000 demodulation algorithm relies on SHR for accurate signal capture and triggering.
2. Physical Layer Header (PHY): Length is 8-bits, where the first 7 bits indicate the length (in bytes) of the subsequent Physical Layer payload.
3. Physical Layer Payload (PHY Payload / PSDU): Variable length (up to 127 bytes), contains actual data passed from the MAC layer and the checksum sequence (FCS).

5. ZigBee Key Measurements

To verify that the ZigBee transmitter is designed to meet IEEE 802.15.4 standards and ensure interoperability between different vendor chips, the RSA6000 ZigBee Option provides a range of professional measurements. The following key parameters require user attention:

- Error Vector Magnitude: The most intuitive and central measure of transmitter modulation quality. Reflects the vector difference between the actual transmitted signal and the ideal reference signal. The IEEE 802.15.4 standard requires that the EVM value for the 2.4GHz band be below a specific limit (typically expressed as%, the standard limit is below 35%).
- Frequency Error / Offset: Measures the difference between the center frequency of the transmitting carrier and the nominal frequency. Excessive frequency deviation can cause the receiver to fail to lock the signal, and standards typically require a frequency deviation of within ±40 ppm.
- Symbol Clock Error: Evaluates the accuracy of the transmitter baseband clock frequency, reflecting the drift of the data chip rate.
- Phase Error & Magnitude Error: Dissects EVM errors. Large phase errors are usually associated with the transmitter Local Vibration (LO) phase noise; large amplitude errors may imply nonlinear distortion of the power amplifier.
- Constellation & Eye Diagram: The option provides intuitive trajectory distribution graphics. By observing the convergence of the O-QPSK constellation graph, engineers can quickly and qualitatively diagnose signal interference or distortion problems.

6. The RSA6000/RSA800 measures the benefits of ZigBee

Very low demodulation threshold to standard compliance:

Fully compliant with IEEE 802.15.4 physical layer specification, built-in standard half-sine pulse shaping filters. Specifically, the RSA6000 features industry-leading signal capture and demodulation algorithms with very low demodulation thresholds (as low as 2 dB for signal-to-noise as compared to SNR tolerance). This means that even in harsh RF environments with high background noise or weak signal, the instrument can robustly lock burst frames and accurately restore effective 0/1 bit streams.

Panorama Multidimensional View Analysis:

Going beyond a single viewing angle, the RSA6000 offers a flexible combined view of demodulated traces, demodulated errors, results statistics, and more. Full coverage time domain (frame capture, EVM error time domain), frequency domain (measurement spectrum) and vector domain (IQ graph, constellation graph, eye). Engineers can visually compare the trace differences between the actual signal and the ideal reference signal to quickly and qualitatively analyze RF front-end problems.

High precision and flexible sampling configuration:

Flexibility to configure sample points (4, 8, or 16 points) per codeTM for the speed and accuracy requirements of different test scenarios. Operating at a sample rate of 1 Msps in up to 16-point configurations, the system provides extremely fine-grained trace transient details for demanding R&D-level validation.

In-depth error code analysis and metric quantification:

In addition to more than ten core RF indicators such as EVM, Freq Offset, and IQ origin offset, the RSA6000 also supports the import of custom reference bit sequences (.xml files) for comparison. The system accurately counts the error rate (BER) in the demodulated bit view and highlights (red) the index position of the error bit directly, greatly improving the efficiency of the underlying data troubleshooting

4. Features of ZigBee analysis software

This chapter introduces the working principles, layout of the interface, configuration of parameters, and the meaning of each measurement view and result of ZigBee VSA (Vector Signal Analysis) software embedded in the RSA6000 series of spectrum analyzers. This chapter helps users quickly become familiar with the operating logic of the instrument.

1. Introduction to how the software works

The ZigBee analysis software for the RSA6000 is based on the IEEE 802.15.4 physical layer specification. It works by capturing the raw burst signal from the RF input port, pre-processing via a built-in half-sine pulse shaping (Half-Sine) filter and de-modulating O-QPSK to restore the actual baseband I/Q signal. The software then compares the actual measured signal with the internally generated ideal reference signal to calculate a multi-dimensional error vector (e.g. EVM) and finally restores the digital bitstream completion error rate (BER) statistics.

2. Description of the main screen

The ZigBee analysis interface of the RSA6000 uses a design architecture that runs in multiple windows in parallel to facilitate simultaneous analysis of test signals from different dimensions. The main interface consists of the following core areas:

- Multi-window operating display area: Occupies the main body of the screen and supports simultaneous side-by-side display of multiple views (e.g., time domain trace, spectrum, constellation chart, parameter table, etc.).
- Status display bar: Located above the interface, displays the current dynamic range (Range), center frequency (CF), bandwidth (Span) in real time. IQ sample rate (SR fixed at 1 Msps) and key hardware and measurement states such as trigger mode.
- Menu control and navigation area: Located on the right and bottom of the screen, provides frequency, amplitude, triggering, Configuration portal for various parameters such as measurement settings and includes quick actions such as adding views, one-click screenshots, presets, and more

3. Parameter configuration description

View selection can be made by clicking on the operating mode key in the lower left corner of the

instrument to enter the ‘Measurement Setup’ menu.
Select ZIGBEE > Apply to enter ZigBee work mode

1. Frequency

Set each frequency parameter of the spectrometer

Center frequency

Preset standards
The center frequency of the ZigBee feature, determined by selecting the channel number in the Measurement Setup > Demodulation Preset > ZigBee Channel Features menu, is not modifiable here and can only be viewed.
The center frequency for the ZigBee channel
16 channels, numbered 11 to 26.

Channel No.	Center Freq	Single-channel Bandwidth
11	2405 MHz	5 MHz
12	2410 MHz	5 MHz
13	2415 MHz	5 MHz
14	2420 MHz	5 MHz
15	2425 MHz	5 MHz
16	2430 MHz	5 MHz
17	2435 MHz	5 MHz
18	2440 MHz	5 MHz
19	2445 MHz	5 MHz
20	2450 MHz	5 MHz
21	2455 MHz	5 MHz
22	2460 MHz	5 MHz
23	2465 MHz	5 MHz
24	2470 MHz	5 MHz
25	2475 MHz	5 MHz
26	2480 MHz	5 MHz

2. Amplitude

Set the spectrometer amplitude parameters. By adjusting these parameters, the signal being measured can be adjusted to a level that is easy to observe and minimizes measurement error
Is displayed in the current window.

Scope

Sets the maximum sine input signal amplitude that is not limited by the medium frequency ADC.

Parameter Remarks	Parameter Remarks
Default	20 dBm
Range	-15 dBm to +25 dBm
Unit	dBm
Knob Step	1 dBm
Left/Right Arrow Key Step	10 dBm

3. Scan

Set scan-related parameters.
Scan Mode
Sets the current scan mode to Single or Continuous.
Rescan

Click Rescan to restart a scan measurement when the scan is a single scan; this function is grayed out when the scan is a continuous scan.

4. Bandwidth

FFT window type

Select the type of FFT window function.
You can choose from four types of window functions: Rectangular, Hanning, Gauss, and Flat Top.
Depending on the actual measurement needs, the user can select the appropriate filter type, as shown in the table below.

Window Function	Characteristics	Application
Rectangular	Its main lobe is relatively concentrated, but its side lobe is relatively high, with negative side lobes. This will result in high-frequency interference and leakage during transform, even worse, the negative spectrum. The frequency recognition accuracy is the highest, and the amplitude recognition accuracy is the lowest.	If you have a high requirement on the accuracy of the frequency readout of the main lobe, without needing to consider the accuracy of the amplitude, then the rectangular window is recommended.
Hanning	It is also called the cosine window. Its main lobe is widened and lowered, and its side lobe is reduced significantly. In terms of leakage reduction, the Hanning window is superior to the Rectangular window. However, the wide main lobe of the Hanning window signifies the widened analysis bandwidth and reduced frequency resolution. Compared with the Rectangular window, the leakage and fluctuation of the Hanning window are reduced, with more choices.	The Hanning window is preferred under the following conditions: the signal under test has several frequency components; the spectrum is very complex; the test aim focuses more on the frequency point rather than the energy size; the signal under test is random or unknown.
Gaussian	It is an exponential window. Its main lobe is wide and frequency resolution is low. It has no negative side lobe, and the attenuation of its first side lobe reaches -55dB. It is often used to truncate some non-periodic signals, such as the exponential decay signal.	For the time-varying exponential decay function, you can use the exponential window to improve the S/N ratio.
Flattop	The flattop window has few low pass band fluctuations in the frequency domain.	As there are minor errors in the amplitude, this window can be used in calibration.

5. Trigger

Select the trigger source and set the trigger-related parameters.

1. Trigger source

Set the trigger source to be the "free-trigger", "external-triggered "mid-range" or "common-purpose" trigger.

2. Free triggering

The trigger condition is met at any time, i.e. the trigger signal is continuously generated.

3. External Triggering

Press Trigger > Trigger Source > External Trigger and then enter an external signal via the rear panel (TRIG IN) connector when
A trigger signal is generated when the signal meets the set trigger conditions.
Note: external trigger interface, input signal frequency not higher than 1 MHz.

- Trigger edge

Sets the trigger polarity for external triggering. Set to a positive slope when a rising edge trigger is required; when a falling edge trigger is required When using a negative slope.

- Trigger the delay switch

Turns the trigger delay feature on or off. You can set the trigger delay time when the trigger delay feature is turned on.

- Trigger delay time

Sets the amount of time to wait after a trigger that meets the trigger requirements is generated before the instrument starts scanning. You can use numbers
Key, rotary knob, arrow key, or touch screen.

Parameter	Remarks
Default	1 μs
Range	-500 ms[1] to 500 ms
Unit	s, ms, us, ns, ps
Knob Step	trigger delay/100, Min = 1 us
Left/Right Arrow Key Step	at 1-1.5-2-3-5-7.5 step

4. Mid-frequency power triggering

A trigger signal is generated when the detected medium frequency signal power exceeds the set trigger voltage.

6. Measurement settings

1. Modulation mode

Fixed as OQPSK and cannot be modified.
O-QPSK (Offset Quadrature Phase Shift Keying) is a physical layer modulation scheme defined by the IEEE 802.15.4 standard for the 2.4 GHz frequency band. Constant envelope, low power, phase continuity, It has high data rate, low power consumption and strong immunity to interference.

2. Measurement interval

Sets the number of symbols analyzed when digital demodulation is performed.
This parameter, along with the symbol rate, determines the overall time record length in seconds used to understand the modulator. It also indirectly sets the resolution bandwidth for various spectral results (ResBW cannot be set independently).

Parameter	Description
Default	50
Range	10 to 4,096
Unit	N/A
Knob Step	1
Left/Right Arrow Key Step	10

3. Bit rate

Bit rate (bitrate) refers to the number of binary bits (bits) transmitted per unit of time, which is the actual data transfer rate. The ZigBee 2.4GHz standard specifies a bit rate of 250 kbps (250,000 bits per second) and a corresponding bit rate (baud rate) of 62.5 ksym/s (4 bits per element).
Here is the IQ sample rate for demodulated analysis, fixed at 1 Msps and cannot be modified. The instrument analyzes the signal with the highest accuracy, ensuring that each codeelement contains 16 sample points (16 × 62.5 ksym/s=1 Msamples/s)

4. Number of sampling points/codets

Sets the number of sampling points per codemeter in the demodulated data, which can be set to 4, 8, 16. Sample rate = coderate × sample number/coderate

Points/Symbol	Symbol Rate	Symbol Duration	Sample Rate
4	62.5 ksym/s	16 μs	250 kHz
8	62.5 ksym/s	16 μs	500 kHz
16	62.5 ksym/s	16 μs	1 MHz

5. Measure the filter

The measurement filter type is used to filter out noise, restore waveforms, and simulate receiver behavior on the measured IQ signal. Fixed as half-sine, cannot be modified.

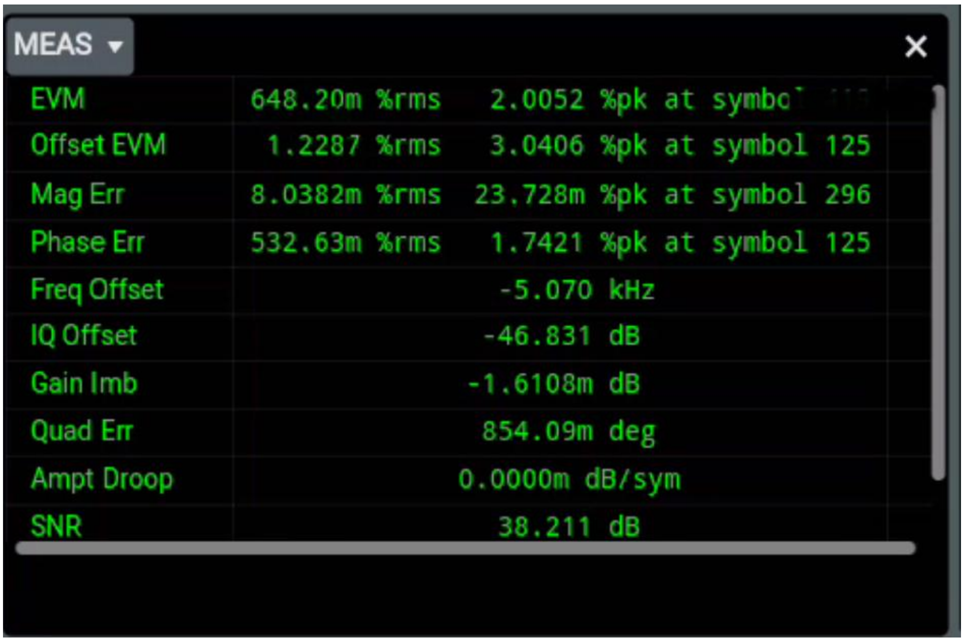
6. Reference filter

The reference filter is used to generate the ideal reference signal as a benchmark for the calculation of EVM. Fixed as half-sine, cannot be modified.

4. Description of the basic measurement results

1. Basic measurements

The basic measurement view shows detailed measurement data after demodulating the ZigBee signal.



The test items included are as follows:

- **EVM (error vector amplitude)**

Measures the vector difference between the actual signal and the ideal signal. The lower the value, the better (standard limit ≤ 35%), directly reflecting the whole
Body modulated mass.

- **Offset EVM**

Specific metrics for ZigBee (O-QPSK) modulation. EVM with the timing offset effect removed, the lower the value
Good, more realistic signal quality.

- **Mag Err (amplitude error)**

Nonlinear jitter or deviation of signal amplitude. Lower values are better, primarily reflecting the linearity and stability of the power amplifier (PA)
Qualitative.

- **Phase Err**

The jitter of the signal phase. The lower the value, the better (usually < 5°), primarily reflecting Local Vibration (LO) stability or phase
Bit noise level.

- **Freq Offset**

The difference between the carrier frequency and the standard center frequency. The closer the value is to 0, the better (standard limit ± 40ppm), reflecting the crystal
Accuracy.

- **IQ Offset**

This is a LOLeak. The lower the value (the deeper the negative value), the better (< -30dB is recommended), reflecting the RF chain isolation and hardware performance.

- **Gain Imb**

The difference between the I and Q-way increases the gain. The closer the value is to 0 dB, the better, reflecting the two hardware circuits of the modulator I/Q Symmetry.

- **Quad Err (orthogonal error)**

The degree to which the I and Q phases differ by 90°. The value closer to 0° is better, reflecting the physical orthogonality of the demodulated link.

- **Ampt Droop**

Power decay rate during packet transmission. The closer the value is to 0, the better, reflecting the power capacity of the PA and thermal stability (No thermal effects).

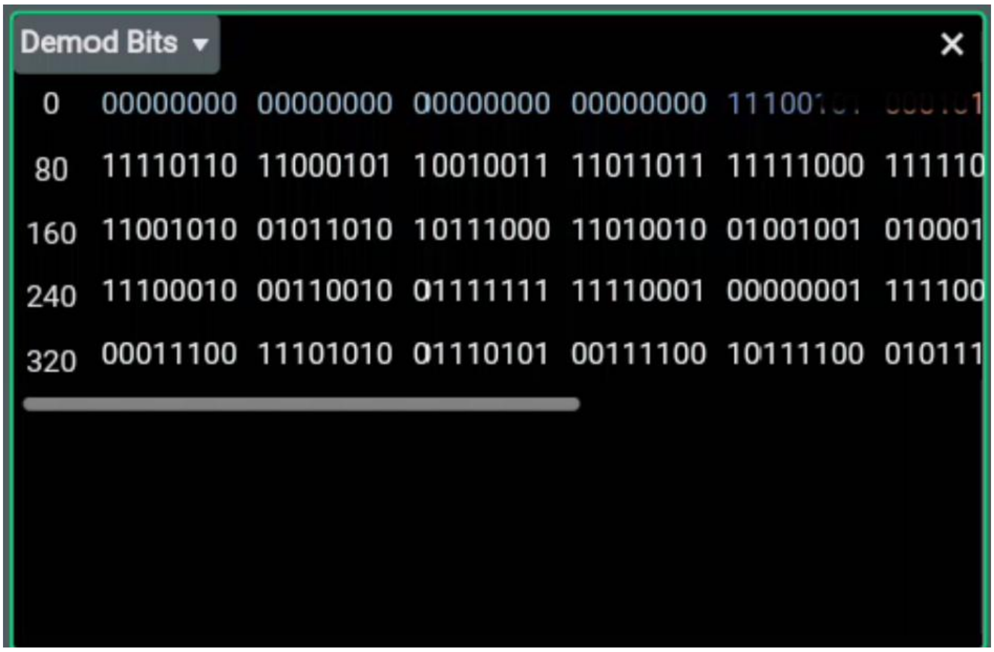
- **SNR (signal-to-noise ratio)**

The ratio of signal power to base noise power. The higher the value, the better (usually > 30dB), reflecting the purity of the signal and its resistance Interference capability.

- **Rho (correlation coefficient)**

The correlation between the actual waveform and the desired waveform. The closer the value is to 1.0, the better, indicating that the waveform is complete and undistorted Change.

2. Demodulated bits



The error rate is used to determine signal data quality. Select the "Error Rate" switch on in the Measurement Setup > Error Rate menu to solve the problem

Bitwise view displays the error rate statistics.

BER = Error Bits / Total Bits

• BER (Bit Error Rate): Error rate

• Error Bits: The number of error bits

• Total Bits: Total number of bits

3. Measure View window item

Display View Type	Y Axis Unit Type	Ref Value	Scale/Div
Raw Time	Peak	dBV_{pk}	dB
	RMS	dBV_{rms}	dB
	Power	dBm	dB
Spectrum	Peak	dBV_{pk}	dB
	RMS	dBV_{rms}	dB
	Power	dBm	dB
MeasLog	N/A	dB	dB
MeasLin	N/A	Without Unit	Without Unit
MeasReal	N/A	Without Unit	Without Unit
MeasImag	N/A	Without Unit	Without Unit
MeasPhase	N/A	°	°
MeasPhaseUnwrap	N/A	°	°
MeasIQ	N/A	Without Unit	Without Unit
MeasCons	N/A	Without Unit	Without Unit
MeasIEye	N/A	Without Unit	Without Unit
MeasQEye	N/A	Without Unit	Without Unit

Display View Type	Y Axis Unit Type	Ref Value	Scale/Div
MeasSpectrum	N/A	dB	dB
RefLog	N/A	dB	dB
RefLin	N/A	Without Unit	Without Unit
RefReal	N/A	Without Unit	Without Unit
RefImag	N/A	Without Unit	Without Unit
RefPhase	N/A	°	°
RefPhaseUnwrap	N/A	°	°
RefIQ	N/A	Without Unit	Without Unit
RefCons	N/A	Without Unit	Without Unit
RefIEye	N/A	Without Unit	Without Unit
RefQEye	N/A	Without Unit	Without Unit
RefSpectrum	N/A	dB	dB
EVMErrorTime	N/A	%	%
EVMErrorSpectrum	N/A	dB	dB
MagError	N/A	dB%	dB%
PhaseError	N/A	°	°

5. Pre-test preparation

To ensure that the RSA6000 spectrum analyzer can accurately and reliably capture and demodulate ZigBee bursts, the test environment needs to be modified prior to formal metric measurements. The test instrument and the equipment under test (DUT) are properly planned and configured.

1. Test the connection diagram

Figure 1: Signal Source + RSA6000 Spectrometer (Built-in ZigBee) combination

2. Test mode selection

Conducted Test is generally recommended for RF transmitter validation of ZigBee equipment. The RF out connector on DUT is connected directly to the RF in port of the RSA6000 via RF coaxial cable. Conduction testing maximizes shielding from electromagnetic interference in space and eliminates the multi-path fading effects of the antenna environment, resulting in the most accurate measurements of EVM, power, and spectral characteristics. For system-level full machine validation, Radiated Test can also be used in conjunction with standard test antennas and dark room environments.

3. Required equipment and accessories

- Spectrum Analyzer: The RIGOL RSA6000 series of real-time spectrum analyzers require the VSA and ZigBee analysis options.
- RF Cable: High quality 50Ω RF coaxial cable.
- Impedance converter (depending on requirements): The instrument default input impedance is 50Ω. If your system under test has an output impedance of 75 Ω, you must connect using a 75 Ω to 50 Ω adapter provided by RIGOL and change the input impedance to 75 Ω in the software's "I/O" menu.
- Attenuators (as required): If the DUT output power is too high, a series of high-power fixed attenuators is required to protect the RF front end of the instrument.

4. Instrument initialization and warm-up

Warmup: To ensure measurement accuracy and stability of the Local Vibration (LO), it is recommended that the instrument warm up for at least 30 minutes after power-on (RF Common Specification).

Automatic Calibration: Check the Automatic Calibration status (Align) on the system status bar to ensure that the instrument is in an accurate amplitude and frequency calibration state.

Restore Defaults: Click the "Restore Defaults Quick Start" button on the main screen (or press the front panel Preset key) to initialize the system status to the factory-set security defaults

5. DUT Preparation

Requires DUT to be able to operate at a specified channel frequency, such as CH11, and continuously output O-QPSK modulated ZigBee standard packets based on the IEEE 802.15.4 specification.

6. The default parameter configuration is recommended

The RSA6000 is internally integrated with the standard preset parameters for ZIGBE2450. For initial signal capture, the following default configuration is recommended for test environment verification:

- Frequency Setting: The default center frequency is set to 2.405 GHz (corresponding to ZigBee Channel 11).

- Demodulation parameters: Modulations are fixed to O-QPSK, the bit rate is fixed at 1 Msps, the measurement interval is set to 50 symbols, and the sample points/code element is recommended to be set to 4. The measurement/reference filters are half-sine (Half-Sine).
- Trigger setting: The default is a "Free Run". For stable locking of burst packets, the trigger source can also be changed to a "IF Power Trigger" in the "Trigger" menu with a default trigger level of −25 dBm.

7. Input level and attenuation recommendations

Setting the Dynamic Range appropriately is key to ensuring that the signal is complete and not distorted. The RSA6000 dynamic range is set between −15 dBm to dBm, and the default is 20 dBm.

- Signal Overload Protection: The dynamic range should be slightly higher than the actual maximum transmit power of DUT.
- External Attenuation Compensation: If a fixed attenuator is in series on the RF link or if the test cable loss is large, enter the "Input Output > External Gain" menu and enter the loss value in negative form (e.g. −10 dB). The attenuation value is automatically compensated for by the instrument in the internal operation, and the trace position is adjusted, but the Y-axis reference value and scale remain unchanged

8. Troubleshoot common issues

If you encounter an exception during testing, you can begin troubleshooting along the following lines:

- Cannot capture signal or demodulated bit interface has no output:

  The instrument transmit IQ data is checked first for compliance with the OQPSK signal specifications described in section 3.3, and then the "center frequency" is consistent with the channel transmitted by DUT. Second, if an intermediate frequency power trigger is used, check that the trigger level (e.g. −25 dBm) is above the spatial undernoise and below the peak power of the signal. Improper setting of the level may result in non-triggering.

- EVM / Offset EVM abnormally high:

  Check if the input signal level is too high to limit the amplitude, or too low to achieve an insufficient signal-to-noise ratio (SNR). In addition, verify that the I/Q initial sampling map timings at the bottom of DUT are within specification, in conjunction with Section 3.3.

- Freq Offset Too Large:

  The standard limit is ±40 ppm. If the instrument often measures a frequency deviation outside this range, which is usually a DUT hardware problem (such as excessive on-board crystal oscillation or insufficient matching capacitance accuracy), it is recommended to focus on the crystal oscillation circuit of the DUT hardware.

6. Typical application testing

1. ZigBee signal capture and time domain trace observations

1. Test purpose

Verifies that the instrument can reliably trigger and fully capture the ZigBee Burst (Burst) from DUT (DUT), the time-domain power envelope of the visual observation signal.

2. Test the connection diagram

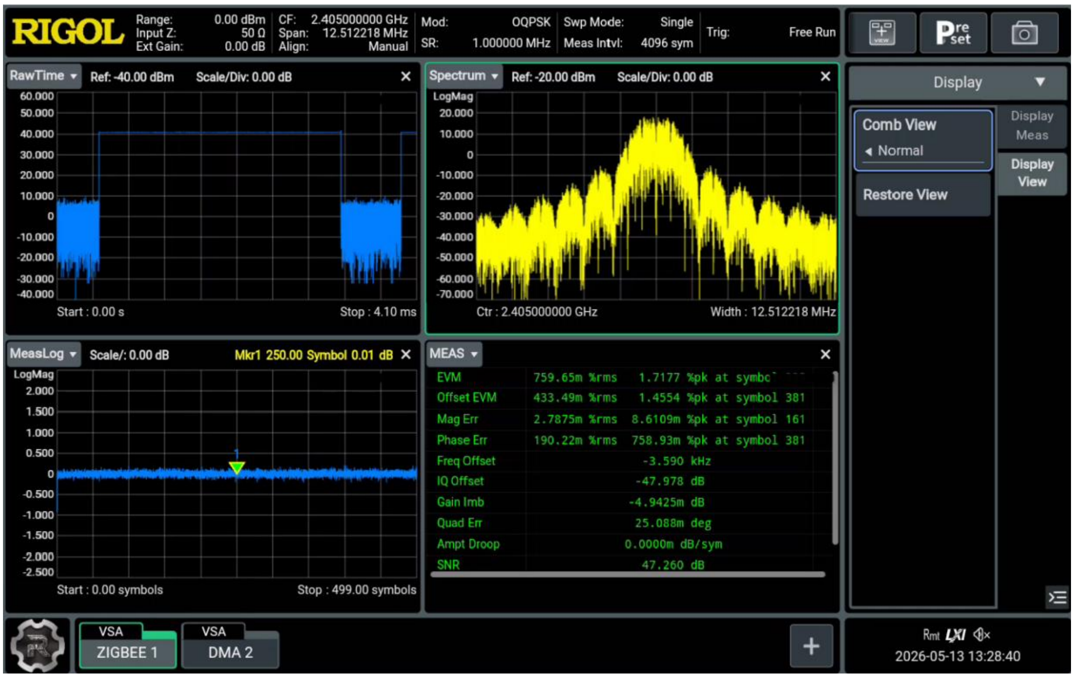
Refer to the5.1 Test the connection diagram

3. Test procedure

Set Frequency and Amplitude: Select a channel (e.g. CH11, center frequency 2405 MHz) that matches DUT in the "Measurement Setup -> Demodulation Preset Family". Adjust the "Amplitude -> Range" slightly above the signal peak power to avoid the mid-frequency limit.

Setting the Trigger Mode: Sets the "Trigger Source" to the "Free-to-Trigger Family".

Configure View: Click Display -> View to set the "Common View".



4. Test results and analysis

In the "original time domain view", the X-axis is the time and the Y-axis is the log power. The power variation characteristics of the rising, falling and flat top sections of the ZigBee burst packets are clearly visible. If the trace jumps over the time axis, the trigger is not set correctly, and if the signal appears as "Top", the instrument range needs to be increased.

2. ZigBee O-QPSK modulation quality and EVM analysis

1. Test purpose

In the "original time domain view", the X-axis is the time and the Y-axis is the log power. The power variation characteristics of the rising, falling and flat top sections of the ZigBee burst packets are clearly visible. If the trace jumps over the time axis, the trigger is not set correctly, and if the signal appears as "Top", the instrument range needs to be increased.

2. Test the connection diagram

Refer to the 5.1 Test the connection diagram

3. Test procedure

Make sure that the steady triggering of the signal is completed in accordance with Section 6.1.

Parameter configuration: Go to the 'Measurement Setup', confirm the Modulated Mode is OQPSK, set the 'Measurement Interval' (e.g. 1000 symbol, recommended to be set to exactly cover 2-3 frames) to cover the payload. The "Sample Number/Code Name" is increased to 16 points for maximum resolution.

To call up a combined view: Click Display -> View Settings -> Generic Family, or manually add the "Measurements" and the "Basic Measurements View."

4. Test results and analysis

Basic Measurement Window: Direct reading of EVM and Offset EVM metrics. EVM reflects the overall modulation quality, with a standard limit requirement of ≤ 35%.
Offset EVM features: Because ZigBee uses O-QPSK modulation, Offset EVM removes the effect of I/Q timing offset and is usually lower than regular EVM (due to timing errors, offset EVM may be higher than EVM). More realistic reflection of the transmitter's underlay modulation quality.
Constellation charts: Ideal O-QPSK measurement constellations should show clear convergence points; scattered or trailing constellations tend to indicate higher EVM errors.

3. ZigBee spectral characteristic observations

1. Test purpose

Observe the energy distribution characteristics of the ZigBee signal in the frequency domain and check the power conditions at the central frequency point and in the frequency band.

2. Test the connection diagram

Refer to the 5.1 Test the connection diagram

3. Test procedure

On a steady demodulation basis, add the "Measurement Spectrum" in the "Display -> View" setting.
X/Y axis optimization: Turns off the "X" axis scale "" auto switch, manually adjusts the "Width" to enlarge the main valve feature of the display signal; optimizes the Y-axis display using the "Amplitude" -> "Automatic Scale".

Cursor Measurement: Turns on the "Cursor -> Cursor Function" and enables the "Bandwidth" function to measure the bandwidth power in a specified frequency band.

4. Test results and analysis

The "Spectrum View" shows the broadband power domain characteristics of the original captured signal; the "Measuring Spectrum" shows the specific frequency domain characteristics of the tuned data segment.

The X-axis center frequency defaults to the selected channel frequency and the default display width (Width) is approximately 3.128 MHz.

Analysis: Main valve energy should be concentrated near the channel center frequency point. In combination with half-sine pulse shaping, the side-flaps of the normal spectrum should show smooth attenuation. A very high sidestep may imply that the amplifier (PA) is in a deep nonlinear saturated region.

4. **ZigBee frequency offset and phase error analysis**

1. Test purpose

In-depth diagnosis of RF transceiver hardware damage, particularly the stability of the local vibration (LO), phase noise levels, and physical isolation of the I/Q modulator.

2. Test the connection diagram

Refer to the5.1 Test the connection diagram

3. Test procedure

On the condition that the signal is successfully demodulated, go to Display > View Settings > Combined View.

Select the demodulated error combination. The combined view will present the "EVM¬F", "amplitude", "phase error" trace, and the "basic measurement form simultaneously on a single screen.

4. Test results and analysis

Combined diagnosis with basic measurement table and error trace:

- Freq Offset: Reads the Freq Offset value from the base measurement table. The standard limit is ±40 ppm. If this value is exceeded, it is usually the DUT reference crystal with a frequency bias.
- Phase Err: Reads the global phase error value (usually requires $< 5^\circ$) and observes the "Phase Error View." If the trace shows large random fluctuations over time, LO has poor phase noise.
- IQ Offset: Evaluate the local vibration leak. The recommended value is < −30 dB. If the value is high (e.g. greater than −20 dB), there is a DC bias at the modulator input or insufficient LO isolation.

5. ZigBee Signal Amplitude Characterization

1. Test purpose

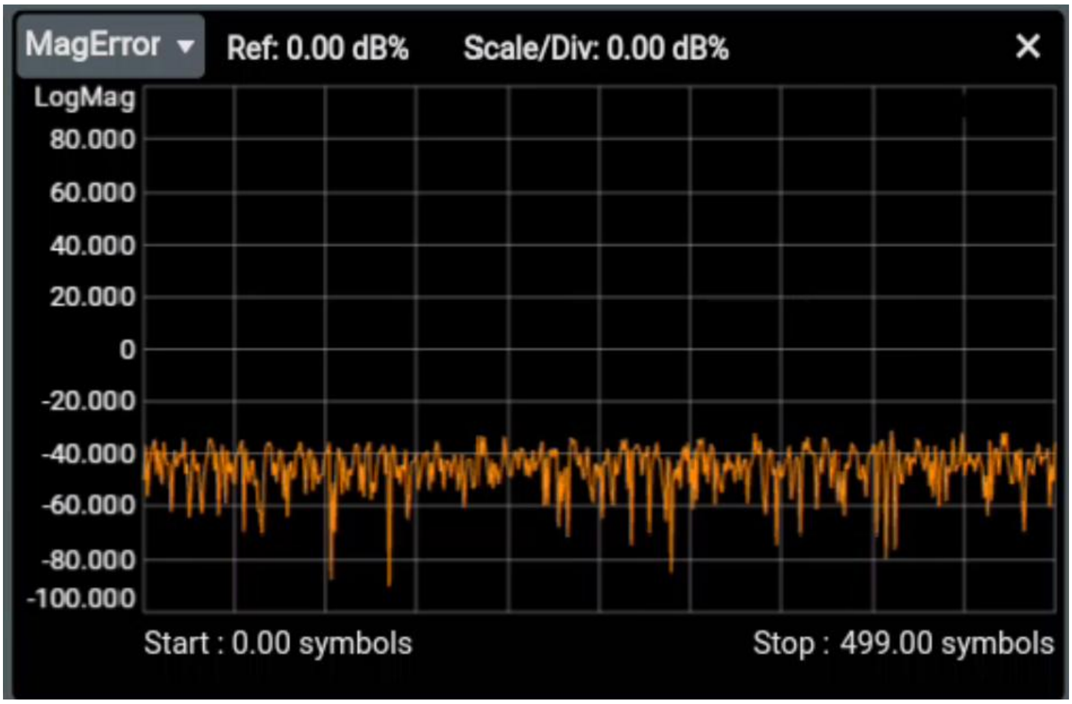
Because ZigBee's O-QPSK with half-sine pulse shaping theoretically has an approximate constant envelope, this test is designed to assess the envelope constancy of the actual transmitted signal and to check for amplitude drop (Droop) or nonlinear distortion of the power amplifier (PA).

2. Test the connection diagram

Refer to the5.1 Test the connection diagram

3. Test procedure

Make sure that the steady triggering and demodulation capture of the signal is done as per Section 6.1. Go to "Display -> View Settings" and check "Meas Time Ampt" under "Measurement and Reference Data".
Check the "Mag Err" in the "Unmodulated error data category" for the "Magnitude Err" view to observe the distribution of errors over time.



4. Test results and analysis

Trace Consistency Assessment: Look at the "Measurement Time Range" view, the ideal ZigBee signal amplitude envelope during a burst payload should be a smooth straight line. If the trace shows a significant downward trend in tilt on the timeline, the PA's power network may have a transient underresponse, resulting in a amplitude drop.
Quantification of amplitude error: View the "Mag Err" in the Basic Measurements Form. When combined with the trajectory of the 'Amplitude Error' view, the error fluctuates dramatically with signal power fluctuations, strongly implying a more severe AM-AM nonlinear distortion of the RF front-end link.

7.Summary

1. Summary of ZigBee analysis software capabilities

The ZigBee vector signal analysis option on the RSA6000 is a professional test tool that strictly adheres to the IEEE 802.15.4 standard. Its core feature highlights include:

- Superior demodulation performance: Very low demodulation threshold as low as 2 dB (SNR), robustly locks burst frames in harsh background noise.
- Panoramic Multidimensional Viewport: Provides rich views of time, frequency, vector (constellation/eye), and error domains, supporting multi-window, simultaneous linkage analysis.

- Quantitative metrics of depth: Over ten key RF parameters such as EVM, Offset EVM, frequency offset, amplitude/phase error, and more can be output with one click.
- Protocol Level Error Correction Assist: Enables the import of .xml reference sequences for accurate error rate (BER) statistics and visual highlighting of error locations, enabling cross-layer scheduling of data from the underlying RF to the protocol layer.

2. Summary of the value of typical ZigBee applications

For hardware engineers working in the network of things (IoT), smart home, and industrial sensing networks, the software has tremendous application value:

- R&D and Validation Phase: Helps RF engineers quickly characterize and quantify deep hardware issues such as transmitter baseband IQ-mapped timing (e.g., O-QPSK half-sine offset format), intrinsic lock phase ring stability and PA linearity, and accelerate product iterations.
- Production line testing phase: With one-click auto-demodulation and an intuitive “Basic Measurements Data Sheet”, the efficiency and reliability of batch consistency testing is greatly improved, ensuring interoperability and communication quality of factory equipment in complex networking environments.

3. Links to related products and resources

To get the latest firmware updates, complete user manuals or for professional technical support, please visit the official RIGOL channel:

- Official website: www.rigol.com
- RSA6000 Product Page: Search the "RSA6000" product flyer, data sheet, and list of the latest options.
- Technical Support & Service: If you have any questions regarding instrument usage or the automated test code (SCPI) writing process, please contact your local RIGOL sales engineer or call the official technical support line.

Boost Smart World and Technology Innovation

- Cellular-5G/WIFI
- UWB/RFID/ ZIGBEE
- Digital Bus/Ethernet
- Optical Communication

- Digital/Analog/RF Chip
- Memory and MCU Chip
- Third-Generation Semiconductor
- Solar Photovoltaic Cells

- New Energy Automobile
- PV/Inverter
- Power Test
- Automotive Electronics

Provide Testing and Measuring Products and Solutions for Industry Customers

HEADQUARTER

RIGOL TECHNOLOGIES CO., LTD.
No.8 Keling Road, New District,
Suzhou,JiangSu, P.R.China
Tel: +86-400620002
Email: info-cn@rigol.com

EUROPE

RIGOL TECHNOLOGIES EU GmbH
Friedrichshafener Str. 5c
82205 Gilching
Germany
Tel: +49-(0)8105-27292-22
Email: johannes.kroiher@rigol.com

NORTH AMERICA

RIGOL TECHNOLOGIES, USA INC.
10220 SW Nimbus Ave.
Suite K-7
Portland, OR 97223
Tel: +1-877-4-**RIGOL**-1
Email: sales@rigol.com

JAPAN

RIGOL JAPAN CO., LTD.
5F,3-45-6,Minamiotsuka, Toshima-Ku,
Tokyo,170-0005,Japan
Tel: +81-3-6262-8932
Fax: +81-3-6262-8933
Email: info.jp@rigol.com

KOREA

RIGOL KOREA CO,. LTD.
5F, 222, Gonghang-daero,
Gangseo-gu, Seoul, Republic of Korea
Tel: +82-2-6953-4466
Fax: +82-2-6953-4422
Email: info.kr@rigol.com

For Assistance in Other Countries

Email: info.int@rigol.com