

IR Version Reader Control Protocol User Manual

Version Control

Date	Version	Content
2019-04-28	V1.0	Initial version
2019-11-16	V1.1	Update some commands

Table of Contents

Table of Contents.....	1
1. Introduction.....	2
2. Data's type and the basic format of protocols.....	3
2.1. Data's Type.....	3
2.2. Basic format of protocol.....	3
2.3. Data Format.....	4
3. Code Table.....	5
4. Communication Protocol.....	7
4.1. Read Type C Ull.....	8
4.2. Read Type C Tag Data.....	9
4.3. Write Type C Tag Data.....	10
4.4. Lock Type C Tag.....	10
4.5. Kill Type C Tag.....	12
4.6. Encrypted Type C Tag *.....	13
4.7. Get Access EPC match status.....	14
4.8. Set Access EPC match status.....	14
4.9. Get Tx Power Level.....	15
4.10. Set Tx Power Level.....	16
4.11. Get Region.....	16
4.12. Set Region.....	17
4.13. Get Modulation.....	18
4.14. Set Modulation.....	19
4.15. Get Base Parameters.....	19
4.16. Set Base Parameters.....	21
4.17. Get Antenna configuration.....	23
4.18. Set Antenna configuration.....	23
4.19. Get Encryption method for Tag *.....	24
4.20. Set Encryption method for Tag *.....	25
4.21. Get Protocol Address.....	26
4.22. Set Protocol Address.....	26
4.23. Get UART Baudrate *.....	27
4.24. Set UART Baudrate *.....	27
4.25. Get Output Mode *.....	27
4.26. Set Output Mode *.....	28
4.27. Reset System.....	29
4.28. Restore Factory Settings.....	30
4.29. Get GPIO Mode *.....	30
4.30. Set GPIO Mode *.....	30

1. Introduction

Communications protocol definition

Support RS232/ RS485;

The mode of information transmission is asynchronous , data bits: 8 , stop bits: 1 , no checksum.

Rate of data transmission: 57.6kb/s;

The monitoring unit (SU) and device control module (SM) communication mainly from the way, the monitoring unit for the host computer, slave computer monitoring module. SU call SM and issue the command, SM receives the command returns response information. SU 500ms is not receiving a SM response or receiving response information error, think of the communication process to fail.

Supervision Unit (SU): like PC or control device;

Supervisory Module (SM): Reader;

Note: Communication data is HEX; Denotation Method xxH;

2. Data's type and the basic format of protocols

2.1. Data's Type

Two types:

- Command: SU to SM;
- Response: SM to SU;

2.2. Basic format of protocol

Table 2-1 basic format of protocols

No.	1	2	3	4	5	6	7
byte	1	2	1	1	1	LENGTH	1
format	SOI	ADR	CID1	CID2	LENGTH	INFO	CHKSUM

Table 2-2 basic format of notes

No.	Symbol	significance	Remarks
1	SOI	START OF INFORMATION	Command(7CH) Response(CCH)
2	ADR	Equip address (1 ~ 65534) ,(65535 public address,0 reserve address)	FFFFH
3	CID1	Control identification code (data type description)	
4	CID2	Command: control identification code (action type description) Response: RTN (Return code Table 2-3)	
5	LENGTH	INFO Data Length	
6	INFO	Command: Command information Response: Response data information	
7	CHKSUM	The checksum code	

Table 2-3 Return code RTN

No.	RTN Value(HEX)	significance	Remarks
1	00H	Succeed	
2	01H	Fail	
	02H	Response message for Command	
3	05H	Auto send to SU	

2.3. Data Format

CHKSUM data format:

- **CHKSUM Introduction**

The calculation of CHKSUM is in addition to CHKSUM, other characters in 16 hex code values of cumulative sum, the result modulo 256 remainder taking anti - plus 1.

For example: Receive or send data is: "CC 02 01 B1 22 04 BB 12 02 03 88". The last byte "88" is CHKSUM.

Calculate as follows:

$$\begin{aligned} & 'CC' + '02' + '01' + \dots + '22' + '04' + 'BB' + '12' + '02' + '03' \\ & = CCH + 02H + 01H + \dots + 22H + 04H + BBH + 12H + 02H + 03H \\ & = 0278H \end{aligned}$$

0278H mode 256 and the remainder is 78H, 78H anti plus 1 is 88H.

- **CHKSUM Calculate refers:**

unsigned char Checksum (unsigned char *uBuff, unsigned char uBuffLen)

```
{
    unsigned char i, uSum =0;
    for(i=0; i<uBuffLen; i++)
    {
        uSum = uSum + uBuff[i];
    }
    uSum = (~uSum) + 1;
    return uSum;
}
```

3. Code Table

CID1、CID2 Code Distribution and Classification as follows :

Table 3-1 Command code Classification (SENIOR CID1)

No.	Content	CID1	Remark
1	Read Type C Ull	20H	
2	Read Type C Tag Data	21H	
3	Write Type C Tag Data	22H	
4	Lock Type C Tag	26H	
5	Kill/Recom Type C Tag	28H	
6	Encrypted Type C Tag *	2AH	
7	Get Access EPC MATCH	2CH	
8	Set Access EPC MATCH	2DH	
9	Get Tx Power Level	50H	
10	Set Tx Power Level	51H	
11	Get Region	52H	
12	Set Region	53H	
13	Get Modulation	58H	
14	Set Modulation	59H	
15	Base Parameter	81H	
16	Antenna configuration	83H	
17	Encryption method for Tag *	84H	
18	Protocol Address	85H	
19	UART Baud rate *	86H	
20	Output Mode *	87H	
21	Reset System	D0H	
22	Restore Factory Settings	D3H	
23	Get GPIO Mode *	D6H	
24	Set GPIO Mode *	D7H	
25			
26			
27			
28			
29			
30			
31			
32			

--	--	--	--

Table 3-2 Command action Classification (CID2)

No.	Content	CID2	Remarks
1	Senior command	00H	
2	Set command	31H	
3	Get command	32H	

4. Communication Protocol

For the use of this protocol in the protocol code as follows.

Table 4-1 protocol code

No.	Content	CID1	CID2	Remarks
1	Read Type C Ull	20H	00H	
2	Read Type C Tag Data	21H	00H	
3	Write Type C Tag Data	22H	00H	
4	Lock Type C Tag	26H	00H	
5	Kill/Recom Type C Tag	28H	00H	
6	Encrypted Type C Tag *	2AH	00H	
7	Get Access EPC MATCH	2CH	00H	
8	Set Access EPC MATCH	2DH	00H	
9	Get Tx Power Level	50H	00H	
10	Set Tx Power Level	51H	00H	
11	Get Region	52H	00H	
12	Set Region	53H	00H	
13	Get Modulation	58H	00H	
14	Set Modulation	59H	00H	
15	Get Base Parameters	81H	32H	
16	Set Base Parameters	81H	31H	
17	Get Antenna configuration	83H	32H	
18	Set Antenna configuration	83H	31H	
19	Get Encryption method for Tag *	84H	32H	
20	Set Encryption method for Tag *	84H	31H	
21	Get Protocol Address	85H	32H	
22	Set Protocol Address	85H	31H	
23	Get Output Mode *	87H	32H	
24	Set Output Mode *	87H	31H	
25	Reset System	D0H	00H	
26	Restore Factory Settings	D3H	00H	
27	Get GPIO Mode *	D6H	00H	
28	Set GPIO Mode *	D7H	00H	
29				
30				
31				
32				
33				
34				
35				
36				

37				

Note: with * command representation is optional command; the reader does not have this feature, if have this feature, should be in accordance with the execution of this agreement. (Hereinafter appearing * place, meaning as described above, not detailed below.)

4.1. Read Type C Ull

When the working mode is set to active, this command does not need to be sent, and the reader will automatically read and response, RTN is 05H;

4.1.1. Command

CID1: 20H

CID2: 00H

INFO: - None.

Example:

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	CHECKSUM
7C	FF	FF	20	00	00	0xNN

4.1.2. Tag Response(When there are multiple tags, the answer returns multiple)

CID1: 20H

RTN: 02H

INFO: - ANT (8-bit): Ant No.(Def 0x00)

- EPC (variable): Target tag's PC+EPCS

- RSSI (8-bit): RSSI

Example: ANT=0x00, PC = 0x3000, EPC = 0xE2003411B802011383258566, RSSI=0xC9

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	ANT
CC	FF	FF	20	02	10	00
PC (MSB)	PC (LSB)	EPC (MSB)	--	--	--	--
30	00	E2	00	34	11	B8
--	--	--	--	--	--	EPC (LSB)
02	01	13	83	25	85	66
RSSI	CHECKSUM					
C9	0xNN					

4.1.3. Response

CID1: 20H

RTN: 00H

INFO: - ANT (8-bit): Ant No.(Def 0x00)

- STC (8-bit): Send Tag Count

- RTC (8-bit): Read Tag Count

Example: ANT=0x00, STC = 0x27, RTC=0x27

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	ANT
CC	FF	FF	20	02	03	00

STC	RCT	CHECKSUM				
27	27	0xNN				

4.2. Read Type C Tag Data

This command should be preceded by a match EPC status command (see 4.8)

4.2.1. Command

CID1: 21H

CID2: 00H

INFO: - AP (32-bit): Access Password if target memory bank was password protected. Otherwise, set AP filed to 0x00000000.

- MB (8-bit): Target memory bank; RFU (0x00), EPC (0x01), TID (0x02), User (0x03)

- SA (8-bit): Starting Address word pointer (Word)

- DL (8-bit): Data Length (Word Count).

Example: **Access Password = 0x00000000,**

Target memory bank = EPC,

Start Address = 0x02,

Length = 2 word

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	AP(MSB)
7C	FF	FF	21	00	07	00
--	--	AP(LSB)	MB	SA	DL	CHECKSUM
00	00	00	01	02	02	0xNN

4.2.2. Response

CID1: 21H

RTN: 00H

INFO: - ANT (8-bit): Ant No.(Def 0x00)

- EPC (variable): Target tag's PC+EPC

- DT(variable): Tag memory contents

Example 如: **ANT=0x00,**

PC = 0x3000,

EPC = 0xE2003411B802011383258566,

DT=0x E2003411

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	ANT
CC	FF	FF	21	00	13	00
PC (MSB)	PC (LSB)	EPC (MSB)	--	--	--	--
30	00	E2	00	34	11	B8
--	--	--	--	--	--	EPC (LSB)
02	01	13	83	25	85	66
DT (MSB)	--	--	DT (LSB)	CHECKSUM		
E2	00	34	11	0xNN		

4.3. Write Type C Tag Data

This command should be preceded by a match EPC status command (see 4.8).

4.3.1. Command

CID1: 22H

CID2: 00H

INFO: - AP (32-bit): Access Password if target memory bank was password protected. Otherwise, set AP filed to 0x00000000.

- MB (8-bit): Target memory bank; RFU (0x00), EPC (0x01), TID (0x02), User (0x03)

- SA (8-bit): Starting Address word pointer (Word)

- DL (8-bit): Data Length (Word Count).

- DT (variable): Data to write.

Example: Access Password = 0x00000000,

Target memory bank = EPC,

Start Address = 0x02,

Data Length = 2 word,

Data to write = 0x12345678

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	AP(MSB)
7C	FF	FF	22	00	0B	00
--	--	AP(LSB)	MB	SA	DL	DT(MSB)
00	00	00	01	02	02	12
--	--	DT(LSB)	CHECKSUM			
34	56	78	0xNN			

4.3.2. Response

CID1: 22H

RTN: 00H

INFO: - ANT (8-bit): Ant No.(Def 0x00)

- EPC (variable): Target tag's PC+EPC

Example: ANT=0x00,

PC = 0x3000,

EPC = 0xE2003411B802011383258566

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	ANT
CC	FF	FF	22	00	0F	00
PC (MSB)	PC (LSB)	EPC (MSB)	--	--	--	--
30	00	E2	00	34	11	B8
--	--	--	--	--	--	EPC (LSB)
02	01	13	83	25	85	66
CHECKSUM						
0xNN						

4.4. Lock Type C Tag

This command should be preceded by a match EPC status command (see 4.8).

4.4.1. Command

CID1: 26H

CID2: 00H

INFO: - AP (32-bit): Access Password if target memory bank was password protected. Otherwise, set AP filed to 0x00000000.

- LD (24-bit): Lock Data.

The high 4 bits of lock operation parameter LD are reserved bits, and the remaining 20 bits are lock operation payload, including mask and action, 10 bits from high to low. For details, please refer to section 6.3.2.11.3.5 of EPC Gen2 protocol version 1.2.0.

Mask is a mask. Only actions with mask bit 1 are valid. Actions in each data area have 2 bits, 00-11, which correspond to opening, permanent opening, locking and permanent locking.

For example, if the kill mask is 2bits 00, the kill action will not take effect regardless of the kill action. When the kill mask is 2bits 10 and the kill action is 2bits 10, it means that the kill password is locked (not perma lock). Only through a valid access password can it be read and written.

The meaning of each bit of mask and action is shown in the table below.

Lock-Command Payload

19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Kill Mask		Access Mask		EPC Mask		TID Mask		User Mask		Kill Action		Access Action		EPC Action		TID Action		User Action	

Masks and Associated Action Fields

	Kill pwd		Access pwd		EPC memory		TID memory		User memory	
	19	18	17	16	15	14	13	12	11	10
Mask	skip/write	skip/write	skip/write	skip/write	skip/write	skip/write	skip/write	skip/write	skip/write	skip/write
Action	9	8	7	6	5	4	3	2	1	0
	pwd read/write	perma lock	pwd read/write	perma lock	pwd write	perma lock	pwd write	perma lock	pwd write	perma lock

pwd-write	permalock	Description
0	0	Associated memory bank is writeable from either the open or secured states.
0	1	Associated memory bank is permanently writeable from either the open or secured states and may never be locked.
1	0	Associated memory bank is writeable from the secured state but not from the open state.
1	1	Associated memory bank is not writeable from any state.
pwd-read/write	permalock	Description
0	0	Associated password location is readable and writeable from either the open or secured states.
0	1	Associated password location is permanently readable and writeable from either the open or secured states and may never be locked.
1	0	Associated password location is readable and writeable from the secured state but not from the open state.
1	1	Associated password location is not readable or writeable from any state.

Example: If you need lock Access Password, then:

Access Password = 0x0000FFFF,

LD = 0x020080

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	AP(MSB)
7C	FF	FF	26	00	07	00
--	--	AP(LSB)	LD(MSB)	--	LD(LSB)	CHECKSUM
00	FF	FF	02	00	80	0xNN

4.4.2. Response

CID1: 26H

RTN: 00H

INFO: - ANT (8-bit): Ant No.(Def 0x00)
 - EPC (variable): Target tag's PC+EPC
 - DT(variable): Tag memory contents

Example: **ANT=0x00,**

PC = 0x3000,

EPC = 0xE2003411B802011383258566

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	ANT
CC	FF	FF	26	00	0F	00
PC (MSB)	PC (LSB)	EPC (MSB)	--	--	--	--
30	00	E2	00	34	11	B8
--	--	--	--	--	--	EPC (LSB)
02	01	13	83	25	85	66
CHECKSUM						
0xNN						

4.5. Kill Type C Tag

This command should be preceded by a match EPC status command (see 4.8).

4.5.1. Command

CID1: 28H

CID2: 00H

INFO: - KP (32-bit): Kill Password. If KP filed set to 0x00000000, 'Kill Type C Tag' command do not work. The target tag ignores it.
 - Recom (8-bit): Recommissioning bits.

Example: **Kill Password =0x87654321, Recom = 0x00**

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	KP(MSB)
7C	FF	FF	28	00	05	87
--	--	KP(LSB)	Recom	CHECKSUM		
65	43	21	00	0xNN		

4.5.2. Response

CID1: 28H

RTN: 00H

INFO: - ANT (8-bit): Ant No.(Def 0x00)
 - EPC (variable): Target tag's PC+EPC

Example: **ANT=0x00,**

PC = 0x3000,

EPC = 0xE2003411B802011383258566

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	ANT
CC	FF	FF	28	00	0F	00
PC (MSB)	PC (LSB)	EPC (MSB)	--	--	--	--
30	00	E2	00	34	11	B8
--	--	--	--	--	--	EPC (LSB)
02	01	13	83	25	85	66
CHECKSUM						
0xNN						

4.6. Encrypted Type C Tag *

(Limited encryption mode, only valid for the company's production equipment)

Before this instruction, set the label encryption method of the device (see 4.20). Otherwise, the encryption command is invalid.

4.6.1. Command

CID1: 2AH

CID2: 00H

INFO: - AP (32-bit): Access Password if target memory bank was password protected. Otherwise, set AP filed to 0x00000000.

Example: Access Password = 0x00000000

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	AP(MSB)
7C	FF	FF	28	00	04	00
--	--	AP(LSB)	CHECKSUM			
00	00	00	0xNN			

4.6.2. Response

CID1: 2AH

RTN: 00H

INFO: - ANT (8-bit): Ant No.(Def 0x00)

- EPC (variable): Target tag's PC+EPC

Example: ANT=0x00,

PC = 0x3000,

EPC = 0xE2003411B802011383258566

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	ANT
CC	FF	FF	2A	00	0F	00
PC (MSB)	PC (LSB)	EPC (MSB)	--	--	--	--
30	00	E2	00	34	11	B8
--	--	--	--	--	--	EPC (LSB)
02	01	13	83	25	85	66
CHECKSUM						
0xNN						

4.7. Get Access EPC match status

4.7.1. Command

CID1: 2CH

CID2: 00H

INFO: -None

Example:

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	CHECKSUM
7C	FF	FF	2C	00	00	0xNN

4.7.2. Response

CID1: 2CH

RTN: 00H

INFO: - MODE (8-bit): Match Mode
 0x00,select tag action,(write,read,lock,kill)
 0x01,Mismatch
 - LEN (8-bit): Mach EPC length,(if len ==0,not return)
 - EPC (variable): Target tag's EPC data ,(if len ==0,not return)

Example1: **MODE=0x01,**

LEN=null,

EPC = null,

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	MODE
CC	FF	FF	2C	00	01	01
CHECKSUM						
0xNN						

Example2: **MODE=0x00,**

LEN=0x0C,

EPC = 0xE2003411B802011383258566,

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	MODE
CC	FF	FF	2C	00	0E	00
LEN	EPC (MSB)	--	--	--	--	--
0C	E2	00	34	11	B8	02
--	--	--	--	--	EPC (LSB)	CHECKSUM
01	13	83	25	85	66	0xNN

4.8. Set Access EPC match status

4.8.1. Command

CID1: 2DH

CID2: 00H

INFO: - MODE (8-bit): Match Mode
 0x00,select tag action,(write,read,lock,kill)
 0x01,Mismatch
 - LEN (8-bit): Match EPC length,(if len ==0,not return)
 - EPC (variable): Target tag's EPC data ,(if len ==0,not return)

Example1: cancel match

MODE=0x01,
LEN=null,
EPC = null,

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	MODE
7C	FF	FF	2D	00	01	01
CHECKSUM						
0xNN						

Example2: Select tag action

MODE=0x00,
LEN=0x0C,
EPC = 0xE2003411B802011383258566,

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	MODE
7C	FF	FF	2D	00	0E	00
LEN	EPC (MSB)	--	--	--	--	--
0C	E2	00	34	11	B8	02
--	--	--	--	--	EPC (LSB)	CHECKSUM
01	13	83	25	85	66	0xNN

4.8.2. Response

CID1: 2DH
 RTN: 00H
 INFO: - None

Example :

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	CHECKSUM
CC	FF	FF	2D	00	00	0xNN

4.9. Get Tx Power Level

4.9.1. Command

CID1: 50H
 CID2: 00H
 INFO: - None

Example :

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	CHECKSUM
7C	FF	FF	50	00	00	0xNN

4.9.2. Response

CID1: 50H

RTN: 00H

INFO: - PWR (8-bit): Tx Power Level,area -- 0~33(0x00-0x21)dBm.

Example : **PWR=0x1A,**

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	PWR
CC	FF	FF	50	00	01	1A
CHECKSUM						
0xNN						

4.10. Set Tx Power Level**4.10.1. Command**

CID1: 51H

CID2: 00H

INFO: - PWR (8-bit): Tx Power Level,area -- 0~33(0x00-0x21)dBm.

Example : **PWR=0x1A,**

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	PWR
7C	FF	FF	51	00	01	1A
CHECKSUM						
0xNN						

4.10.2. Response

CID1: 51H

RTN: 00H

INFO: - None

Example :

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	CHECKSUM
CC	FF	FF	51	00	00	0xNN

4.11. Get Region**4.11.1. Command**

CID1: 52H

CID2: 00H

INFO: - None

Example :

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	CHECKSUM
7C	FF	FF	52	00	00	0xNN

4.11.2. Response

CID1: 52H
 RTN: 00H
 INFO: - Region (8-bit): RF Region
 0x01 : US (902.000~ 928.000MHz),
 0x02 : Europe (865.000~ 868.000MHz),
 0x03 : China (920.000~ 925.000MHz),
 0x04 : Custom,
 - FS(8-bit):
 Region value is not 0x04,than it is start freq,unit is 0.50MHz, Europe Area (0~6),US Area (0~52),China Area(0~10);
 Region value is 0x04,then it is frequency spacing (1~255),unit is10KHz
 - FE(8-bit):
 Region value is not 0x04,than it is stop freq,unit is 0.50MHz,Europe Area (0~6),US Area (0~52),China Area(0~10);
 Region value is 0x04,than it is Frequency point quantity(1~255),Include the number of frequency points of the starting frequency, 1 is to set the frequency at the starting frequency. This parameter must be greater than 0.
 - CFS(24-bit):
 Region value is not 0x04,than it is not valid,fill 0xFFFFFFFF;
 Region value is 0x04,than it is start freq, unit is KHz,
 For example, 92000khz returns 0x0E09C0

Example : Hopping freq ,Europe 866.50MHz~867.50MHz

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	Region
CC	FF	FF	52	00	06	02
FS	FE	CSF(MSB)		CSF(LSB)	CHECKSUM	
03	05	FF	FF	FF	0xNN	

4.12. Set Region

4.12.1. Command

CID1: 53H
 CID2: 00H
 INFO: - Region (8-bit): RF Region
 0x01 : US (902.000~ 928.000MHz),
 0x02 : Europe (865.000~ 868.000MHz),
 0x03 : China (920.000~ 925.000MHz),
 0x04 : Custom,
 - FS(8-bit):
 Region value is not 0x04,than it is start freq,unit is 0.50MHz, Europe Area (0~6),US Area (0~52),China Area(0~10);
 Region value is 0x04,then it is frequency spacing (1~255),unit is10KHz
 - FE(8-bit):
 Region value is not 0x04,than it is stop freq,unit is 0.50MHz,Europe Area (0~6),US Area

(0~52),China Area(0~10);

Region value is 0x04,than it is Frequency point quantity(1~255),Include the number of frequency points of the starting frequency, 1 is to set the frequency at the starting frequency. This parameter must be greater than 0.

- CFS(24-bit):

Region value is not 0x04,than it is not valid,fill 0xFFFFFFFF;

Region value is 0x04,than it is start freq, unit is KHz,

For example, 92000khz returns 0x0E09C0

Example : Custom,fix Freq 920MHZ

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	Region
7C	FF	FF	53	00	06	04
FS	FE	CSF(MSB)		CSF(LSB)	CHECKSUM	
32	01	0E	09	C0	0xNN	

4.12.2. Response

CID1: 53H

RTN: 00H

INFO:

- None

Example :

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	CHECKSUM
CC	FF	FF	53	00	00	0xNN

4.13. Get Modulation

4.13.1. Command

CID1: 58H

CID2: 00H

INFO: - None

Example :

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	CHECKSUM
7C	FF	FF	58	00	00	0xNN

4.13.2. Response

CID1: 58H

RTN: 00H

INFO: - MODE(8-bit): Modulation mode,def 0x01

0x00-tari 25us,fm0,40KHz

0x01-tari 25us,miller4,250KHz

0x02-tari 25us,miller4,300KHz

0x03-tari 6.25us,fm0,400KHz

Example : **MODE=0x01**

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	MODE
CC	FF	FF	58	00	01	01
CHECKSUM						
0xNN						

4.14. Set Modulation

4.14.1. Command

CID1: 59H

CID2: 00H

INFO: - MODE(8-bit): Modulation mode, def 0x01

0x00-tari 25us, fm0, 40KHz

0x01-tari 25us, miller4, 250KHz

0x02-tari 25us, miller4, 300KHz

0x03-tari 6.25us, fm0, 400KHz

Example 1: **MODE=0x01,**

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	MODE
7C	FF	FF	59	00	01	01
CHECKSUM						
0xNN						

4.14.2. Response

CID1: 59H

RTN: 00H

INFO: - None

Example :

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	CHECKSUM
CC	FF	FF	59	00	00	0xNN

4.15. Get Base Parameters

4.15.1. Command

CID1: 81H

CID2: 32H

INFO: - None

Example:

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	CHECKSUM
7C	FF	FF	81	32	00	0xNN

4.15.2. Response

CID1: 81H

RTN: 00H

INFO: - OM (8-bit): Output mode, (when the working mode is active, the reader data active output interface)

0x00 - 232(BLE/SPP)

0x01 - 485(USB/HID/WIFI/TCPIP/PDA)

0x02 - WG26

0x03 - WG34

0x04 - WG66

0x05 - WG98 *(not used temporarily)

- WM (8-bit): Working mode,

0x00- Command,

0x01- Active,

0x02- Passive.

- RT (8-bit): Read Type,

0x02-EPC,

0x03-EPC+OTHER DATA. (Valid by active mode)

- RI (8-bit): reading interval, 2~200,unit is 10ms

- RD (8-bit): Read delay,delayed reading after command interaction,0~255,unit is second.

(Valid by active mode)

- WG (32-bit): Including (data offset, output period, pulse width, pulse period). (Valid by WG)

Offset (8-bit): (0~14) Byte, Def (0x02)

Interval (8-bit): (0~255) *10ms, Def (0x1E)

Width (8-bit): (0~255) *10us, Def (0x0A)

Period (8-bit): (0~255) *100us, Def (0x0F)

- SI (16-bit): Same ID output interval,(Valid by active mode)

- BZ (8-bit): buzzer enabled; Disabled (0x00) Enabled (0x01),

- UD (112-bit): Additional data for additional send Tags; (Valid by Read Type = 0x03)

AP (32-bit): Access Password if target memory bank was password protected. Otherwise, set AP filed to 0x00000000;

MB (8-bit): Target tag block selection;

0x00 RFU, 0x01 EPC, 0x02 TID, 0x03 User

SA (8-bit): Target tag data address offset (Word)

DL (8-bit): Target tag data length (Word Count).

CT (8-bit): Target tag data capture method.

0x00- EPC+TID,

0x01- TID,

0x02- TID+EPC,

0x03- EPC+TIDKEY.

EL(8-bit): Target tag EPC value length.

KL(8-bit): Target label KEYS value length.

KS(32-bit): Target label KEYS value.

- REV (8-bit): reserve

Note: the red font in information is an extension function, which is not enabled yet. Fill in 0x00 or the default value.

Example:

OM=0x00, WM=0x01, RT=0x02, RI=0x28, RD=0x0A,
 Offset = 0x02, Interval=0x1E, Width=0x0A, Period=0x0F,
 SI=0x0001, BZ=0x01,
 AP =0x00000000, MB=0x02, SA=0x00, DL=0x06,
 CT =0x00, EL=0x00, KL=0x00,KS =0x00000000,
 REV=0x00,

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	OM
CC	FF	FF	81	00	1B	01
WM	RT	RI	RD	Offset	Interval	Width
01	02	28	0A	02	1E	0A
Period	SI(MSB)	SI(LSB)	BZ	AP(MSB)	--	--
0F	00	01	01	00	00	00
AP(LSB)	MB	SA	DL	CT	EL	KL
00	02	00	06	00	00	00
KS(MSB)	--	--	KS(LSB)	REV	CHECKSUM	
00	00	00	00	00	0xNN	

4.16. Set Base Parameters

4.16.1. Command

CID1: 81H

CID2: 31H

INFO: - OM (8-bit): Output mode, (when the working mode is active, the reader data active output interface)

0x00 - 232(BLE/SPP)

0x01 - 485(USB/HID/WIFI/TCP/IP/PDA)

0x02 - WG26

0x03 - WG34

0x04 - WG66

0x05 - WG98 *(not used temporarily)

- WM (8-bit): Working mode,

0x00- Command,

0x01- Active,

0x02- Passive.

- RT (8-bit): Read Type,

0x02-EPC,

0x03-EPC+OTHER DATA. (Valid by active mode)

- RI (8-bit): reading interval, 2~200,unit is 10ms

- RD (8-bit): Read delay,delayed reading after command interaction,0~255,unit is second.

(Valid by active mode)

- WG (32-bit): Including (data offset, output period, pulse width, pulse period). (Valid by WG)

Offset (8-bit): (0~14) Byte, Def (0x02)

- Interval (8-bit): (0~255) *10ms, Def (0x1E)
 Width (8-bit): (0~255) *10us, Def (0x0A)
 Period (8-bit): (0~255) *100us, Def (0x0F)
 - SI (16-bit): Same ID output interval,(Valid by active mode)
 - BZ (8-bit): buzzer enabled; Disabled (0x00) Enabled (0x01),
 - UD (112-bit): Additional data for additional send Tags; (Valid by Read Type = 0x03)
 AP (32-bit): Access Password if target memory bank was password protected. Otherwise, set AP filed to 0x00000000;
 MB (8-bit): Target tag block selection;
 0x00 RFU, 0x01 EPC, 0x02 TID, 0x03 User
 SA (8-bit): Target tag data address offset (Word)
 DL (8-bit): Target tag data length (Word Count).
 CT (8-bit): Target tag data capture method.
 0x00- EPC+TID,
 0x01- TID,
 0x02- TID+EPC,
 0x03- EPC+TIDKEY.
 EL(8-bit): Target tag EPC value length.
 KL(8-bit): Target label KEYS value length.
 KS(32-bit): Target label KEYS value.

- REV (8-bit): reserve

Note: the red font in information is an extension function, which is not enabled yet. Fill in 0x00 or the default value.

Example:

OM=0x00, WM=0x01, RT=0x04, RI=0x28, RD=0x0A,
 Offset = 0x02, Interval=0x1E, Width=0x0A, Period=0x0F,
 SI=0x0001, BZ=0x01,
 AP =0x00000000, MB=0x02, SA=0x00, DL=0x06,
 CT =0x00, EL=0x00, KL=0x00,KS =0x00000000,
 REV=0x00,

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	OM
7C	FF	FF	81	31	1B	00
WM	RT	RI	RD	Offset	Interval	Width
01	04	28	0A	02	1E	0A
Period	SI(MSB)	SI(LSB)	BZ	AP(MSB)	--	--
0F	00	01	01	00	00	00
AP(LSB)	MB	SA	DL	CT	EL	KL
00	02	00	06	00	00	00
KS(MSB)	--	--	KS(LSB)	REV	CHECKSUM	
00	00	00	00	00	0xNN	

4.16.2. Response

CID1: 5BH
 RTN: 00H
 INFO: - None
 Example:

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	CHECKSUM
CC	FF	FF	5B	00	00	0xNN

4.17. Get Antenna configuration

Antenna configuration - multi antenna reader active.

4.17.1. Command

CID1: 83H
 CID2: 32H
 INFO: -None
 Example :

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	CHECKSUM
7C	FF	FF	83	32	00	0xNN

4.17.2. Response

CID1: 83H
 RTN: 00H
 INFO: - CA (8-bit): current ant (1~16)
 - EA (16-bit): enabled ant , bit set , for example value is 0x0009,Indicates enable antenna 1 and antenna 4;

Example 1: CA=0x01,
 EA=0x0009,

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	CA
CC	FF	FF	83	00	03	01
EA(MSB)	EA(LSB)	CHECKSUM				
00	09	0xNN				

4.18. Set Antenna configuration

Antenna configuration - multi antenna reader active.

4.18.1. Command

CID1: 83H
 CID2: 31H
 INFO: - MA (8-bit):
 -0x00: Set enabled ant,do not save configuration

-0xFF: Set enabled ant,save configuration

-0x01~0x10: change current ant (Ignore EA)

- EA (16-bit): enabled ant , bit set , for example value is 0x0009,Indicates enable antenna 1 and antenna 4;

Example 1: enabled antenna 1,4,do not save configuration

CA=0x01,

EA=0x0009,

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	MA
7C	FF	FF	83	31	03	00
EA(MSB)	EA(LSB)	CHECKSUM				
00	09	0xNN				

Example 2: enabled antenna 1,2,3,4, save configuration

CA=0xff,

EA=0x000f,

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	MA
7C	FF	FF	83	31	03	FF
EA(MSB)	EA(LSB)	CHECKSUM				
00	0F	0xNN				

Example 3: Change ant to 1

CA=0x01,

EA=null,

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	MA
7C	FF	FF	83	31	01	01
CHECKSUM						
0xNN						

4.18.2. Response

CID1: 83H

RTN: 00H

INFO: - None

Example :

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	CHECKSUM
CC	FE	FF	83	00	00	0xNN

4.19. Get Encryption method for Tag *

Get tag encryption, pairing encryption or CRC verification encryption.

4.19.1. Command

CID1: 84H

CID2: 32H

INFO: - None

Example:

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	CHECKSUM
7C	FF	FF	84	32	00	0xNN

4.19.2. Response

CID1: 84H

RTN: 00H

INFO: - TYPE(8-bit): 0x00-No encryption,0x01-pairing,0x02-CRC
 - PM (8-bit): Password high byte,(Pairing encryption is only valid for PM);
 - PL (8-bit): Password low byte,(CRC encryption mode PM + PL is effective);

Example: TYPE=0x01, PM=0x01, PL=0x00,

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	TYPE
CC	FE	FF	84	00	03	01
PM	PL	CHECKSUM				
01	00	0xNN				

4.20. Set Encryption method for Tag *

Set tag encryption, pairing encryption or CRC verification encryption.

After set the tag encryption mode, the tags needs to be encrypted (see 4.6), otherwise the card will not be actively identified.

4.20.1. Command

CID1: 84H

CID2: 31H

INFO: - TYPE(8-bit): 0x00-No encryption,0x01-pairing,0x02-CRC
 - PM (8-bit): Password high byte,(Pairing encryption is only valid for PM);
 - PL (8-bit): Password low byte,(CRC encryption mode PM + PL is effective);

Example: TYPE=0x01, PM=0x01, PL=0x00,

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	TYPE
7C	FF	FF	84	31	03	01
PM	PL	CHECKSUM				
01	00	0xNN				

4.20.2. Response

CID1: 84H

RTN: 00H

INFO: - None

Example:

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	CHECKSUM
CC	FE	FF	84	00	00	0xNN

4.21. Get Protocol Address

Get Current communication address. (when there are multiple readers, this address can be used to distinguish Readers)

4.21.1. Command

CID1: 85H

CID2: 32H

INFO: - None

Example:

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	CHECKSUM
7C	FF	FF	85	32	00	0xNN

4.21.2. Response

CID1: 85H

RTN: 00H

INFO: - ADDR(16-bit): protocol address

Example: ADDR=0xFFFE,

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	ADDR(MSB)
CC	FE	FF	85	00	02	FF
ADDR(LSB)	CHECKSUM					
FE	0xNN					

4.22. Set Protocol Address

4.22.1. Command

CID1: 85H

CID2: 31H

INFO: - ADDR(16-bit): protocol address

Example: ADDR=0xFFFE,

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	ADDR(MSB)
7C	FF	FF	85	31	02	FF
ADDR(LSB)	CHECKSUM					
FE	0xNN					

4.22.2. Response

CID1: 85H

RTN: 00H

INFO: - None

Example:

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	CHECKSUM
CC	FE	FF	85	00	00	0xNN

4.23. Get UART Baudrate *

Get UART Baudrate.

4.24. Set UART Baudrate *

Set UART Baudrate.

4.25. Get Output Mode *

Get the output mode of custom data format in the active reading mode.

Working mode is active and effective.

4.25.1. Command

CID1: 87H

CID2: 32H

INFO: - None

Example:

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	CHECKSUM
7C	FF	FF	87	32	00	0xNN

4.25.2. Response

CID1: 87H

RTN: 00H

INFO: - EN(8-bit): 0x00-Disabled,0x01-Enabled

- TYPE(8-bit): Output Type. (0~4)

0x00- Decimal ,

0x01- Hex ,

0x02-Wiegand,

0x03-ASCII,

0x04-BAILING

- SL(8-bit): Display the minimum data length. If the data length is less than this value, fill in 0.

- ENTER(8-bit): Whether the last position of the output data brings Carriage return character.

- ST(8-bit): Address offset value of data to be output (byte count).

- DL(8-bit): Length of data to be output (byte count).

- HL(8-bit): Whether to append fixed data length before output data.(0~20)

- HD(160-bit): Add fixed data value (fixed 20 bytes) in front of output data, fill in data according to HL value, default value is 0.

- EL(8-bit): Whether to append fixed data length after output data.(0~20)

- ED(160-bit): Add fixed data value (fixed 20 bytes) after output data, fill in data according to EI value, default value is 0.

Example:

EN=0x01, TYPE=0x00, SL=0x08, ENTER=0x01,

ST=0x02, DL=0x03,

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	EN
7C	FF	FF	87	31	30	01
TYPE	SL	ENTER	ST	DL	HL	HD(MSB)
01	08	01	02	03	01	02
--	--	--	--	--	--	--
00	00	00	00	00	00	00
--	--	--	--	--	--	--
00	00	00	00	00	00	00
--	--	--	--	HD(LSB)	EL	ED(MSB)
00	00	00	00	00	01	03
--	--	--	--	--	--	--
00	00	00	00	00	00	00
--	--	--	--	--	--	--
00	00	00	00	00	00	00
--	--	--	--	ED(LSB)	CHECKSUM	
00	00	00	00	00	0xNN	

4.26.2. Response

CID1: 87H
RTN: 00H
INFO: - None
Example:

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	CHECKSUM
CC	FE	FF	87	00	00	0xNN

4.27. Reset System

Reset System.

4.27.1. Command

CID1: D0H
CID2: 00H
INFO: - None
Example:

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	CHECKSUM
7C	FF	FF	D0	00	00	0xNN

4.27.2. Response

```
CID1:  D0H
RTN:   00H
INFO:  - None
```

Example:

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	CHECKSUM
CC	FF	FF	D0	00	00	0xNN

4.28. Restore Factory Settings

4.28.1. Command

CID1: D3H

CID2: 00H

INFO: - ARG (8-bit): Erase (0xFF)

Example : ARG=0xFF,

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	CID2	LENGTH	ARG
7C	FF	FF	D3	00	01	FF
CHECKSUM						
0xNN						

4.28.2. Response

CID1: D3H

RTN: 00H

INFO: - None

Example :

HEAD	ADDR(LSB)	ADDR(MSB)	CID1	RTN	LENGTH	CHECKSUM
CC	FF	FF	D3	00	00	0xNN

4.29. Get GPIO Mode *

Get GPIO Mode.

4.30. Set GPIO Mode *

Set GPIO Mode.