E18-2G4U04B User Manual

CC2531 ZigBee USB Wireless packet capture tool

成都亿佰特电子科技有限公司

Chengdu Ebyte Electronic Technology Co.,Ltd.

1 Overview

1.1 Brief Introduction

E18-2G4U04B is a very small USB interface 2.4GHz band ZigBee protocol wireless packet capture tool designed and produced by EBAI.

E18-2G4U04B uses the original imported CC2531 RF chip of Texas Instruments (TI) company in the United States. The chip integrates 8051 single-chip microcomputer and wireless transceiver. The factory firmware supports TI Packet Sniffer software to carry out packet capture test. Packet Sniffer can be used to analyze the protocol quickly, and users can also do secondary development.

1.2 Feature

- Communication distance tested is up to 200m;
- Maximum transmission power of 2.5mW, software multi-level adjustable;
- Built-in ZigBee protocol stack;
- Support direct drive of peripherals such as ADC, PWM, GPIO;
- Support UART transparent transmission, easy to use;
- Built-in 32.768kHz clock crystal oscillator;
- Support the global license-free ISM 2.4GHz band;
- Built-in low-power 8051 core processing;
- Rich resources, 256KB FLASH, 8KB RAM;
- Support 2.0V~3.6V/USB power supply, and the power supply above 3.3V can guarantee the best performance;
- Industrial grade standard design, support for long-term use in -40 to 85 °C;
- PCB antenna

1.3 Application

- Home security alarm and remote keyless entry;
- Smart home and industrial sensors;
- Wireless alarm security system;
- Building automation solutions;
- Wireless industrial-grade remote control;
- Health care products;
- Advanced Meter Reading Architecture(AMI);
- Automotive industry applications.

2. Specification

2.1 Limit parameter

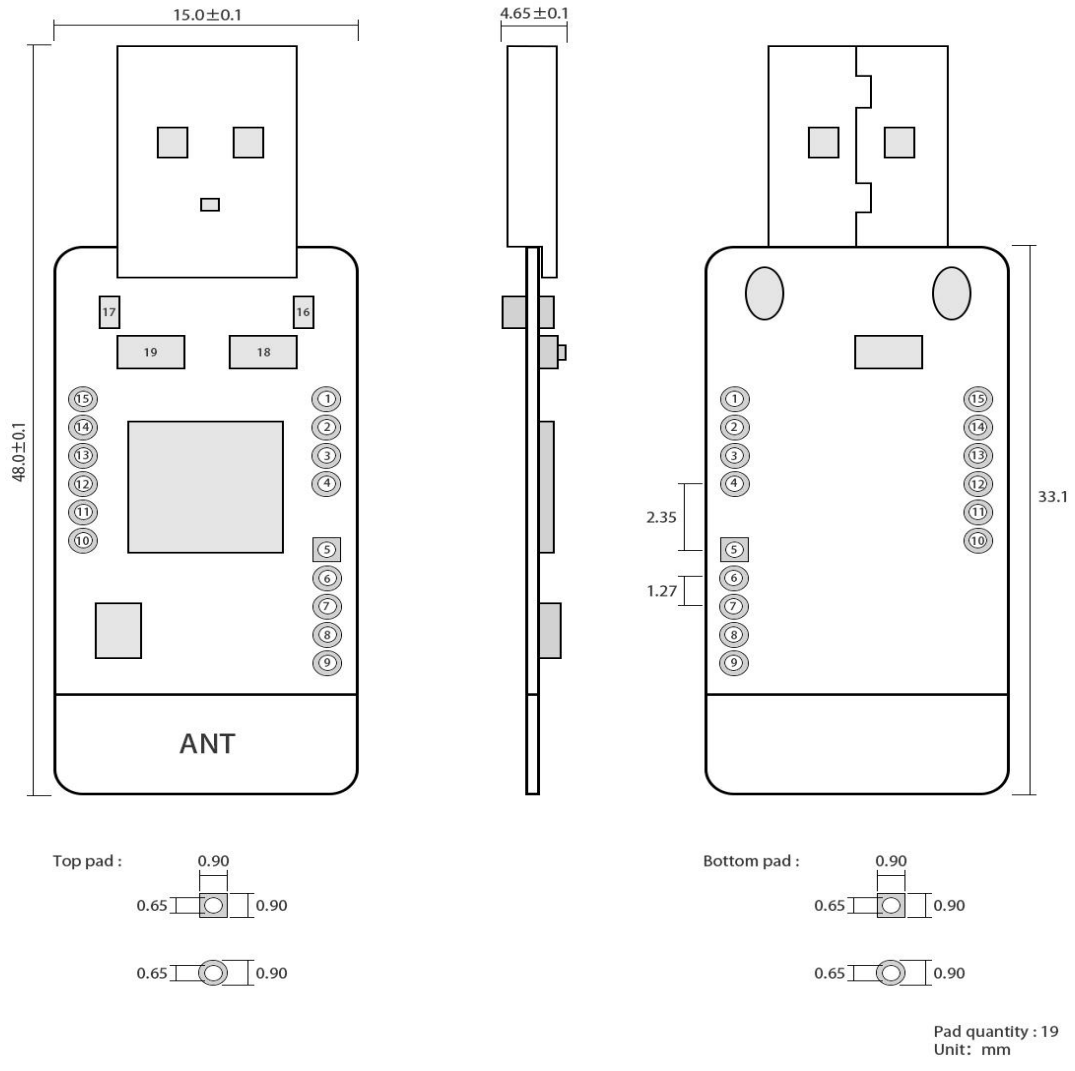
Main parameter	Performance		Remark
	Min.	Max.	
USB supply voltage（V）	0	5.5	Voltage over 5.5V will cause permanent damage to module
PCB power supply voltage（V）	0	3.6	Voltage over 3.6V will cause permanent damage to module
Blocking power（dBm）	-	10	Chances of being burn down is slim when used in short distance
Operating temperature（℃）	-40	85	

2.2 Operating parameter

Main parameter		Performance			Remarks
		Min.	Typ.	Max.	
Operating voltage（V）		2.7	5	5.5	powered by USB
Operating voltage（V）		2.0	3.3	3.6	powered by pcb power supply hole
Communication level（V）			3.3		For 5V TTL, it may be at risk of burning down
Operating temperature（℃）		-40	-	85	Industrial design
Operating frequency（MHz）		2.394	-	2.507	Support ISM band
Power consumption	TX current（mA）		31.5		Instant power consumption
	RX current（mA）		26		powered by USB
	Sleep current （μA）				
Max Tx power（dBm）		3.6	4.0	4.5	
Receiving sensitivity（dBm）		-95.5	-96.4	-97.5	air data rate is 250kbps

Main parameter	Description	Remarks
Distance for reference	200 m	Test condition：clear and open area, antenna gain: 5dBi，antenna height: 2.5m，air data rate: 250kbps
Protocol	ZigBee	
Powered by	USB	
Interface	1.27mm	
IC	CC2531F256RHAT/QFN40	
FLASH	256 KB	
RAM	8 KB	
Core	8051 MCU	
Size	59* 18mm	with housing
Antenna	PCB	

3 Size and pin definition



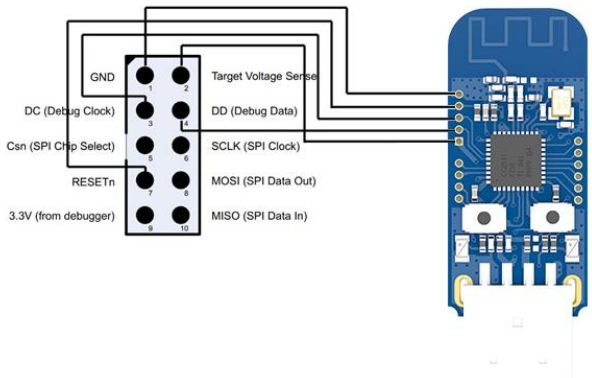
No.	Name	Direction	Function
1	P1.4	Input/output	GPIO（see more from CC2531 datasheet）
2	P1.5	Input/output	GPIO（see more from CC2531 datasheet）
3	P1.6	Input/output	GPIO（see more from CC2531 datasheet）
4	P1.7	Input/output	GPIO（see more from CC2531 datasheet）
5	VCC	Power supply	2.0V—3.6V（do not power the module via USB at same time）
6	DD	Input/output	P2_1 for program download（see more from CC2531 datasheet）
7	DC	Input/output	P2_2 for program download（see more from CC2531 datasheet）
8	RESET	Input	Reset(Reset circuit available）
9	GND	Power supply	Ground
10	P0.2	Input/output	GPIO（see more from CC2531 datasheet）
11	P0.3	Input/output	GPIO（see more from CC2531 datasheet）
12	P0.4	Input/output	GPIO（see more from CC2531 datasheet）
13	P0.5	Input/output	GPIO（see more from CC2531 datasheet）
14	P0.6	Input/output	GPIO（see more from CC2531 datasheet）
15	P0.7	Input/output	GPIO（see more from CC2531 datasheet）
16	LED	Signal indicator	Connect to P1.1 of CC2531，drive of high level lights
17	LED	Signal indicator	Connect to P0.0 of CC2531，drive of low level lights
18	Button	Function	Connect to P1.3 of CC2531，effective at low level
19	Button	Function	Connect to P1.2 of CC2531，effective at low level
See detailed size from pcb lib.			

- About more details about pin definition,software drive and protocol, please refer to official *CC2531 Datasheet* from TI.

4 Instruction

4.1 Burn program

E18-2G4U04B wireless packet capture tool built-in 8051 MCU, program download can use CC Debugger;



4.2 TI Packet Sniffer

The factory firmware is with TI Packet Sniffer available, easy to use and test. With Packet Sniffer, user can do protocol analysis quickly. Click link below to download, http://www.ebyte.com/pdf-down.aspx?id=1093

5 Software Programming

It is recommended to use the Code Composer Studio (CCS) Integrated Development Environment (IDE) for wireless connectivity.

Code Composer Studio is an integrated development environment (IDE) that supports TI's family of microcontrollers and embedded processors. Code Composer Studio includes a complete set of tools for developing and debugging embedded applications. It includes a C/C++ compiler for optimization, a source code editor, a project build environment, a debugger, a descriptor, etc.. The intuitive IDE provides a single user interface to help you through every step of the application development process. Familiar tools and interfaces allow users to get started faster than ever before. Code Composer Studio combines the benefits of the Eclipse software framework with TI's advanced embedded debugging capabilities to provide embedded developers with a compelling, feature-rich development environment.

5.1 FAQ about TI ZigBee

There are differences between different versions of TI's ZigBee protocol stack, how to choose the appropriate protocol stack for product development.

TI ZigBee protocol stack Z-Stack from the original Z-Stack 0.1 to the familiar Z-Stack 2.5.1a, and now Z-Stack Home 1.2.1, Z-Stack Lghting 1.0.2, Z-Stack Energy 1.0 .1, Z-Stack Mesh 1.0.0. During the upgrade process of the protocol stack, TI mainly worked on the protocol stack in two aspects. 1) According to the ZigBee Alliance's ZigBee Specification, some new feature additions were made. For example, ZigBee2007 is a tree routing, Mesh routing is in ZigBee Pro, and routing algorithms such as MTO and Source Routing are considered, i.e. corresponding new features are added to the protocol stack. There are some amendments to related bugs in Spec, for example, some descriptions are ambiguous; 2) Fixing bugs in the TI ZigBee protocol stack itself. The difference between a version of the protocol stack and the previous version of the protocol stack can be found in the Release Note in the protocol stack installation directory.

After Z-Stack 2.5.1a, TI's protocol stack did not continue to be released directly in the form of Z-Stack 2.6.x, but was released in accordance with the Application Profile, because TI hopes that developers choose protocol according to the actual application. A more targeted protocol stack is being developed. A protocol stack such as Z-Stack Home 1.2.1 mainly consists of two parts, 1) Core Stack, which is the continuation of the previous Z-Stack 2.5.1a, which can be installed in the protocol stack. Found in the Z-Stack Core Release Notes.txt file, Version 2.6.2. 2) Application protocol stack Profile related, this part is mainly related to the actual application. The Home Automation protocol stack is related to ZigBee Home Automation Profile. Similarly Z-Stack Lghting 1.0.2 and Z-Stack Energy 1.0.1 are also a Core Stack plus a profile on the app.

1)Z-Stack Home 1.2.2a for the development for smart home

2)Z-Stack Lighting 1.0.2 for the development of ZLL related product

3)Z-Stack Energy 1.0.1 for the development of smart energy, Meter, In Home Display

4)Z-Stack Mesh 1.0.0 for the development of private application,standard ZigBee, Mesh routing, etc. Defined by users themselves.

After the ZigBee Alliance released the ZigBee 3.0 protocol, the latest ZigBee protocol stack is Z-Stack 3.0. Currently it supports CC2530 and CC2538.

How do products carry out standard ZigBee test certification, what do you need to know and what process you need to take?

Take the development of standard ZigBee Home Automation related products as an example. First, developers develop products in accordance with the products described in the ZigBee Home Automation Profile Specification, which can be downloaded at www.zigbee.org. After completing the product development, the development needs to understand the ZigBee Home Automation Profile Test Specification. This document describes the relevant test items that a specific product needs to be tested in Test House. The document can also be downloaded at www.zigbee.org, in addition to the above. There is also a PICS document in addition to the two documents. This document is dedicated to describing the functions that need to be supported by the certification test product. The developer checks the document according to the actual function of the development product and the functions required in the specification. The following is the flow of testing,

1) First join the ZigBee Alliance, usually with the help of a test lab.

2) Send the sample to the test lab and complete the PICS document.

3) The first round of pre-test, the test laboratory feedback on the test results, and the developer to modify the sample code.

4) The test laboratory verifies the modified sample and begins the formal test.

5) The test lab assists the developer in completing the preparation and submission of the ZigBee Alliance online certification application.

6) The test lab submits a formal test report to the ZigBee Alliance. The alliance will complete the review and issue the certificate.

At present, there are two test laboratories that can complete standard ZigBee testing in China.

1) CESI Beijing China Institute of Standardization Electronics.

2) Element Shenzhen Office (headquartered in the UK)

For details, please refer to the wiki address below.

http://processors.wiki.ti.com/index.php/ZigBee_Product_Certification_Guide

How is the 64-bit MAC address of the device selected?

It is divided into two IEEE addresses in CC2530/CC2538/CC2630, one is called Primary IEEE address, and the other is called Secondary address. The Primary IEEE address is stored in the Information Page of the chip. This address is purchased by TI from the IEEE Association. The address of each chip is unique, which value is for read only, there is no way to erase/modify. Osal_memcpy(aExtendedAddress, (uint8 *)(P_INFOPAGE+HAL_INFOP_IEEE_OSET), Z_EXTADDR_LEN) can be obtained by directly reading the address in the protocol stack. The Secondary address is stored in the last page of Flash in CC2530. The user can perform Read/Write. The function HalFlashRead(HAL_FLASH_IEEE_PAGE, HAL_FLASH_IEEE_OSET, aExtendedAddress, Z_EXTADDR_LEN);

The operation of the protocol stack is how to select the Primary IEEE address or the Secondary address as the MAC address of the device, specifically in the function zmain_ext_addr(void).

1) Read the IEEE address from the NV. If it already exists (not 0xFF), use this address as the MAC address.

2) If nothing is found in 1), read from the Secondary IEEE address storage location. If there is (not 0xFF), write the address to NV, and use this address as the MAC address later.

3) If nothing is found in 2), read from the primary IEEE address storage location. If there is (not 0xFF), write the

address to NV, and use this address as the MAC address later.
4) If nothing is found in 3), a 64-bit variable is randomly generated and written to the NV as the MAC address.

How can I prevent a node from continuously searching the network or increase the interval between sending Beacon Requests?

End Device is a low-power device, battery supplied. After the node is disconnected, how can the node be prevented from continuously searching the network or increase the interval between sending Beacon Requests?

1)Start to search network uint8 ZDApp_StartJoiningCycle(void)
Stop to search network uint8 ZDApp_StopJoiningCycle(void)
2) Change interval of sending Beacon Request
Modify variant zgDefaultStartingScanDuration

```
// Beacon Order Values
#define BEACON_ORDER_NO_BEACONS        15
#define BEACON_ORDER_4_MINUTES         14   // 245760 milliseconds
#define BEACON_ORDER_2_MINUTES         13   // 122880 milliseconds
#define BEACON_ORDER_1_MINUTE          12   //  61440 milliseconds
#define BEACON_ORDER_31_SECONDS        11   //  30720 milliseconds
#define BEACON_ORDER_15_SECONDS        10   //  15360 MSecs
#define BEACON_ORDER_7_5_SECONDS        9   //   7680 MSecs
#define BEACON_ORDER_4_SECONDS          8   //   3840 MSecs
#define BEACON_ORDER_2_SECONDS          7   //   1920 MSecs
#define BEACON_ORDER_1_SECOND           6   //    960 MSecs
#define BEACON_ORDER_480_MSEC           5
#define BEACON_ORDER_240_MSEC           4
#define BEACON_ORDER_120_MSEC           3
#define BEACON_ORDER_60_MSEC            2
#define BEACON_ORDER_30_MSEC            1
#define BEACON_ORDER_15_MSEC            0
```

How to make the End Device enter the low power state, how is the sleep time set?

After enabling POWER_SAVING in the protocol stack macro definition, and then make -DRFD_RCVC_ALWAYS_ON=FALSE in the f8wConfig.cfg file, the End Device can be put to sleep.
The time to sleep is determined by the scheduling of the OSAL operating system. Each sleep time is based on an event timeout that occurs most recently as the sleep time. Specifically, it is described in the protocol stack hal_sleep function.
This timeout is mainly divided into two categories, one is the timeout of the application layer event, and the other is the timeout of the MAC layer event.
1) The timeout time of the application layer is obtained by osal_next_timeout() in the osal_pwrmgr_powerconserve(void) function.
2) The timeout time of the MAC layer is obtained by MAC_PwrNextTimeout(); in the halSleep(uint16 osal_timeout) function.

What's new in the ZigBee 3.0 protocol stack?

Please refer to the link below for an introduction to the ZigBee 3.0 stack compared to the previous ZigBee Home Automation/ZigBee Light Link.

http://processors.wiki.ti.com/index.php/What%27s_New_in_ZigBee_3.0

State machine switching on terminal devices in the TI ZigBee protocol stack

http://www.deyisupport.com/question_answer/wireless_connectivity/zigbee/f/104/t/104629.aspx

About the difference between OAD and OTA in the TI protocol stack

OAD is short for Over the Air Download, OTA is short for Over the Air. These two implementations have the same function, which is an aerial upgrade of the program. In the early ZigBee protocol standard, there was no standard for node program air upgrades, but many customers had requirements for air upgrades, so TI developed a protocol stack for program air upgrades and named it OAD. Later, the ZigBee Alliance saw more and more demand for air upgrades. It also specified the standard for air upgrades. It was named OTA. The standard also referred to TI's OAD implementation and made related changes. Therefore, in TI's early protocol stack, the air upgrade was called OAD, and the subsequent protocol stack followed the ZigBee Alliance's air upgrade protocol, called OTA.

If you develop a private application based on the ZigBee Mesh network, which protocol stack should you choose?

Many users only want to use the functions of the zigbee mesh network in their own systems or products. They do not need to be completely in accordance with the application layer specifications defined by zigbee, especially some industry applications. For such application needs, how should I choose TI's appropriate protocol stack for product development?

http://www.deyisupport.com/question_answer/wireless_connectivity/zigbee/f/104/t/132197.aspx

6 Basic operation

6.1 Hardware design

- It is recommended to use a DC stabilized power supply. The power supply ripple factor is as small as possible, and the module needs to be reliably grounded.;
- Please pay attention to the correct connection of the positive and negative poles of the power supply. Reverse connection may cause permanent damage to the module;
- Please check the power supply to ensure it is within the recommended voltage otherwise when it exceeds the maximum value the module will be permanently damaged;
- Please check the stability of the power supply, the voltage can not be fluctuated frequently;
- When designing the power supply circuit for the module, it is often recommended to reserve more than 30% of the margin, so the whole machine is beneficial for long-term stable operation.;
- The module should be as far away as possible from the power supply, transformers, high-frequency wiring and other parts with large electromagnetic interference.;
- High-frequency digital routing, high-frequency analog routing, and power routing must be avoided under the module. If it is necessary to pass through the module, assume that the module is soldered to the Top

Layer, and the copper is spread on the Top Layer of the module contact part(well grounded), it must be close to the digital part of the module and routed in the Bottom Layer;

- Assuming the module is soldered or placed over the Top Layer, it is wrong to randomly route over the Bottom Layer or other layers, which will affect the module's spurs and receiving sensitivity to varying degrees;
- It is assumed that there are devices with large electromagnetic interference around the module that will greatly affect the performance. It is recommended to keep them away from the module according to the strength of the interference. If necessary, appropriate isolation and shielding can be done;
- Assume that there are traces with large electromagnetic interference (high-frequency digital, high-frequency analog, power traces) around the module that will greatly affect the performance of the module. It is recommended to stay away from the module according to the strength of the interference.If necessary, appropriate isolation and shielding can be done.
- If the communication line uses a 5V level, a 1k-5.1k resistor must be connected in series (not recommended, there is still a risk of damage);
- Try to stay away from some physical layers such as TTL protocol at 2.4GHz , for example: USB3.0;
- The mounting structure of antenna has a great influence on the performance of the module. It is necessary to ensure that the antenna is exposed, preferably vertically upward. When the module is mounted inside the case, use a good antenna extension cable to extend the antenna to the outside;
- The antenna must not be installed inside the metal case, which will cause the transmission distance to be greatly weakened.

6.2 Software editing

- The core of this module is CC2531, and its driving method is completely equivalent to CC2531. Users can operate according to the CC2531 chip manual (see CC2531 manual for details);
- It is recommended to use the Code Composer Studio (CCS) Integrated Development Environment (IDE) for wireless connectivity.
- Code Composer Studio is an integrated development environment (IDE) that supports TI's microcontrollers and embedded processors. Code Composer Studio consists of a complete set of tools for developing and debugging embedded applications. It includes a C/C++ compiler for optimization, a source code editor, a project build environment, a debugger, a descriptor, etc. The intuitive IDE provides a single user interface to help you with every step of the application development process. Familiar tools and interfaces allow users to get started much faster. Code Composer Studio combines the benefits of the Eclipse software framework with TI's advanced embedded debugging capabilities to provide embedded developers with a compelling, feature-rich development environment.
- Re-initialize the register configuration when the chip is idle for higher stability.

7 FAQ

7.1 Communication range is too short

- The communication distance will be affected when obstacle exists.
- Data lose rate will be affected by temperature, humidity and co-channel interference.
- The ground will absorb and reflect wireless radio wave, so the performance will be poor when testing near ground.
- Seawater has great ability in absorbing wireless radio wave, so performance will be poor when testing near the sea.
- The signal will be affected when the antenna is near metal object or put in a metal case.
- Power register was set incorrectly, air data rate is set too high (the higher the air data rate, the shorter the distance).
- The power supply low voltage under room temperature is lower than recommended value, the lower the voltage, the lower the transmitting power.
- Due to antenna quality or poor matching between antenna and module.

7.2 Module is easy to damage

- Please check the power supply source, ensure it is 2.0V~3.6V, voltage higher than 3.6V will damage the module.
- Please check the stability of power source, the voltage cannot fluctuate too much.
- Please make sure antistatic measure are taken when installing and using, high frequency devices have electrostatic susceptibility.
- Please ensure the humidity is within limited range, some parts are sensitive to humidity.
- Please avoid using modules under too high or too low temperature.

7.3 BER(Bit Error Rate) is high

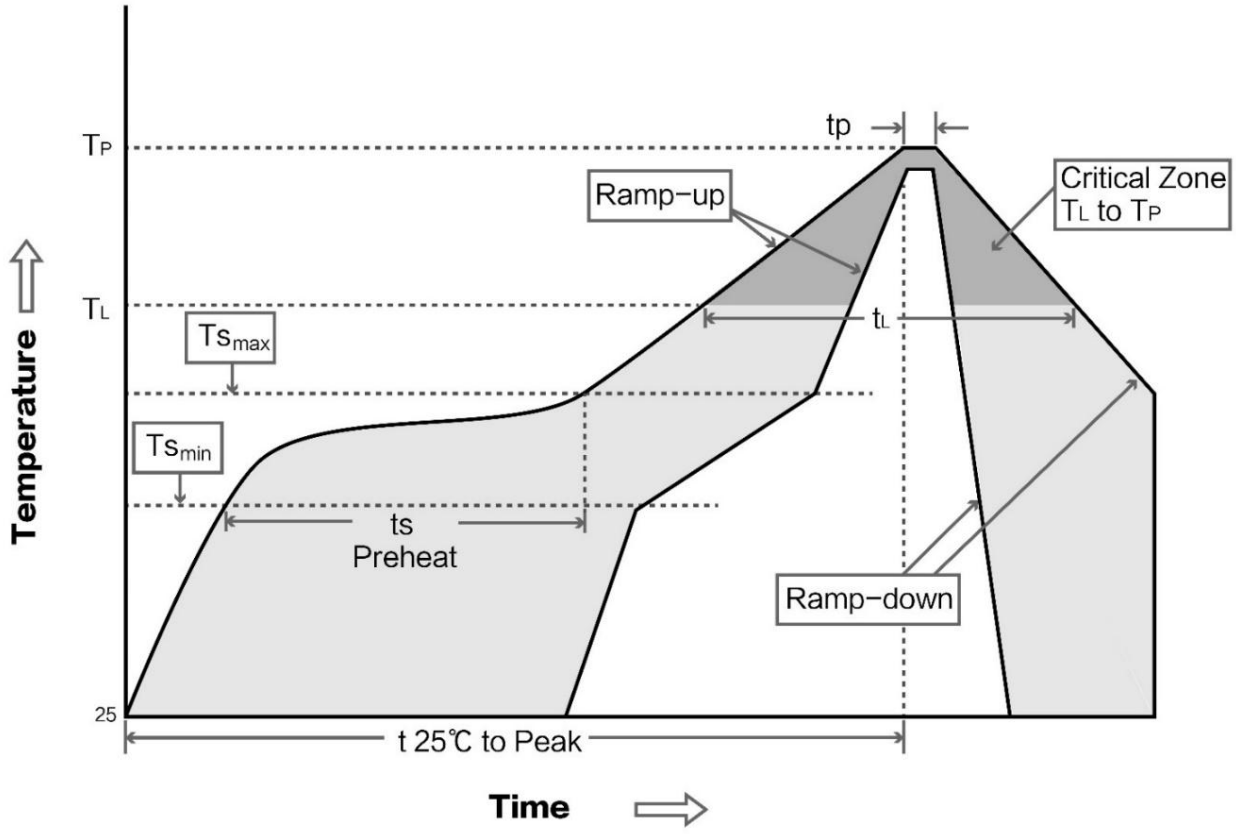
- There are co-channel signal interference nearby, please be away from interference sources or modify frequency and channel to avoid interference;
- Poor power supply may cause messy code. Make sure that the power supply is reliable.
- The extension line and feeder quality are poor or too long, so the bit error rate is high;

8 Production guidance

8.1 Reflow soldering temperature

Profile Feature	Curve characteristics	Sn-Pb Assembly	Pb-Free Assembly
Solder Paste	Solder paste	Sn63/Pb37	Sn96.5/Ag3/Cu0.5
Preheat Temperature min （Tsmin）	Min preheating temp.	100℃	150℃
Preheat temperature max (Tsmax)	Mx preheating temp.	150℃	200℃
Preheat Time (Tsmin to Tsmax)(ts)	Preheating time	60-120 sec	60-120 sec
Average ramp-up rate(Tsmax to Tp)	Average ramp-up rate	3℃/second max	3℃/second max
Liquidous Temperature (TL)	Liquid phase temp.	183℃	217℃
Time（tL）Maintained Above（TL）	Time below liquid phase line	60-90 sec	30-90 sec
Peak temperature（Tp）	Peak temp.	220-235℃	230-250℃
Aveage ramp-down rate（Tp to Tsmax）	Aveage ramp-down rate	6℃/second max	6℃/second max
Time 25℃ to peak temperature	Time to peak temperature for 25℃	max 6 minutes	max 8 minutes

8.2 Reflow soldering curve



9 E18 series

Model No.	IC	Frequency Hz	TX power dBm	Distance km	Interface	Package	Size mm
E18-MS1PA1-IPX	CC2530	2.4G	20	1	IPX	SMD	16 * 22.5
E18-MS1PA1-PCB	CC2530	2.4G	20	0.8	PCB	SMD	16 * 27
E18-MS1-IPX	CC2530	2.4G	4	0.24	IPX	SMD	14.1 * 20.8
E18-MS1-PCB	CC2530	2.4G	4	0.2	PCB	SMD	14.1 * 23

Revision history

Version	Date	Description	Issued by
1.0	2019-01-10	Initial version	huaa
1.1	2023-1-7	Error correction	Bin

About us

Technical support: support@cdebyte.com

Documents and RF Setting download link: https://www.cdebyte.com

Thank you for using Ebyte products! Please contact us with any questions or suggestions: info@cdebyte.com

---

Fax:028-61543675 ext. 821

Web: https://www.cdebyte.com

Address: Innovation Center B333-D347, 4# XI-XIN Road,Chengdu, Sichuan, China

成都亿佰特电子科技有限公司
Chengdu Ebyte Electronic Technology Co.,Ltd.