HRZB211
2.4GHz ZigBee Module

User Manual

Version 1.0

Beijing HangRuiTuoYu Technology Co.,Ltd

Information published here is current or planned as of the date of publication of this document. Because we are improving and adding features to our products continuously, the information in this publication is subject to change without notice.

Revision and Iteration History

Version	**Publication Date**	**Authors**	**Summary of Changes and Updates**
1.0.00	08/01/2013	WF	Document Creation

FCC Information

Agency Identification Number

FCC Notice	"This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation."
FCC Labeling Requirement Notice	If the FCC ID is not visible when the module is installed inside another device, the outside of the device into which the module is installed must also display a label referring to the enclosed module. This exterior label can use wording such as the following: **Contains "FCC ID: 2AA43HRTYZB211"**
FCC Changes/Modifications Warning	"Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment"
RF Exposure Guidance	"This equipment complies with FCC radiation exposure limits. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and persons. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter, except in accordance with FCC multi-transmitter product procedures."

1 Overview

HRZB211 is HangRuiTuoYu's first embeddable, IEEE 802.15.4/ZigBee-compliant wireless module. HRZB211 can operate over 16 channels in the unlicensed 2.4GHz frequency band (or ISM, short for *Industrial, Science and Medical*) across the world.

In addition to its IEEE-standard-based RF and PHY/MAC air interfaces, HRZB211's embedded stack support a wide variety of useful networking features. HRZB211's network support is designed to cover a whole range of application needs, ranging from a simple beaconing network to complicated multi-story full ad hoc networks.

Whether your applications need the robustness and simplicity of IEEE 802.15.4 standard or the versatility of ZigBee Compliance Platform, HangRuiTuoYu's HRZB211 is the vehicle to enable your applications to the power and cost advantages of standard-based short-range wireless networking. HRZB211 is ideal for a wide range of remote monitoring and control applications such as home control, meter reading, industrial automation, building automation, and security monitoring.

This manual contains vital information about HangRuiTuoYu HRZB211 embedded wireless transceiver modules. It includes information on how the HRZB211 can be easily provisioned, managed, and integrated into your existing products.

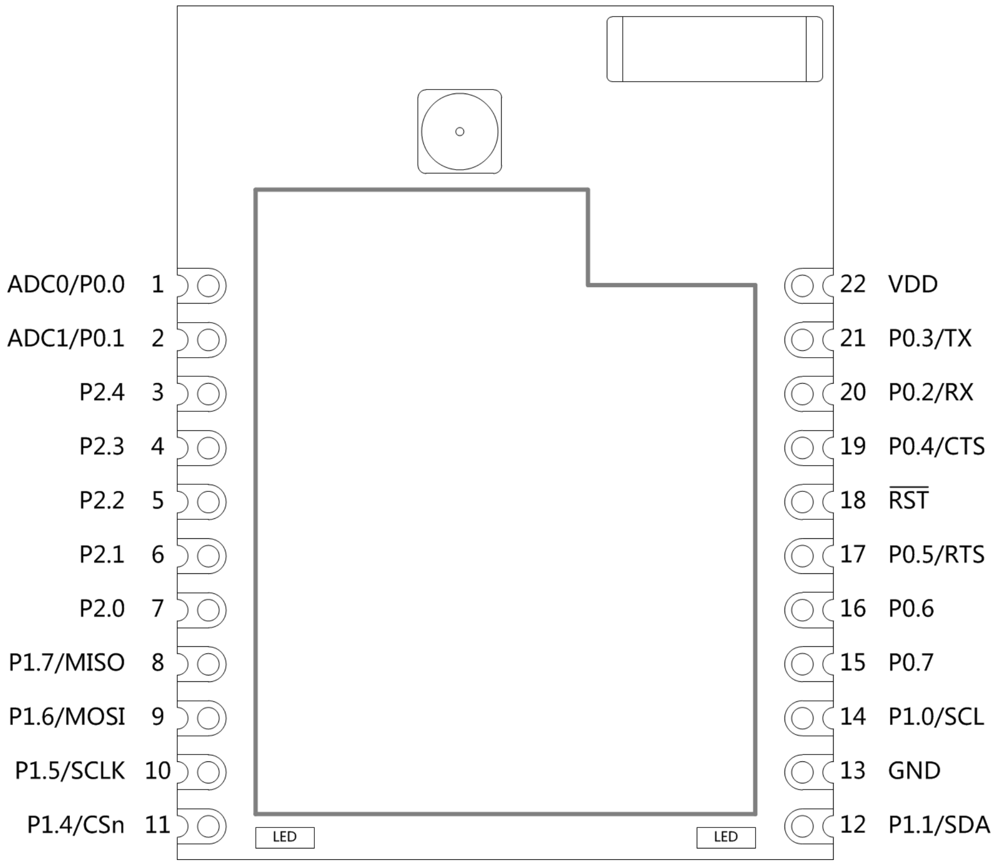
Following is the structure of this document.

- Chapter 2 contains information on the HRZB211 interface, performance and electrical specifications.
- Chapter 3 gives the absolute maximum ratings to warn users using the device in the proper circumstance.
- Chapter 4 specifies the operating conditions.
- Chapter 5 offers a high-level description of the network operations supported by the HRZB211, and how various network topologies can be configured to meet your application requirements.
- Chapter 6 contains step-by-step instructions on setting up an HRZB211 network. This network configuration guide is followed by a detailed description of the HangRuiTuoYu Command Set.
- Chapter 8 contains the example of HRZB211 module's installation.
- Chapter 10 gives readers definitions and invocation mechanisms needed to develop their own host applications based on HRZB211's flexible networking capabilities.
- Chapters 11 through 4 contain acronyms, mechanical dimensions, manufacturing re-flow specification, and part number information.

2 Module Specifications

Micro-controller (MCU)	MCU Clock Rate	32MHz
	FLASH ROM	256KB
	RAM	8 KB
RF	Frequency	2.4 GHz
	Receiver Sensitivity	-104dBm
	Air Data Rate	250 Kbps
	Transmit Range	~2000 meters (LOS)
	RF Channels	16 (5MHz)
	Transmit Power	1 to 20dBm
	Data Encryption	128-bit AES
	Antenna	Chip/Pin out
	Certification	FCC Part 15
Power Consumption	Transmit/Receive	120mA/35mA
	Sleep	1uA
Input/Output	Physical Pins	22
	Serial	UART
	A-to-D	Two 12-bit ADC
	# of Programmable GPIO	15
Physical	Operating Temperature	-40ºC to +85ºC
	Humidity (non-condensing)	10% to 90%

2.1 HRZB211 Interface Pin Definitions



HRZB211

Pin No	Name	Type	Function description
1	ADC0/P0.0	AI	ADC Input（0V~VDD）
2	ADC1/P0.1	AI	ADC Input（0V~VDD）
3	P2.4	DIO	Digital Input/Output
4	P2.3	DIO	Digital Input/Output
5	P2.2	DIO	Digital Input/Output
6	P2.1	DIO	Digital Input/Output
7	P2.0	DIO	Digital Input/Output
8	P1.7/MISO	DIO	Digital Input/Output
9	P1.6/MOSI	DIO	Digital Input/Output
10	P1.5/SCLK	DIO	To LED，Signal strength indication
11	P1.4/CSn	DIO	To LED, working status
12	P1.1/SDA	DIO	Digital Input/Output
13	GND	G	
14	P1.0/SCL	DIO	Digital Input/Output
15	P0.7	DIO	Digital Input/Output
16	P0.6	DIO	Digital Input/Output
17	P0.5/RTS	DIO	Digital Input/Output
18	RST	DI	Reset,low active
19	P0.4/CTS	DIO	Digital Input/Output
20	P0.2/RX	DI	UART receive for module（3.3V）
21	P0.3/TX	DO	UART transmit from module（3.3V）
22	VDD	P	Input Power（3.3V）

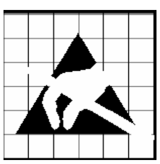
2.2 Firmware Capabilities Specification

Serial Port	Baud Rate	115200/57600/38400/19200/9600/…
	Configuration	8/N/1
	Maximum Payload over Serial Port	100 Bytes
	Header Length	5
	Checksum	1-byte XOR
	Command Modes Supported	AT Mode (off-line provisioning) Binary Command Mode Binary Data Mode Transparent: RS-232/485 emulation
Networking	Maximum of Network Identifiers	65534 (0 ~ 65533)
	Range of Node Identifiers	0: Reserved for Network Master 65534: Reserved for self-loop back 65535: Reserved for broadcast
Sleep Mode	External Wakeup	POR (Power On Reset) Pin input

3 Absolute Maximum Ratings

Parameter	Conditions	Min	Type	Max	Units
Voltage on any Pin		-0.3		3.6	V
Maximum Total Current through VCC, AV+, GND, and AGND,RFGND				800	mA
Maximum Output Current Sunk by any Port pin				100	mA
Maximum Output Current Sunk by any other I/O pin				50	mA
Maximum Output Current Sourced by any Port pin				100	mA
Maximum Output Current Sourced by any other I/O				50	mA
Storage Temperature		-55		125	°C

*Note: The absolute maximum ratings given above should under no circumstances be violated. Stress exceeding one or more of the limiting values may cause permanent damage to the device.



Caution! ESD sensitive device. Precaution should be used when handling the device in order to prevent permanent damage.

4 Operating Conditions

Parameter	Conditions	Min	Type	Max	Units
Supply voltage		2.7		3.6	V
Operating ambient temperature range		-40		85	°C
Humidity(non-condensing)		10%		90%	

5 Theory of Networking Operations

HRZB211 can be configured in a number of network topologies to meet different application needs. It allows the users to design a network that best matches their installation conditions and applications' needs. To design a network, it is empirical to understand how each individual HRZB211 should be configured, and what each nodes individual capabilities as well as constrains are.

In this Chapter we discuss the theory of networking operation of HRZB211's networking capabilities to lay the groundwork for later chapters. After reading this Chapter, users should have the system knowledge in assessing, configuring, deploying, and finally fine-tuning their HRZB211 networks in real installations.

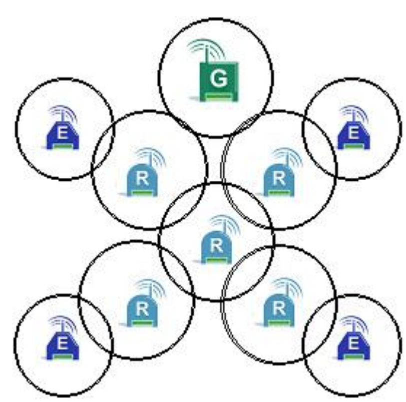
5.1 Wireless Networking Topologies

In this section, we describe the key distinctions between "connectivity" and "routing" topologies to establish the basic framework of wireless network design. We then describe the working details, benefits, and constraints and recommended use case scenarios for the several routing options the HRZB211 supports. This section provides a conceptual platform for readers before they use HRZB211 to build wireless networks.

5.1.1 Connectivity Topology Versus Routing Topology

While the generic phrase *network topologies* suggests wires or cables connecting a host with communicating nodes, wireless communication modules like the HRZB211 use a wireless broadcast medium to communicate. The HRZB211 is a low-power transceiver module optimized for low-cost and low power consumption. So rather than transmitting at high power or having a huge antenna to improve receiver sensitivity, a single HRZB211 transmits at relatively low power (10mW) and utilizes message routing capability to cover a larger area if necessary in some applications. And because of the broadcast nature of wireless transmission, it is important to realize the differences between *connectivity topology* and *messaging topology*.

Connectivity topology refers to the interconnect patterns at the Link level. In a wired network, topology refers to the physical wiring patterns among the nodes. Bus segments or point-to-point Links are some common connectivity topologies seen in Local Area Networks (LAN) or Wide Area Networks (WAN). In contrast, the connectivity pattern of a wireless network is usually visualized as overlapping radio circles or spheres, as illustrated here. The RF sphere implies both range and channelization, which means that nodes with overlapping bubbles are directly connected with one another.



So when considering a connectivity topology, the designer is usually concerned with design parameters such as overall coverage area, nodal density, and the transmission / reception characteristics of the transceiver modules. The characteristics could accidentally change due to varying external conditions and variables such as trucks, walls, trees, and other RF emitters.

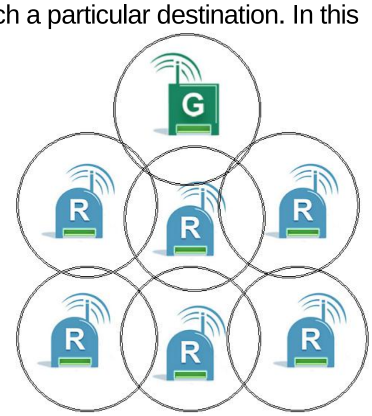
On the other hand, a routing topology is a routing pattern over a multi-hop network. It describes an imaginary wiring diagram, weaving together all network nodes, allowing any arbitrary point to initiate a message (either unicast or multicast) to any fellow node in the network. A routing topology is constrained by the underlying connectivity topology. But for some connectivity topology patterns in which multiple routing options are available (like most wireless networks), selecting the optimal routing topology for your network can be a challenge. Two scenarios are presented here for demonstration.

- **Scenario 1: Linear Network**

Let us examine a linear or “chain fence” scenario, in which any radio can only reach two immediate neighbors in opposite direction. In this extreme case, the choice of routing topology is constrained by the connectivity because there is only one deterministic way of getting a message from point A to point B in the whole network. This topology is common in pipeline monitoring applications and some traffic management and parking meter applications.

- **Scenario 2: Fully Meshed Network**

In this scenario, we increase the size of the RF sphere and make some changes to the relative position. Now one can see that the new connectivity topology offers a wider array of routing options. In this particular diagram, each node will have two or more paths to reach a particular destination. In this case, the routing topology is no longer a simple choice.



As illustrated in this scenario, routing topology decision for a low-power radio network involves the balance of many design objectives. The wireless network itself is a dynamic system, interacting with its environment incessantly. People movement, intermittent use of electrical appliances, and outside interference sources are all affecting the bubble size. Further complicating the decision process is the design objective to conserve battery consumption for battery-operated devices.

HRZB211’s rich wireless routing algorithm is designed to simplify the decision process and expedite the deployment of a reliable, inexpensive wireless infrastructure. Its feature-rich and flexible networking capability aims to provide the network designers with sufficient alternatives and performance margin to easily come to a “just-right” routing topology to adapt to or even overcome the constraints imposed by underlying connectivity topologies.

5.1.2 Star Topology

As its name suggests, a star routing topology is actually a hub-and-spoke system in which data traffic and network commands are routed through a central node, the **Master**. In this routing topology, peripheral nodes require direct radio contact with the **Master**, and interference or the failure of a specific node can render the network less reliable, as each node provides a single point of failure. Especially, the failure of the master node will result in complete system crash. To construct a star network using HRZB211, only one HRZB211 module needs to be configured as a **Master** node. The remaining HRZB211 modules can be programmed as an **End** node.

The most significant benefit of a star routing topology is its simplicity. The simplicity translates into very low-overhead protocol implementation, much lower overall device cost, very low-overhead routing information, and ease of administration. The central **Master** node can also assume many administrative roles such as certificate authority for authentication, or remote management gateway.

However, the simplicity comes with a price of flexibility. Because of the requirement to put every single end node within the reach of the **Master** node, the overall network coverage is limited. And star topology networks cannot scale up easily to accommodate high-density deployment. The concentrated message routing towards the **Master** node can easily create a hot spot and lead to congestion, packet loss, and performance degradation, depending on the data traffic profile.

The star topology is by far the most common architecture deployed today, and it is well suited for a variety of remote monitoring and control applications that do not need or cannot afford the cost and complexity overhead of a more sophisticated network topology.

5.1.3 Peer-to-peer (Mesh) Topology

Peer-to-peer, also known as mesh networking, is a free-form topology designed to be highly adaptive to the environment. Each node in an HRZB211 mesh network is a little router capable of re-assessing its routing decisions to provide the most robust, reliable network infrastructure possible. After configured as a mesh node (RN+ or Master), each HRZB211 is capable of monitoring surrounding RF conditions, neighboring node activities, and end-to-end packet error rate statistics to adjust its local routing decisions on the fly. Such adaptability is extremely valuable to network designs that are facing uncertain or unpredictable Link conditions.

Mesh topology uses both the RF broadcast nature as well as a set of route inquiry and maintenance commands to dynamically update the distributed routing information across the entire network. The mesh protocol supported by HRZB211 is similar to Ad hoc On-Demand Vector (AODV) routing, in which the node originating a message is responsible for establishing a suitable route by querying its immediate neighbors. The route queries process gradually ripples through the network until the destination confirms connectivity and initiates a reply. Such reply now ripples backwards toward the originator, accumulating vital routing statistics along its way. Finally, the originating node receives the most up-to-date route information and makes a routing decision based on that information. The newly computed routing information will age within a certain window and mandate new route computation after it expires to ensure route decision is based on fresh information.

Mesh is ideal for highly unstructured network deployment. When the deployment premise is open and potential interference sources or barriers are anticipated, mesh topology is a reliable way of ensuring wireless connectivity. Especially when deployment density is medium or high, the added redundancy by mesh topologies can add significant design margin and flexibility into the overall networks.

Given its more sophisticated capabilities, however, characterizing and validating a mesh network is more difficult and complicated compared to star or cluster tree networks. Unlike star or cluster tree, a mesh network dynamically adjusts the routing topologies and does not exhibit a fixed, predictable routing pattern. This makes the messaging latency highly dependent on the instantaneous Link quality and difficult to predict. More importantly, a qualitative comparison of mesh algorithms is always a challenging task even for the most savvy network designer.

Network designers usually deploy mesh for applications that require a highly reliable, highly available wireless infrastructure. Mesh networks should also be considered as a means to reduce initial network setup cost and post-installation maintenance needs by leveraging the self-configuring capabilities embedded inside HRZB211 modules.

5.2 Topology Selection

HRZB211's rich wireless routing algorithm is designed to simplify the decision process and expedite the deployment of a reliable, inexpensive wireless infrastructure. Its feature-rich and flexible networking capability aims to provide the network designers with sufficient alternatives and performance margin to easily come to a "just-right" routing topology to adapt to or even overcome the constraints imposed by underlying connectivity topologies.

Deciding the routing topology of your applications can be very easy with HRZB211. The decision usually needs answers for the following series of questions:

1. Worst-case and average-case connectivity topologies: What type of installation density do your applications call for (e.g., what is the longest and average distance between your devices), and what is the surrounding environment's conditions in terms of RF interference, building structure and moving objects?

2. Evaluate routing alternatives: select from one of the topologies discussed in this chapter. Based on the information from (1), select a core routing topology that meets your design objectives.

3. Fine-tune routing alternatives by selectively upgrading potential weak spots and balancing against power/resource design constraints.

6 Quick Steps in Establishing an HRZB211 Network

In this chapter we provide a simple guide to forming an HRZB211 network（The establishment of Mesh network please re. 6.1 and 6.2）. The generic flow of building an HRZB211 network consists of a series of steps provisioning the Master Node and non-Master nodes and making them recognize one another. The configuration procedure discussed in this chapter is based on those AT Mode or Binary Mode commands detailed in Chapter 7. This chapter also provides tips on verifying the connectivity of a newly formed network and describes procedures users should follow to reconfigure a network.

6.1 Special Note: Establishing a Full Mesh Network

A full ad hoc mesh network is appealing to many users because of its ease of configuration. In this configuration, all nodes are viewed as equals, and each of them will be a "trustworthy" neighbor to any other nodes within its radio contact. And many users prefer to deploy a full mesh network without going through the sequential process of joining each and every device into the network. Rather than assigning Network Layer address one at a time via Master Node, some users choose to pre-configure address information. Pre-configure address assignment works particularly well for full mesh network, since run-time path is established dynamically rather than relying on static parent-child relationship.

1. It is quite straight-forward to configure your HRZB211 devices into a full-mesh-capable device. You should prepare to setup every node with the following common configurations:
   - An identical RF Channel
   - An identical MAC Layer Network Identifier (from 0 to 65535)

   Note: the particular configure information please re. 6.2
2. Now provision a unique MAC Node Identifier into each module. The unique Node Identifier can be selected from the range of 0 to 65533. Note that Node 0 in a full mesh network does not have any supremacy over other nodes any more. A full mesh network can operate even without Node 0.
3. Turning on devices: For a full mesh network, devices can be turned on at any arbitrary order.
4. Validating connection: It is strongly recommended that you "walk" the entire network from any node that has an external connection that accepts HangRuiTuoYu's Binary Mode Command Set. For example, you can hook up a Personal Computer to any node and start querying the entire crew in the network. You can run such a "scan" continuously over an extended period to develop some ideas on your deployment environment as well as the network's stability.

6.2 About the Mesh Topology Configuration of Module

Introduce how to use binary command to configure mesh topology.

About the binary command, please reference to 7.2 **Binary Mode.**

The method is to set some related registers, command code is 0x87

The registers need to be set are:

0X70: send power, range from 0 to 7, 0 is the max

0X72: channel，0~15，

0X96: node type，master is 0，client is 1

0X99: set to 1

0X9A: set to 1

0X9E: 0

0X9F: 0xFF

0XA0: 0x62

0XB4: 0x01

0XB5: 0x01

0XB7: 0x00

0XBC: high bits of net node ID

0XBD: low bits of net node ID

0XBE: high bits of net ID

0XBF: low bits of net ID

0XC0: high bits of mac node ID, the same as 0xBC

0XC1: low bits of mac node ID, the same as 0xBD

For example, send command code: 81 00 FF FE 03 87 70 00 74, the function of this command is setting power to 0.

Return：C1 00 00 01 02 87 00 45

7 HRZB211 Command Set

HangRuiTuoYu supports two categories of external command sets. One is the familiar AT command set that is similar to those supported by Hayes-compatible modems. The second category of commands consists of binary instructions that enable a host processor to use HRZB211 as a wireless network interface.

Application developers usually use AT command set to query and set attributes on a standalone module. After the configuration completes, application software can then invoke a binary command set to issue commands and exchange data packets across the wireless network.

Based on these two command set categories, HRZB211 supports two modes when it communicates to the outside applications: **AT Mode** and **Binary Mode**. When HRZB211 powers up, it defaults to the binary mode. User issues special escape sequence to switch into AT Mode, and another special AT command to switch back into data mode.

This chapter is organized as follows:

- Section 7.1 presents the AT command set and detailed definitions on HRZB211's S Register definitions.
- Section 7.2.1 introduces the structure of HRZB211's generic frame format and field definitions.
- Sections 7.2.2 through 7.2.6 give detailed descriptions of the four types of command frames supported by HRZB211.
- Section 7.3 provides detailed information on every command request and its corresponding responses.

7.1 AT Command Mode

HRZB211 provides a host of AT commands to allow easy configuration of key attributes of an HRZB211 module. The following texts describe the AT commands, their parameters, and the responses. You can use any terminal emulation utility or UART communication library on a particular host platform to issue these AT commands to HRZB211.

AT String	Purpose	Parameter	Return String
+++	Escape sequence into AT Mode	N/A	Successful: no return value; returns O when a second "+++" is issued Error: Exxx
- - -N-	Escape sequence into transparent Mode	N = 0 ~ 65533, 65535, in decimal	N/A
===	Switch to Binary Mode	N/A	N/A
AT#n\r	Set MAC Layer Network Identifier	n = 0 ~ 65535	Successful: O Error: Exxx

AT String	Purpose	Parameter	Return String
AT@n\r	Set MAC Layer Node Identifier	n = 0 ~ 65534	Successful: O Error: Exxx
ATSxxx?\r	Query Register Value	xxx: S register index (in decimal)	Successful: O Error: Exxx
ATSxxx=yyy\r	Set Register Value	xxx: register index (in decimal) yyy: register value (in decimal)	Successful: O Error: Exxx
AT/$\r	Get IEEE MAC Address	N/A	LongMac=0xhhhhhhhhhhhhhhh h
AT/B\r	Get module firmware built timestamp	N/A	Month dd yyyy hh:mm:ss
AT/#\r	Get MAC Layer Network Identifier	N/A	MacNetID=n
AT/@\r	Get MAC Layer Node Identifier	N/A	ShortMacAddress=n
AT/S\r	Query All Register Values	N/A	S100=aaa S101=bbb S102=8 … S230=x
AT/V\r	Query Module Firmware Release Number	N/A	a.b.c
ATW\r	Write Back Settings	N/A	Successful: O Error: Exxx
ATR\r	Restore Default Settings	N/A	Successful: O Error: Exxx

7.1.1 AT Register Table

In this section we present a table of HRZB211 S Registers and valid range for each register location. These register entries can be read and set through the commands described in the previous section. The exact Register indexes and acceptable input values are summarized in the table below.

For maintenance reasons, some of these S Registers should not be modified and are only displayed for informational purpose. These entries are labeled as “Reserved” under the field “Access Type.” Readers are strongly advised **NOT** to modify these S Register settings, or HangRuiTuoYu cannot guarantee the firmware’s performance.

Register Name

Register Name	S Register Index (decimal)	Access Type	Purpose	Range (decimal)	Manufacturer Default (decimal)
UART Baud Rate	101	R/W	UART Baud Rate	1: 57600 bps 2: 38400 bps 3: 19200 bps 4: 9600 bps	2
UART Data Bit	102	R/W	Number of data bits	8:8 bit 9:9 bit	8
UART Parity	103	R/W	Parity bit	0:none 1:odd 2:even	0
UART Timeout	104	R/W	Timeout value, in milliseconds, for UART	N/A	8
UART Buffer Size	105	Reserved	UART Buffer size in bytes		143
UART Flow control	106	R/W	UART Flow control	0:FALSE 1:TRUE	0
RF Baud Rate	111	R	RF Baud Rate	0: 250 Kbps	0
RF Send Power	112	R/W	RF Send Power select Register	0: 20 dBm 1: 17 dBm 2: 14 dBm 3: 11 dBm 4: 8 dBm 5: 5 dBm 6: 2dBm 7: 1 dBm	0
RF Accept and Send buffer size	113	Reserved	RF Accept and Send buffer size		116
RF Channel	114	R/W	RF Channel Select Register	0 ~ 15 0: 2.405 GHz 1: 2.410 GHz ... 14: 2.475 GHz 15: 2.480 GHz	0
RF Frequency	115	R	RF Frequency	3: 2.4 GHz	3

Register Name	S Register Index (decimal)	Access Type	Purpose	Range (decimal)	Manufacturer Default (decimal)
Wait ACK TimeOut	141	R/W	Timeout, in 10 milliseconds	0 ~ 255	50
Retry Send Rreq For Myself	142	R/W	Number of retry times	0 ~ 255	1
Retry Send Mac Packet	143	R/W	Number of retry times	0 ~ 255	1
Wait Rrep TimeOut	144	R/W	Timeout, in milliseconds	0 ~ 255	100
Retry Send Rreq For Others	145	R/W	Number of retry times	0 ~ 255	1
Repeat MultiBroadCast	147	R/W	Number of repeat times	0 ~ 255	1
Node Type	150	R/W	Node Type Select Register	0: Master 1: RN+ 2: RN- 3: RFD 255: Unassigned	255
Routing Algorithm	158	R/W		0: AODV 1: Cluster Tree 2: CT/AODV	2
Table Expiration Value	159	Reserved	Expiration time, in seconds		255
Topology Type	160	R/W		0 ~ 255	255
Aodv TTL Value	163	R/W		0 ~ 255	21
Network State	170	R/W		0: Unassigned 1: JOIN NETWORK 2: LEAVE NETWORK 3: REPORT ACCEPT CHILD 4: REPORT LOST CHILD	0

Register Name	S Register Index (decimal)	Access Type	Purpose	Range (decimal)	Manufacturer Default (decimal)
Work Mode	173	R/W		0: HANGRUITUOYU FRAME MODE 1: AT COMMAND MODE 2: TRANSPARENT MODE	0
Transparent Mode destination, Upper Byte	174	R/W		0 ~ 255	255
Transparent Mode Destination, Low Byte	175	R/W		0 ~ 255	255
Transparent Mode LoopBack Flag	176	R/W		0: FALSE 1: TRUE	0
MAC Layer Ack Flag	180	R/W		0: FALSE 1: TRUE	1
NET Layer Ack Flag	181	R/W		0:FALSE 1:TRUE	1
Time Control	183	R/W	Control the time space of Net Link Checking, in seconds	0 ~ 255	0
Digital Input sleep gap	184	R/W	Refer to Digital Input Commands definition	0 ~ 20, in 100ms 0: Disable this function	0
Digital Input monitor's Node ID, Upper Byte	185	R/W		0 ~ 255	0
Digital Input monitor's Node ID, Lower Byte	186	R/W		0 ~ 255	0

Register Name	S Register Index (decimal)	Access Type	Purpose	Range (decimal)	Manufacturer Default (decimal)
Network Layer Node ID, Upper Byte	188	R/W		0 ~ 255	255
Network Layer Node ID, Lower Byte	189	R/W		0 ~ 255	255
MAC Layer PAN ID, Upper Byte	190	R/W		0 ~ 255	255
MAC Layer PAN ID, Lower Byte	191	R/W		0 ~ 255	255
MAC Layer Node ID, Upper Byte	192	R/W		0 ~ 255	255
MAC Layer Node ID, Lower Byte	193	R/W		0 ~ 255	255
MAC Layer Beacon Mode(reserved for future use)	194	R/W		0 ~ 255	0
MAC Layer Node Type(reserved for future use)	195	R/W		0 ~ 255	0
Security Mode(reserved for future use)	196	R/W		0 ~ 255	255
AppLocalizer Time	230	R/W	Control the time space of Tag request, in 0.1seconds	0 ~ 255 0: Disable this function	0
LED Flag	231	R/W	Set the ports used by LEDs free when this flag is FALSE, then they can be used as GPIOs	0: FALSE 1: TRUE	1
Remote Flash	232	R/W	Allow writing	0: FALSE	0

Register Name	S Register Index (decimal)	Access Type	Purpose	Range (decimal)	Manufacturer Default (decimal)
Flag			remote flash or not	1: TRUE	
Sleep mode flag	233	R/W	Entry sleep mode	0:FALSE, 1:TRUE	0
Sleep base time	234	R/W	Sleep base time	1~40	4
Uart Tag	236	R/W	Entry Uart Tag mode or choose the tag table type	0~4	0
Set ADC Vref	242	R/W	Set ADC Vref	0~3	0

7.1.2 AT Command Error Codes

When AT commands execute successfully, HRZB211 firmware returns an upper case “**O**” as a success indication. In the case of execution failure, HRZB211 firmware returns one of the following three error codes to indicate the condition.

Error Code	Error Diagnosis
100	Invalid Command
101	Invalid Register
102	Invalid Value

7.2 Binary Mode

In Binary Mode, host applications use binary-formatted command and responses to command the local modules as well as communicate to remote nodes across the network. This highlights the key utility of Binary Mode operations compared to AT Mode: to communicate and command remote modules over the network formed by multiple modules. That said, there are still shortcut commands in Binary Mode to allow users to quickly perform local module access without forcing the application to go through mode switches. In the simplest terms, Binary Mode and AT Mode have overlapping functionalities and are designed to complement each other.

HRZB211 supports four types of frames in its Binary Mode. **Command Request, Command Response, Data Request, and Acknowledgment.**

To use HRZB211's Binary Mode, a Host Application starts with building **Command Request Frames** to query, configure, and command a remote HRZB211 for networking-related functions. The remote HRZB211 module will automatically return a **Command Response Frame** to notify the execution result to the command-issuing module. The sending application then parses the **Command Response Frame** to take further actions. Some configuration records and sensor information natively supported by HRZB211 can also be retrieved using **Command Request** and **Command Response**. These commands are built-in to HRZB211, and these **Commands** cannot be extended or modified by the users.

On the other hand, host applications use **Data Request** and **Acknowledgement Frames** to exchange user-specific data. HRZB211's transport the data frames in an end-to-end fashion without interpreting or manipulating the payload in a **Data Request Frame**. The destination HRZB211 will automatically generate an Acknowledgement Frame to report the reception status of the Data Request Frame. After the network topology is established, **Data Request Frame** is the main interface that application developers can use to exchange information among multiple HRZB211 modules. These frames can also be used to carry user-defined network-wide commands, such that HRZB211 can be extended to support any custom commands users desire.

All these frames can be exchanged from one HRZB211 module to a peer module within the same network. The routing of these frames over any given topology is handled by HRZB211's embedded firmware transparently.

7.2.1 Generic Frame Format

All four types of frames – Command Request, Command Response, Data Request, and Acknowledgment – use the same generic frame structure: five (5) bytes of packet header descriptor, 0 to 97 bytes of frame payload, and one (1) byte of XOR checksum at the end of packet.

All binary frames follow the following variable-length frame structure:

Control Header (1)	Link Quality Indicator (1)	Destination Address (2)	Payload Length (1)	Payload (0 – 100)	XOR Checksum (1)

Following is the detailed description of the common packet header descriptor.

7.2.1.1 Control Header Field

Length: one byte

Bit Field Definition:

Bit 7,6,5: Binary Frame Type:

100	command request
110	command response

101	data request
111	data acknowledgement

Bit 4: Reserved for future use. Default to 0.

Bit 3,2,1,0: Packet Sequence Number, modulo 16.

NOTE: This sequence number is specifically designed for user applications, the nearby packets must have different sequence numbers, for example, the sequence numbers change circularly from 0 to 15。 HRZB211's firmware maintains separate sequence numbers for data packets. They are transparent to Binary Mode users.

7.2.1.2 Link Quality Indicator

Length: one byte

Bit Field Definition:

Bit 7 ~ 0: A 8-bit hex value representing the incoming packet's Link Quality

Description: The Link Quality Indicator (LQI) is an estimate on the packet's signal integrity. Its value ranges from 0 to 255. The higher the value, the better the signal quality. This estimate is derived from IEEE 802.15.4 PHY layer processing performed by any compliant IEEE 802.15.4 transceiver. Users can use this information to assess the MAC-Link quality of a node's surrounding devices. This estimate can be used in conjunction with RSSI.

7.2.1.3 Destination Address Field

Length: two bytes

Bit Field Definition:

Bit 15 ~ 0: Destination Node’s Network Address

Description: 0x0000, 0xFFFE, and 0xFFFF are all reserved address -- 0x0000 for Network Master, 0xFFFE for loopback (to the sender itself), and 0xFFFF for broadcast.

7.2.1.4 Payload Length Field

Length: one byte

Bit Field Definition:

Bit 7~0: Represents the payload length (excluding the 5-byte header and 1-byte XOR checksum) in hexadecimal.

Description: Its valid range should be from 0x00 to 0x61 (decimal 97).

7.2.1.5 Payload Field

Length: variable length from 0 to 97 bytes

Bit Definition: User defined.

Description: The magic number 97 is due to the limitation from IEEE 802.15.4 MAC Layer's maximum payload size.

7.2.1.6 XOR Checksum Field

Length: one byte

Bit Definition:

Bit 7~0: XOR Checksum

Description: The XOR checksum is calculated by perform a byte-wide XOR sum on the entire packet header and payload. If an XOR checksum fails, the frame will be discarded automatically.

7.2.2 User Command Request Frame

In Command Request Frame, an additional byte is used to denote a **Command Code** identifier. HangRuiTuoYu provides a set of built-in command/responses to allow users to manage and retrieval information regarding the networks as well as the sensor information provided by HangRuiTuoYu's hardware solution. Each command code identifier will possess its own syntax for both request and response.

Control Header (1)		Link Quality Indicator (1)	Destination Address (2)	Payload Length (1)	Command Code (1)	Parameters (0 – 99)	XOR Checksum (1)
Command Request (4-bit) **b1000**	Sequence Number (4-bit)						

When composing a Command Request Frame, user applications should supply the following information:

- A four-bit, user-defined packet sequence number: this number will be echoed back in receiver's Command Response Frame.

- Destination node's network address: Combined with the Packet Sequence Number, users can use these two numbers to uniquely match an incoming Response to a pending Command.
- The total payload length (up to 0x60)
- The command code: refer to the table in this section.
- The Command parameter: refer to Command Synopsis
- And the XOR checksum on all the bytes preceding the last

When sending a Command Request Frame, user applications should be ready to manage three possibilities:

1. First, the request completes successfully with the expected Response. In this case, the Command Response Frame will be available in the receiving buffer, and host applications can read the serial port input buffer to gather the Response frame.
2. The second condition is that a remote node returns an error indication. In this case, the end-to-end communication is working properly, but the command request is not accepted. Check command syntax and values to correct such problems.
3. The third condition is potentially a communication failure or invalid local command. For communication failure, users may experience continuing checksum error or timeout. In this case, check your communication quality and environment (e.g., moving the destination node closer to the transmitter, or switch to a simpler network topology.) For an invalid local command, verify that you are using the correct network address to address the local module, and the command is formatted correctly.

7.2.3 HRZB211 Command Request Code Summary

Following is a summary of the Command Request set currently supported by HRZB211, firmware release v2.1.05. Please refer to Command Request Frame Synopsis in Section 7.3 , for complete, individual command's information.[1]

Command Category	Command Name	Command Code (hex)
Sample and ADC	Get HRZB211 ADC Sample	0x81
	Get HRZB211 RSSI Sample	0x82
Module Settings	Get AT Mode S Register Setting	0x86
	Set AT Mode S Register Setting	0x87
Module MAC Settings	Get MAC Address	0x8B
Power Management	Get Firmware Version Number	0x8C

[1] The command set can be subject to change without notice. Please refer to HangRuiTuoYu's website for the latest documentation and firmware release.

Command Category	Command Name	Command Code (hex)
	Soft Reset Module	0x8F
	TRACERT	0xAA

7.2.4 HangRuiTuoYu Command Response Format

<table>
<tr><td colspan="2">Control Header
(1)</td><td rowspan="2">Link
Quality
Indicator
(1)</td><td rowspan="2">Destination
Address
(2)</td><td rowspan="2">Payload
Length
(1)</td><td rowspan="2">Command
Code
(1)</td><td rowspan="2">Response
(0 – 99)</td><td rowspan="2">XOR
Checksum
(1)</td></tr>
<tr><td>Command
Request
(4-bit)
b1100</td><td>Sequence
Number
(4-bit)</td></tr>
</table>

Command Response Frame is used to indicate back to the originator the execution results of a Command Request Frame.

If the command executes correctly, first the Command Code field in the Response Frame will echo the original command code. Further, a destination node will return any result in the RESPONSE field. If there is no result to return to the sender a value of 0x00 will be placed in the RESPONSE field

If the command execution fails, the destination node will place a 0xFF into the Command Code field. Further the very first byte in Response field will contain an error code for diagnosis purpose. The following table is a summary of possible error codes.

Error Code	Value (hex)	Comments
ERROR_XOR_ERROR	0x01	Checksum error
ERROR_SEND_FAIL	0x02	Send failure
ERROR_COMMAND	0x03	Invalid Command
ERROR_CMD_PARAM	0x06	Invalid Command Parameter
ERROR_DEST_ERROR	0x07	Invalid Destination Address
ERROR_NET_BUSY	0x09	Network Busy

7.2.5 HangRuiTuoYu Data Request Frame

Control Header (1)		Link Quality Indicator (1)	Destination Address (2)	Payload Length (1)	Data Payload (0 – 100)	XOR Checksum (1)
Command Request (4-bit) **b1010**	Sequence Number (4-bit)					

In this Data Request Frame, applications can deposit the application-specific data (of up to 97 bytes) into the Data Payload and transmit it to the target receiver. The receivers are expected to return an Acknowledgment Frame.

7.2.6 HangRuiTuoYu Acknowledgment Frame

<table>
<tr><td colspan="2">Control Header
(1)</td><td rowspan="2">Link
Quality
Indicator
(1)</td><td rowspan="2">Destination
Address
(2)</td><td rowspan="2">Payload
Length
(1)</td><td rowspan="2">Error Code
(1)</td><td rowspan="2">Error Type
(1)</td><td rowspan="2">XOR
Checksum
(1)</td></tr>
<tr><td>Command
Request
(4-bit)
b1110</td><td>Sequence
Number
(4-bit)</td></tr>
</table>

If a Data Request Frame is received successfully, the receiver will return a Data Acknowledgement Frame, back to the originator, with 0x00 for both Error Code and Error Type fields. For error conditions, Error Code will be set to 0xFF and error type will contain one of the diagnostic error code shown in the table below.

Error Type	Value (hex)	Comments
ERROR_XOR_ERROR	0x01	Checksum Error
ERROR_SEND_FAIL	0x02	Transmission Failed
ERROR_DEST_ERROR	0x07	Invalid Destination Address
ERROR_NET_BUSY	0x09	Network Busy

7.3 HangRuiTuoYu Command Synopsis

The following sections describe in detail the current command set available on HRZB211. Users can refer to this information to build the command library for their particular host application platforms.

Get HRZB211 ADC0 Sample

Read the sample from HRZB211's ADC

Command Code

0x81

Description

This command is used to retrieve the sample from HRZB211's built-in analog-to-digital converter (ADC).

.

Command Parameters

ADC Channel	1 Byte	0x00: enable ADC#0 0x01: enable ADC#1

Response

ADC High Byte	1 Byte	the most significant 4 bits of the sample (right-aligned)
ADC Low Byte	1 Byte	the 8 least significant bits of the sample

Get HRZB211 RSSI Reading

Read HRZB211 RSSI reading

Command Code

0x82

Description

This command retrieves the RSSI value, in dBm, from HRZB211. The dBm is a signed value. For instance, a reading of “B0” (hex) represents an RSSI value of-80dBm.

Command Parameters

N/A

Response

RSSI	1 Byte	RSSI value in hexadecimal, a signed value

Get AT Mode S Register Setting

Get AT Mode S Register Setting

Get a particular S Register's value under AT Mode

Command Code

0x86

Description

This is a shortcut for getting an S Register's value under AT Mode. It is equivalent to issuing ATSxxx? under AT Mode. The difference is that now this capability now can be used across the network.

Command Parameters

S Register Location	1 Byte	S Register index in hexadecimal

Response

S Register Value	1 Byte	Value in the requested S Register in hexidecimal

Set AT Mode S Register Setting

Set a particular S Register's under AT Mode

Command Code

0x87

Description

This command can be used to set a remote module's S Register. Users are advised to use this command with caution. Improper use of this command can result in modules unable to communicate to the rest of the network.

Command Parameters

S Reigster Location	1 Byte	S Register index in hexadecimal
S Register Value	1 Byte	Value for the S Register in hexidecimal

Response

Command Confirmation	1 Byte	0x00 (constant)

Get MAC Address

Get MAC layer hardware address

Command Code

0x8B

Description

This command retrieves an HRZB211 module’s IEEE 64-bit MAC hardware address. For HRZB211, this attribute is unused.

Command Parameters

N/A

Response

MAC Address	8 Byte	64-bit IEEE MAC address, MSB first

Get Firmware Version Number

Get release number of HRZB211 module firmware

Command Code

0x8C

Description

This command retrieves the firmware release number on the destination HRZB211 module.

Command Parameters

N/A

Response

Major	1 Byte	Major release number, in hex
Minor	1 Byte	Minor release number, in hex
Revision	1 Byte	Revision number, in hex

Soft Reset

Reset HRZB211 module

Command Code

0x8F

Description

This command triggers a soft reset of the destination HRZB211. The destination module will retain all its network settings and be able to communicate with the rest of the network after this soft reset.

Command Parameters

N/A

Response

Command Confirmation	1 Byte	0x00 (constant)

TRACERT

Trace the routing path

Command Code

0xAA

Description

This command retrieves the outgoing path from local HRZB211 module to the destination module and the returning path from the destination module to local module. Each path records the ordinal Network Layer Node IDs.

Command Parameters

N/A

Response

Marker(0xAA 0x55)	2 Byte
Outgoing Path	2 Byte per hop
Marker(0xAA 0x55)	2 Byte
Returning Path	2 Byte per hop

8 Example of installation

When put the module on the target PCB to perform ZigBee wireless transmission. Plug the module into socket with correct direction shown below. Make sure no ESD discharge happened. Make sure do not hot plug.

ZigBee module

Put the end up which chip antenna mounted.

When power on, the green LED on the module will be flashing (power), about 5 seconds later, the module into the working state.

9 Code of PC obtain the module's firmware version information

```
...

// Open com port

DCB      dcb   = {0};

HANDLE hCOM = CreateFile(_T("COM1"), GENERIC_READ | GENERIC_WRITE,
0, 0, OPEN_EXISTING, 0, NULL);

// Set baud rate

dcb.DCBlength = sizeof(DCB);

dcb.BaudRate   = 38400;

dcb.ByteSize   = 8;

dcb.StopBits   = ONESTOPBIT;

dcb.Parity     = NOPARITY;


SetCommState(hCOM, &dcb);

...

BYTE   btBuf[256];

int    i       = 0;

int    nXOR    = 0;

DWORD dwLen = 0;
```

```
static int nSN;


// Build packet
nSN++;
btBuf[0] = 0X80 + (0X0F & nSN);   // Packet head.
btBuf[1] = 0X00;                  // LQI。
btBuf[2] = 0X00;                  // High 8 bits of destination address
btBuf[3] = 0X01;                  // Low 8 bits of destination address
btBuf[4] = 0X01;                  // Payload length
btBuf[5] = 0X8C;                  // Payload. Obtain firmware version command
// Compute XOR bit by bit
for (i = 0, nXOR = 0; i < 6; i++)
{
    nXOR ^= btBuf[i];
}
btBuf[6] = nXOR;                  // XOR bit by bit
...
// Send packet
WriteFile(hCOM, btBuf, 7, &dwLen, NULL);
...
```

```
ZeroMemory(btBuf, sizeof(btBuf));

// Receive Packet

ReadFile(hCOM, btBuf, 10, &dwLen, NULL);

// Check length

if (dwLen != (btBuf[4] + 6))

{

        ...

}

// Compute XOR bit by bit

for (i = 0, nXOR = 0; i < dwLen; i++)

{

        nXOR ^= btBuf[i];

}

// Chenk parity

if (0 != nXOR)

{

        ...

}

// Check packet head

if (0XC0 != (btBuf[0] & 0XF0))
```

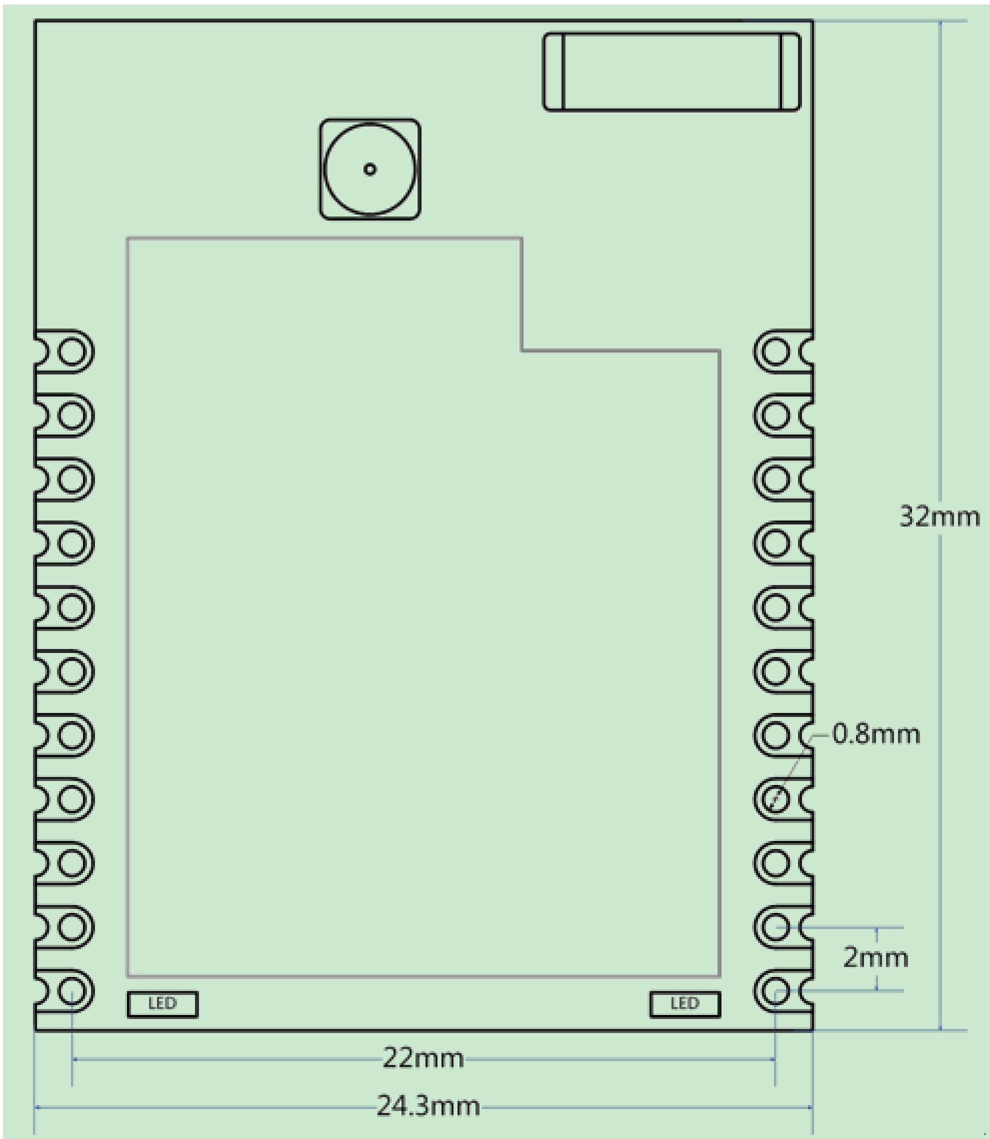
```
{
        ...
}
// Check command code
if (0XFF == btBuf[5])
{
        ...
}
...
// btBuf[6] is main version
// btBuf[7] is subsidiary version
// btBuf[8] is revised version
```

10 Terminologies and Acronyms

ADC	Analog to Digital Converter
AMR	Automatic Meter Reading
CFB	Cipher Feedback Mode
CMOS	Complementary Metal Oxide Semiconductor
CPU	Central Processor Unit
DES	Data Encryption Standard
FCC	Federal Communication Committee
FSK	Frequency Shift Keying
IDE	Integrated Development Environment
IF	Intermediate Frequency
ISM	Industrial Scientific Medical
ISR	Interrupt Service Routine
LOS	Line of Sight
LPF	Loop Filter
LQI	Link Quality Indicator
LSB	Least Significant Bit (or Byte)
MAC	Medium Access Layer
MSB	Most Significant Bit (or Byte)
PCB	Printed Circuit Board
PHY	Physical Layer
POR	Power On Reset
RAM	Random Access Memory
RF	Radio Frequency
RSSI	Received Signal Strength Indicator
RTC	Real-Time Clock
RX	Receive
SFR	Special Function Register
SPI	Serial Peripheral Interface
SRAM	Static Random Access Memory
SRD	Short Range Device
TQFP	Thin Quad Flat Pack
TX	Transmit
UART	Universal Asynchronous Receiver/Transmitter

11 Mechanical Drawings and Ordering Information

11.1 HRZB211 Dimensions



11.2 Re-flow Temperature Specifications

Recommend soldering base on OPC/JEDEC J-STD-020B standard.

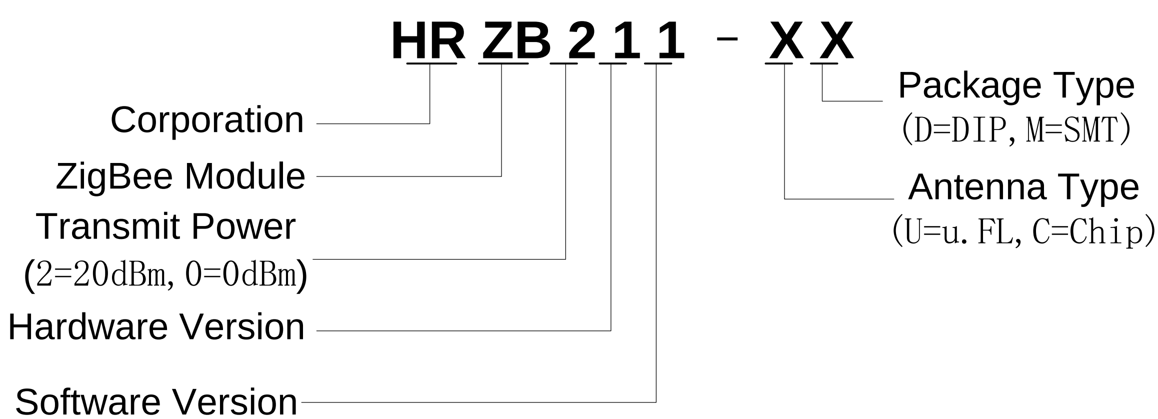
	Ideal (ºC)	Maximum (ºC)
Maximum Re-flow Temperature	215	230

11.3 Solder Paste Recommendations

Recommend soldering base on OPC/JEDEC J-STD-020B standard.

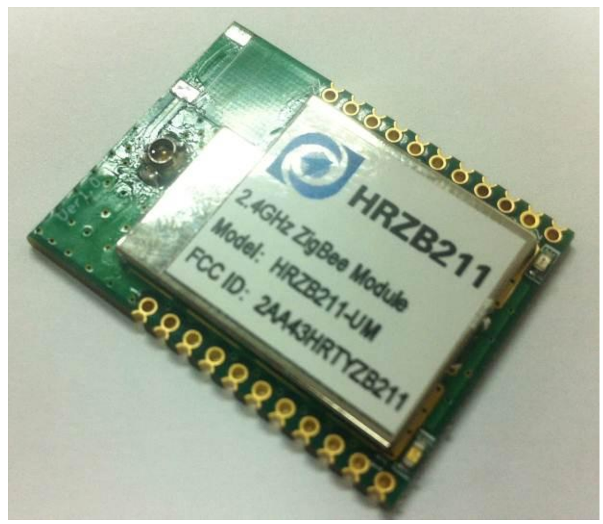
	Alloy Composition	Solidus (ºC)	Liquidus (ºC)	Shear MPa
Johnson Alloy #806	In/48Sn (e)	118	118	

11.4 Ordering Information



11.5 Photos of Product

HRZB211-CD **HRZB211-CM**



HRZB211-UD **HRZB211-UM**