SL130 UHF RFID Reader User's Manual
V1.6

Content

1. COMMUNICATION INTERFACE SPECIFICATION

The reader communicates with host (MCU，MPU，Controller) using serial communication interface RS232 or RS485 and complete corresponding operation according to the host command. The communication parameter is 57600bps 1 start bit, 8 data bits, 1 stop bit without parity check bit. In the process of serial communication, the least significant bit of one byte is transmitted first and the least significant byte of command data sequence is transmitted first.

2. PROTOCOL DESCRIPTION

A communication procedure is sponsored by the host sending commands and data to the reader and the reader returns the result status and data to host after command execution.

Reader receives a command executes a command, only the reader complete the implementation of a command, to receive the next command. During the implementation of the command in the reader, if sending commands to the reader, the command will be lost.

The following table shows the process of the host computer command:

HOST	DIRECTION	READER
Command Data Block	→	

The interval between two consecutive bytes in the command data block should be less than 15ms. During command data block sending, synchronization will lost if the host receives any data from the reader and the host should stop command sending and restart the communication after 15ms.

The reader completes command execution in inventory ScanTime (not including host sending data time) except inventory command after receiving host command and returns the results. During the period, it doesn’t process any host data. The feedback of command execution results is as follows:

READER	DIRECTION	HOST
Command Data Block	→	

The interval between two consecutive bytes in the response data block should be less than 15ms.

3. DATA BLOCK FORMAT

3.1 COMMAND DATA BLOCK

Len	Adr	Cmd	Data[]	LSB-CRC16	MSB-CRC16

COMMENT:

	LENGTH(Byte)	COMMENT
Len	1	Command data block length 1 byte (not including itself). Value range is 4~96. The number of Len equals the length of Data [] plus 4.
Adr	1	Reader address, 1 byte. Value range is 0~254. Only will the reader conforming to the address response the command data block. Value 255 is broadcasting address. All the readers will response to the command data block with a broadcasting address. The default value shall be zero.
Cmd	1	Operation command symbol, 1 byte.
Data[]	Variable	Operation command parameters. There is no parameter if the LEN item equals 4.
LSB-CRC16	1	CRC-16 LSB. CRC-16 checksum, 2 bytes with least significant byte first.
MSB-CRC16	1	CRC-16 MSB.

3.2 RESPONSE DATA BLOCK

Len	Adr	reCmd	Status	Data[]	LSB-CRC16	MSB-CRC16

COMMENT:

	LENGTH(Byte)	COMMENT
Len	1	Response data block length 1 byte (not including itself). The number of Len equals the length of Data [] plus 5.
Adr	1	Reader address, 1 byte. Value rang is 0~254.
reCmd	1	Response command symbol, 1 byte. If the command is unrecognized, the reCmd is 0x00.
Status	1	Result status value, 1byte. Refer to following table for details.
Data[]	Variable	Response data. There is no this item if Len equals 5.
LSB-CRC16	1	CRC16 LSB .CRC-16 checksum, 2 bytes with least significant byte first.
MSB-CRC16	1	CRC16 MSB

The default value of the reader address is 0x00. The host may change it by using reader-defined command

“Write Adr”.

Cyclic Redundancy Check (CRC) computation includes all data from Len. A reference CRC computation program is presented as follow:

C-Example:

```
#define PRESET_VALUE 0xFFFF
#define POLYNOMIAL    0x8408
unsigned int uiCrc16Cal(unsigned char const    * pucY, unsigned char ucX)
{
    unsigned char ucI,ucJ;
    unsigned short int    uiCrcValue = PRESET_VALUE;

        for(ucI = 0; ucI < ucX; ucI++)
        {
            uiCrcValue = uiCrcValue ^ *(pucY + ucI);
            for(ucJ = 0; ucJ < 8; ucJ++)
            {
              if(uiCrcValue & 0x0001)
              {
                  uiCrcValue = (uiCrcValue >> 1) ^ POLYNOMIAL;
              }
              else
              {
                  uiCrcValue = (uiCrcValue >> 1);
              }
        }
    }
    return uiCrcValue;
}
```

4. OPERATION COMMAND (CMD) SUMMARY

4.1 EPC C1 G2（ISO18000-6C）COMMAND

NUM	COMMAND	CODE	COMMENT
1	Inventory	0x01	The function is used to inventory tags in the effective field and get their EPC values.
2	Read Data	0x02	The function is used to read part or all of a Tag’s Password, EPC, TID, or User memory. To the word as a unit, start to read data from the designated address.
3	Write Data	0x03	The function is used to write several words in a Tag’s Reserved, EPC, TID, or User memory.

4	Write EPC	0x04	The function is used to write EPC value in a Tag's EPC memory. Random write one tag in the effective field.
5	Kill Tag	0x05	The function is used to kill tag. After the tag killed, it never process command.
6	Lock	0x06	The function is used to set Password area as readable and writeable from any state, readable and writeable from the secured state, permanently readable and writeable, never readable and writeable. It used to set EPC, TID or User as writeable from any state, writeable from the secured state, permanently writeable, never writeable.
7	Block Erase	0x07	The function is used to erase multiple words in a Tag's Password, EPC, TID, or User memory.
8	Inventory(Single)	0x0f	The function is used to inventory one tag in the effective field and get their EPC values.
9	Block Write	0x10	The function is used to write multiple words in a Tag's Reserved, EPC, TID, or User memory.

4.2 READER DEFINED COMMAND

NUM	COMMAND	CODE	CONNECT
1	GetReader Information	0x21	This function is used to get reader-related information such as reader address (Adr), firmware version, supported protocol type, Inventory ScanTime, power and frequency.
2	Set Region	0x22	Sets the current region. The function is used to set the reader working of the lower limit and the upper limit of frequency.
3	Set Address	0x24	This function is used to set a new address of the reader. The address value will store in reader's inner nonvolatile memory. Default address value is 0x00. The value range is 0x00~0xFE. The address 0xFF is reserved as the broadcasting address. When user tries to write a 0xFF to Adr, the reader will set the value to 0x00 automatically.
4	Set ScanTime	0x25	This function is used to set a new value to Inventory ScanTime of an appointed reader. The range is 3~255 corresponding to 3*100ms~255*100ms Inventory ScanTime. The default value of Inventory ScanTime is 10*100ms.
5	Set Baud Rate	0x28	The function is used to change the serial port baud rate.
6	Set Power	0x2F	The function is used to set the power of reader.
7	Set Wiegand	0x34	The function is used to set Wiegand parameter.
8	Set WorkMode	0x35	The function is used to set work mode parameter.
9	Get WorkMode	0x36	The function is used to get work mode parameter.
10	SetRealay	0x3c	The function is used to set relay status.

11	Set query-tags parameters	0x3d	The function is used to set query-tag-parameter on actived mode
12	Get query-tags parameters	0x3e	The function is used to get query-tag-parameter on actived mode

5. LIST OF COMMAND EXECUTION RESULT STATUS

RESPONSE DATA BLOCK						**STATES**	**CONNECT**
Len	**Adr**	**reCmd**	**Status**	**Data[]**	**CRC16**		
Length of Data[] +5	0xXX	0xXX	0x00	……..	LSB+MSB	Success	Return status 0x00 to host after command is executed successfully. Data block contains result data.
Length of Data[] +5	0xXX	0x01	0x01	……..	LSB+MSB	Return before Inventory finished	Return status 0x01 to host when the reader executes an Inventory command and gets some complete **G2** tags' EPC before user-defined Inventory-ScanTime finished.
Length of Data[] +5	0xXX	0x01	0x02	……..	LSB+MSB	the Inventory-scan-time overflow	Return status 0x02 when the reader executes an Inventory command and does not get all **G2** tags' EPC before user-defined Inventory-ScanTime overflows.
Length of Data[] +5	0xXX	0x01	0x03	……..	LSB+MSB	More Data	Return status 0x03 when the reader executes an Inventory command and gets many **G2** tags' EPC, Data can not be completed within in a message, and then send in multiple.
Length of Data[] +5	0xXX	0x01	0x04	……..	LSB+MSB	Reader module flash is Full	Return status 0x04 when the reader executes an Inventory command and gets **G2** tags' EPC too much, more than the storage capacity of reader.

5	0xXX	0xXX	0x05	__	LSB+MSB	Access Password error	Return status 0x05 when the reader implements a command whit password, while the password is wrong.
5	0xXX	0x05	0x09	__	LSB+MSB	Kill Tag error	Return status 0x09 when the reader implement a Kill command, while the kill password error, or poor communication reader and tag.
5	0xXX	0x05	0x0a	__	LSB+MSB	Kill Password error can't be zero	Return status 0x0a when the Kill Password is zero.
5	0xXX	0xXX	0x0b	__	LSB+MSB	Tag Not Support the command	Return status 0x0b when the **G2 Tag** dose not supports the command.
5	0xXX	0xXX	0x0c	__	LSB+MSB	Use the command, Access Password Can't be Zero	Return status 0x0c when the **NXP UCODE EPC G2X Tag** is set read protection or EAS Alarm, the access password is zero.
5	0xXX	0x0a	0x0d	__	LSB+MSB	Tag is protected, cannot set it again	Return status 0x0d when the **NXP UCODE EPC G2X Tag** is protected.
5	0xXX	0x0a	0x0e	__	LSB+MSB	Tag is unprotected, no need to reset it	Return status 0x0e when the **NXP UCODE EPC G2X** Tag is unprotected or the tag does not support the command.
5	0xXX	0x53	0x10	__	LSB+MSB	There is some locked bytes, write fail	Return status 0x10 when the **6B Tag** is written data, while there are some locked bytes, write fail.
5	0xXX	0x55	0x11	__	LSB+MSB	can not lock it	Return status 0x11 when the **6B Tag** can't be locked.
5	0xXX	0x55	0x12	__	LSB+MSB	Be locked, cannot lock it again	Return status 0x12 when the **6B Tag** has been locked.

5	0xXX	0xXX	0x13	__	LSB+MSB	Save Fail, Can Use Before Power	Return status 0x13 when the parameter is save fail.
5	0xXX	0xXX	0x14	__	LSB+MSB	Cannot adjust	Return status 0x14 when the power can not be adjusted.
Length of Data[] +5	0xXX	0x51	0X15	……..	LSB+MSB	Return before Inventory finished	Return status 0x15 to host when the reader executes an Inventory command and gets some complete **6B** tags' UID before user-defined Inventory-ScanTime finished.
Length of Data[] +5	0xXX	0x51	0x16	……..	LSB+MSB	Inventory-Scan-Time overflow	Return status 0x16 when the reader executes an Inventory command and does not get all **6B** tags' UID before user-defined Inventory-ScanTime overflows.
Length of Data[] +5	0xXX	0x51	0x17	……..	LSB+MSB	More Data	Return status 0x17 when the reader executes an Inventory command and gets many **6B** tags' UID, Data can not be completed within in a message, and then send in multiple.
Length of Data[] +5	0xXX	0x51	0x18	……..	LSB+MSB	Reader module flash is Full	Return status 0x18 when the reader executes an Inventory command and gets **6B** tags' UID too much, more than the storage capacity of reader.
5	0xXX	0xXX	0x19	__	LSB+MSB	Not Support Command Or Access Password	Return status 0x19 when the tag can't set EAS Alarm. There may be the tag does not support the command, or the tag's access password be zero.
5	0xXX	0xXX	0xF9	__	LSB+MSB	Command execute error	Return status 0xF9 when Command execute error

5	0xXX	0xXX	0xFA	__	LSB+MSB	Get Tag, Poor Communication, Inoperable	Return status 0xFA when there are some tags in the effective field, but Poor Communication between reader and tag.
5	0xXX	0xXX	0xFB	__	LSB+MSB	No Tag Operable	Return status 0xFB when there is no tag in the effective field.
6	0xXX	0xXX	0xFC	Err_code	LSB+MSB	Tag Return Error Code	Return status 0xFC when the tag returns Error Code.
5	0xXX	0xXX	0xFD	__	LSB+MSB	Command length wrong	Return status 0xFD when the length of command operands doesn't conform to the command request.
5	0xXX	0x00	0xFE	__	LSB+MSB	Illegal command	Return status 0xFE when the command is an unrecognized command or CRC error.
5	0xXX	0xXX	0xFF	__	LSB+MSB	Parameter Error	Return status 0xFF when the command parameter is invalid.

6. TAG ERROR CODES

EPC C1G2（ISO18000-6C）Tag error codes：

Error-Code Support	Error-Code	Error-Code Name	Error Description
Error-specific	0x00	Other error	Catch-all for errors not covered by other codes.
	0x03	Memory overrun	The specified memory location does not exist or the EPC length field is not supported by the Tag.
	0x04	Memory locked	The specified memory location is locked and/or perm locked and is either not writeable or not readable.
	0x0b	Insufficient power	The Tag has insufficient power to perform the memory-write operation
Non-specific	0x0f	Non-specific error	The Tag does not support error-specific codes

7. TAG MEMORY AND ISSUES REQUIRING ATTENTION

A. EPC C1G2 TAG（G2 TAG）

Tag memory shall be logically separated into four distinct banks, each of which may comprise zero or more memory words. The four storage areas:

Reserved memory (password memory) shall contain the kill and and/or access passwords, if passwords are implemented on the Tag. The kill password shall be stored at memory addresses 00h to 1Fh; the access password shall be stored at memory addresses 20h to 3Fh.

EPC memory shall contain a Stored CRC at memory addresses 00h to 0Fh, a Stored PC at addresses 10h to 1Fh, a code (such as an EPC, and hereafter referred to as an EPC) that identifies the object to which the Tag is or will be attached beginning at address 20h, and if the Tag implements Extended Protocol Control (XPC) then either one or two XPC word(s) beginning at address 210h.

TID memory shall contain an 8-bit ISO/IEC 15963 allocation class identifier at memory locations 00h to 07h. TID memory shall contain sufficient identifying information above 07h for an Interrogator to uniquely identify the custom commands and/or optional features that a Tag supports.

User memory is optional. This area of different manufacturers is different. There is no user area in G2 tag of Inpinj Company. There are 28 words in Philips Company.

Can write protect in four distinct banks. It means this memory is never writeable or not writeable under the non-safe state; only password area can set unreadable.

B. 18000-6B TAG

6B tag has a memory space, the minimum 8 bytes (byte 0- 7) is UID of the tag, and can't be rewritten. Following byte all can be rewritten, can be locked too, but once locking, can't rewrite and unblock again.

8. DETAILED DESCRIPTION OF OPERATION COMMAND

8.1 COMMAND OVERVIEV

The reader supports three kinds of command, one kind is the ISO/IEC 18000-6 protocol command, another kind is reader-defined command, and also one kind is the transparent command.

If the host input of the command is an unrecognized command, such as the command does not support, or CRC error in the command, then the return value is as follows:

Len	Adr	reCmd	Status	CRC-16	
0x05	0xXX	0x00	0xFE	LSB	MSB

If the length of command operands doesn’t conform to the command request, the return value is as follows:

Len	Adr	reCmd	Status	CRC-16	
0x05	0xXX	0xXX	0xFD	LSB	MSB

Two kinds of command reader cannot respond:

1. The reader’s address error.
2. The command is incomplete, namely the command **Len** is longer than the actual command length.

8.2 EPC C1G2 COMMAND

8.2.1 Inventory

The command function is used to inventory tags in the effective field and get their EPC or TID values. The reader executes an ***Inventory*** command and gets tag's EPC before any other operation.

The user may accord need to establish this command the first biggest running time (Inventory scan time), before the command enquires. The reader completes command execution in inventory ScanTime (not including host sending data time) except inventory command after receiving host command and returns the results.

The default value is 0x0A (corresponding to 10*100ms=1s). The value range is 0x03~0xFF (corresponding to 3*100ms~255*100ms). In various environments, the actual inventory scan time may be 0~75ms longer than the InventoryScanTime defined.

If the inventory scan time establishes excessively short, possibly will inventory no tag appear in inventory scan time.

Command:

Len	Adr	Cmd	Data[]				CRC-16	
			Qvalue	Session	AdrTID	LenTID		
0xXX	0xXX	0x01	0xXX	0xXX	0xXX	0xXX	LSB	MSB

Parameter Connect:

Qvalue: one byte.tag number=$2^{Q,}$ range is 0 to 15.

Session: one byte.
0x00 session is S0;
0x01 session is S1;
0x02 session is S2;
0x03 session is S3;

AdrTID: One byte. It specifies the starting word address for the TID memory read. For example, **AdrTID** = 00h specifies the first 16-bit memory word, **AdrTID** = 01h specifies the second 16-bit memory word, etc.

LenTID: One byte. It specifies the number of 16-bit words to be read. The value is less then 16, otherwise, it returns the parameters error message.

Notes: *It will get tags' EPC values when the* ***AdrTID*** *and* ***LenTID*** *vacant. Otherwise, get tags' TID values. TID-inventory function is only available for reader with firmware version V2.36 and above.*

Respond:

Len	Adr	reCmd	Status	Data[]		CRC-16	
				Num	EPC ID		
0xXX	0xXX	0x01	0xXX	0xXX	EPC-1, EPC-2, EPC-3…	LSB	MSB

Parameter Connect:

Status Table:

Status	Connect
0x01	Command over, and return inventoried tag's EPC (TID).
0x02	The reader does not get all **G2** tags' EPC/TID before user-defined Inventory-ScanTime overflows. Command force quit, and returns inventoried tags' EPC (TID).
0x03	The reader executes an ***Inventory*** command and gets many **G2** tags' EPC (TID). Data can not be completed within in a message, and then send in multiple.
0x04	The reader executes an ***Inventory*** command and gets **G2** tags' EPC (TID) too much, more than the storage capacity of reader, and returns inventoried tags' EPC (TID).

Num: The number of tag detected.

EPC ID: Inventoried tag's EPC (TID) data, **EPC-1** is the first tag **EPC Len** + **EPC Data+RSSI** (**TID Len** + **TID Data+RSSI**), etc. The most significant word (EPC C1 G2 data in word units) of EPC is transmitted first and the most significant byte of word is transmitted first. **EPC** (**TID**) **Len** is one byte.

8.2.2 Read Data

The command is used to read part or all of a Tag's Password, EPC, TID, or User memory. To the word as a unit, start to read data from the designated address.

Command:

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x02	——	LSB	MSB

Data as follows:

Data[]							
ENum	**EPC**	**Mem**	**WordPtr**	**Num**	**Pwd**	**MaskAdr**	**MaskLen**
0xXX	Variable	0xXX	0xXX	0xXX	4Byte	0xXX	0xXX

Parameter Connect:

ENum: EPC length，in word units. The length of EPC is less than 15 words, can be 0 or 15. Otherwise, it returns the parameters error message.

EPC: Be operated tag's EPC number. **EPC** length according to the decision of the EPC number, EPC numbers in word units, and must be an integer number of lengths. High word first, the high byte of each word first. Requirement given here is a complete EPC number.

Mem: One byte. It specifies whether the Read accesses Password, EPC, TID, or User memory. 0x00: Password memory; 0x01: EPC memory; 0x02; TID memory; 0x03: User memory. Other values reserved. Other value when error occurred.

WordPtr: One byte. It specifies the starting word address for the memory read. For example, **WordPtr** = 00h specifies the first 16-bit memory word, **WordPtr** = 01h specifies the second 16-bit memory word, etc.

Num: One byte. It specifies the number of 16-bit words to be read. The value is less then 120, can not be 0.

Otherwise, it returns the parameters error message.

Pwd: Four bytes, they are Access Password. The most significant word of Access Password is first, the most significant byte of word is first. The first bit of 32-bit access password is left, and the last bit of 32-bit access password is right. Only done the memory set to lock and the Tag's Access Password is not zero, it needs right **Pwd**. In other cases, **Pwd** can be zero.

MaskAdr: One byte, it specifies the starting byte address for the memory mask. For example, **MaskAdr** = 0x00 specifies the first **EPC** bytes, **MaskAdr** = 0x01 specifies the second **EPC** bytes, etc.

MaskLen: One byte, it is the mask length. That a Tag compares against the memory location that begins at **MaskAdr** and ends **MaskLen** bytes later. **MaskAdr + MaskLen** must be less the length of ECP number. Otherwise, it returns the parameters error message.

Notes: *That a tag compares against complete EPC number when the* ***MaskAdr*** *and* ***MaskLen*** *vacant.*

Respond:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0xXX	0xXX	0x02	0x00	Word1，Word2,…	LSB	MSB

Parameter Connect:

Word1, Word2….: In word units, one word is two bytes. High byte is first. **Word1** is the word which reads from the start address, **Word2** is the word which reads from the second address, etc.

8.2.3 Write Data

The command is used to write several words in a Tag's Reserved, EPC, TID, or User memory.

Command:

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x03	——	LSB	MSB

Data as follows:

Data[]								
WNum	**ENum**	**EPC**	**Mem**	**WordPtr**	**Wdt**	**Pwd**	**MaskAdr**	**MaskLen**
0xXX	0xXX	Variable	0xXX	0xXX	Variable	4Byte	0xXX	0xXX

Parameter Connect:

WNum: One byte. It specifies the number of 16-bit words to be written. The value can not be 0. Otherwise, it returns the parameters error message.

ENum: EPC length，in word units. The length of EPC is less than 15 words, can be 0 or 15. Otherwise, it returns the parameters error message.

EPC: Be operated tag's EPC number. **EPC** length according to the decision of the EPC number, EPC

numbers in word units, and must be an integer number of lengths. High word first, the high byte of each word first. Requirement given here is a complete EPC number.

Mem: One byte. It specifies whether the Write accesses Password, EPC, TID, or User memory. 0x00: Password memory; 0x01: EPC memory; 0x02; TID memory; 0x03: User memory. Other values reserved. Other value when error occurred.

WordPtr: One byte. It specifies the starting word address for the memory write. For example, **WordPtr** = 00h specifies the first 16-bit memory word, **WordPtr** = 01h specifies the second 16-bit memory word, etc.

Wdt: Be written words. The most significant byte of each word is first. **Wdt** specifies the array of the word to be written. For example, **WordPtr** equal 0x02, then the first word in Data write in the address 0x02 of designated Mem, the second word write in 0x03, etc.

Pwd: Four bytes, they are Access Password. The most significant word of Access Password is first, the most significant byte of word is first. The first bit of 32-bit access password is left, and the last bit of 32-bit access password is right. Only done the memory set to lock and the Access Password is not zero, it needs **Pwd**. In other cases, **Pwd** can be zero.

MaskAdr: One byte, it specifies the starting byte address for the memory mask. For example, **MaskAdr** = 0x00 specifies the first **EPC** bytes, **MaskAdr** = 0x01 specifies the second **EPC** bytes, etc.

MaskLen: One byte, it is the mask length. That a Tag compares against the memory location that begins at **MaskAdr** and ends **MaskLen** bytes later. **MaskAdr + MaskLen** must be less the length of ECP number. Otherwise, it returns the parameters error message.

Notes: *That a tag compares against complete EPC number when the* ***MaskAdr*** *and* ***MaskLen*** *vacant.*

Respond:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x03	0x00	——	LSB	MSB

8.2.4 Write EPC

The command is used to write EPC number in a Tag's EPC memory. Random write one tag in the effective field.

Command:

Len	Adr	Cmd	Data[]			CRC-16	
			ENum	Pwd	WEPC		
0xXX	0xXX	0x04	0xXX	4Byte	Variable	LSB	MSB

Parameter Connect:

ENum: One byte, it specifies the array of the word to be written EPC length，in word units. The length of EPC is not more than 15 words, can't be 0. Otherwise, it returns the parameters error message.

Pwd: Four bytes, they are Access Password. The most significant word of Access Password is first, the most

significant byte of word is first. The first bit of 32-bit access password is left, and the last bit of 32-bit access password is right. Only done the memory set to lock and the Access Password is not zero, it needs **Pwd**. In other cases, **Pwd** can be zero.

WEPC: Be written EPC value. **WEPC** is not more than 15 words, can't be 0. Otherwise, it returns the parameters error message.

Respond:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x04	0x00	——	LSB	MSB

8.2.5 Kill Tag

The command is used to kill tag. After the tag killed, it never process command.

Command:

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x05	——	LSB	MSB

Data as follows:

Data[]				
ENum	**EPC**	**Killpwd**	**MaskAdr**	**MaskLen**
0xXX	Variable	4Byte	0xXX	0xXX

Parameter Connect:

ENum: EPC length，in word units. The length of EPC is less than 15 words, can be 0 or 15. Otherwise, it returns the parameters error message.

EPC: Be operated tag's EPC number. **EPC** length according to the decision of the EPC number, EPC numbers in word units, and must be an integer number of lengths. High word first, the high byte of each word first. Requirement given here is a complete EPC number.

Killpwd: Four bytes, they are Kill Password. The most significant word of Kill Password is first, the most significant byte of word is first. The first bit of 32-bit Kill Password is left, and the last bit of 32-bit Kill Password is right. Tag's whose Kill Password is zero do not execute a kill operation; if such a Tag receives a ***Kill*** command it ignores the command and backscatters an error code

MaskAdr: One byte, it specifies the starting byte address for the memory mask. For example, **MaskAdr** = 0x00 specifies the first **EPC** bytes, **MaskAdr** = 0x01 specifies the second **EPC** bytes, etc.

MaskLen: One byte, it is the mask length. That a Tag compares against the memory location that begins at **MaskAdr** and ends **MaskLen** bytes later. **MaskAdr + MaskLen** must be less the length of ECP number. Otherwise, it returns the parameters error message.

Notes: *That a tag compares against complete EPC number when the* ***MaskAdr*** *and* ***MaskLen*** *vacant.*

Respond:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x05	0x00	——	LSB	MSB

8.2.6 Lock

The ***Lock*** command Lock reversibly or permanently locks a password or an entire EPC, TID, or User memory bank in a readable/writeable or unreadable/unwriteable state.

Once tag's password memory establishes to forever may be readable and writable or unreadable and unwriteable, then later cannot change its read-write protection again. Tag's EPC memory, TID memory or user memory, if establishes to forever may be writeable or unwriteable, then later cannot change its read-write protection again. If sends the command to want forcefully to change the above several states, then the tag will return to the error code.

When the tag's memory established in a readable/writeable state, the command must give the Access Password, so tag's Access Password is not zero.

Command:

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x06	——	LSB	MSB

Data as follows:

Data[]						
ENum	**EPC**	**Select**	**SetProtect**	**Pwd**	**MaskAdr**	**MaskLen**
0xXX	Variable	0xXX	0xXX	4Byte	0xXX	0xXX

Parameter Connect:

ENum: EPC length，in word units. The length of EPC is less than 15 words, can be 0 or 15. Otherwise, it returns the parameters error message.

EPC: Be operated tag's EPC number. **EPC** length according to the decision of the EPC number, EPC numbers in word units, and must be an integer number of lengths. High word first, the high byte of each word first. Requirement given here is a complete EPC number.

Select: One byte, defined as follows:

0x00: Control Kill Password protection setting.
0x01: Control Access password protection setting.
0x02: Control EPC memory protection setting.
0x03: Control TID memory protection setting.
0x04: Control User memory protection setting.
Other value when error occurred.

SetProtect:

When Select is 0x00 or 0x01, **SetProtect** means as follows:

0x00: readable and writeable from any state.
0x01: permanently readable and writeable.
0x02: readable and writeable from the secured state.
0x03: never readable and writeable
When Select is 0x02, 0x03 or 0x04, **SetProtect** means as follows:
0x00: writeable from any state.
0x01: permanently writeable.
0x02: writeable from the secured state.
0x03: never writeable.
Other value when error occurred.

Pwd: Four bytes, they are Access Password. The most significant word of Access Password is first, the most significant byte of word is first. The first bit of 32-bit access password is left, and the last bit of 32-bit access password is right. **Pwd** must be right Access Password.

MaskAdr: One byte, it specifies the starting byte address for the memory mask. For example, **MaskAdr** = 0x00 specifies the first **EPC** bytes, **MaskAdr** = 0x01 specifies the second **EPC** bytes, etc.

MaskLen: One byte, it is the mask length. That a Tag compares against the memory location that begins at **MaskAdr** and ends **MaskLen** bytes later. **MaskAdr + MaskLen** must be less the length of ECP number. Otherwise, it returns the parameters error message.

Notes: *That a tag compares against complete EPC number when the* ***MaskAdr*** *and* ***MaskLen*** *vacant.*

Respond:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x06	0x00	——	LSB	MSB

8.2.7 BlockErase

The command is used to erase multiple words in a Tag's Password, EPC, TID, or User memory.

Command:

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x07	——	LSB	MSB

Data as follows:

Data[]							
ENum	**EPC**	**Mem**	**WordPtr**	**Num**	**Pwd**	**MaskAdr**	**MaskLen**
0xXX	Variable	0xXX	0xXX	0xXX	4Byte	0xXX	0xXX

Parameter Connect:

ENum: EPC length，in word units. The length of EPC is less than 15 words, can be 0 or 15. Otherwise, it returns the parameters error message.

EPC: Be operated tag's EPC number. **EPC** length according to the decision of the EPC number, EPC

numbers in word units, and must be an integer number of lengths. High word first, the high byte of each word first. Requirement given here is a complete EPC number.

Mem: One byte. It specifies whether the Erase accesses Password, EPC, TID, or User memory. 0x00: Password memory; 0x01: EPC memory; 0x02; TID memory; 0x03: User memory. Other values reserved. Other value when error occurred.

WordPtr: One byte. It specifies the starting word address for the memory block erase. For example, **WordPtr** = 00h specifies the first 16-bit memory word, **WordPtr** = 01h specifies the second 16-bit memory word, etc. **WordPtr** must be bigger than 0x00 when it erases EPC memory.

Num: One byte. It specifies the number of 16-bit words to be erased. If **Num** = 0x00, it returns the parameters error message.

Pwd: Four bytes, they are Access Password. The most significant word of Access Password is first, the most significant byte of word is first. The first bit of 32-bit access password is left, and the last bit of 32-bit access password is right. Only done the memory set to lock and the Access Password is not zero, it needs **Pwd**. In other cases, **Pwd** can be zero.

MaskAdr: One byte, it specifies the starting byte address for the memory mask. For example, **MaskAdr** = 0x00 specifies the first **EPC** bytes, **MaskAdr** = 0x01 specifies the second **EPC** bytes, etc.

MaskLen: One byte, it is the mask length. That a Tag compares against the memory location that begins at **MaskAdr** and ends **MaskLen** bytes later. **MaskAdr + MaskLen** must be less the length of ECP number. Otherwise, it returns the parameters error message.

Notes: *That a tag compares against complete EPC number when the* ***MaskAdr*** *and* ***MaskLen*** *vacant.*

Respond:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x07	0x00	——	LSB	MSB

8.2.8 Inventory (Single)

Command:

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x0f	——	LSB	MSB

Respond:

Len	Adr	reCmd	Status	Data[]		CRC-16	
				Num	EPC ID		
0xXX	0xXX	0x0f	0x01	0x01	EPC-1	LSB	MSB

Num: The number of tag detected.

EPC ID: Inventoried tag's EPC data, **EPC-1** is the first tag **EPC Len** + **EPC** data. The most significant word (EPC C1 G2 data in word units) of EPC is transmitted first and the most significant byte of word is transmitted first. **EPC Len** is one byte.

8.2.9 Block Write

The command is used to write multiple words in a Tag's Reserved, EPC, TID, or User memory.

Command:

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x10	——	LSB	MSB

Data as follows:

Data[]								
WNum	**ENum**	**EPC**	**Mem**	**WordPtr**	**Wdt**	**Pwd**	**MaskAdr**	**MaskLen**
0xXX	0xXX	Variable	0xXX	0xXX	Variable	4Byte	0xXX	0xXX

Parameter Connect:

WNum: One byte. It specifies the number of 16-bit words to be written. The value can not be 0. Otherwise, it returns the parameters error message.

ENum: EPC length，in word units. The length of EPC is less than 15 words, can be 0 or 15. Otherwise, it returns the parameters error message.

EPC: Be operated tag's EPC number. **EPC** length according to the decision of the EPC number, EPC numbers in word units, and must be an integer number of lengths. High word first, the high byte of each word first. Requirement given here is a complete EPC number.

Mem: One byte. It specifies whether the Write accesses Password, EPC, TID, or User memory. 0x00: Password memory; 0x01: EPC memory; 0x02; TID memory; 0x03: User memory. Other values reserved. Other value when error occurred.

WordPtr: One byte. It specifies the starting word address for the memory write. For example, **WordPtr** = 00h specifies the first 16-bit memory word, **WordPtr** = 01h specifies the second 16-bit memory word, etc.

Wdt: Be written words. The most significant byte of each word is first. **Wdt** specifies the array of the word to be written. For example, **WordPtr** equal 0x02, then the first word in Data write in the address 0x02 of designated Mem, the second word write in 0x03, etc.

Pwd: Four bytes, they are Access Password. The most significant word of Access Password is first, the most significant byte of word is first. The first bit of 32-bit access password is left, and the last bit of 32-bit access password is right. Only done the memory set to lock and the Access Password is not zero, it needs **Pwd**. In other cases, **Pwd** can be zero.

MaskAdr: One byte, it specifies the starting byte address for the memory mask. For example, **MaskAdr** = 0x00 specifies the first **EPC** bytes, **MaskAdr** = 0x01 specifies the second **EPC** bytes, etc.

MaskLen: One byte, it is the mask length. That a Tag compares against the memory location that begins at **MaskAdr** and ends **MaskLen** bytes later. **MaskAdr + MaskLen** must be less the length of ECP number. Otherwise, it returns the parameters error message.

Notes: *That a tag compares against complete EPC number when the* ***MaskAdr*** *and* ***MaskLen*** *vacant.*

Respond:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x10	0x00	——	LSB	MSB

8.3 18000-6B COMMAND

8.4 READ-DEFINED COMMAND

8.4.1 Get Reader Information

The host sends this command to get the reader's information including reader's address (**Adr**), firmware version, reader's type (**Type**), supported protocol (**Tr_Type**), reader power, work frequency, and InventoryScanTime value.

Command:

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x21	——	LSB	MSB

Respond:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x0d	0xXX	0x21	0x00	Version，Type，Tr_Type，DMaxFre，DMinFre，Power，Scntm	LSB	MSB

Parameter Connect:

Parameter	Length(Byte)	Connect
Version	2	The first byte is version number; the second byte is sub-version number.
Type	1	The reader type byte. 0x0D lines on
Tr_Type	1	One byte supported protocol information. Bit1 is 1 for18000-6C protocol; Bit0 is 1 for 18000-6B protocol.
DMaxFre	1	Bit7-Bit6 indicates Frequency Band and Bit5-Bit0 indicates the reader current maximum frequency.
DMinFre	1	Bit7-Bit6 indicates Frequency Band and Bit5-Bit0 indicates the reader current minimum frequency.

Power	1	The output power of reader. Range is 0 to 30, when Power is 0xFF, it means the output power of reader unknown.
Scntm	1	Inventory Scan Time, the value of time limit for ***inventory*** command.

Frequency Band:

MaxFre(Bit7)	MaxFre(Bit6)	MinFre(Bit7)	MinFre(Bit6)	FreqBand
0	0	0	0	User band
0	0	0	1	Chinese band2
0	0	1	0	US band
0	0	1	1	Korean band
0	1	0	0	RFU
0	1	0	1	RFU
…	…	…	…	…
1	1	1	1	RFU

8.4.2 Set Region

The host sends this command to change the current region of the reader. The value is stored in the reader's inner EEPROM and is nonvolatile after reader powered off.

Command:

Len	Adr	Cmd	Data[]		CRC-16	
			MaxFre	MinFre		
0x06	0xXX	0x22	0xXX	0xXX	LSB	MSB

Parameter Connect:

MaxFre: One byte, Bit7-Bit6 indicates Frequency Band and Bit5-Bit0 indicates the reader current maximum frequency.

MinFre: One byte, Bit7-Bit6 indicates Frequency Band and Bit5-Bit0 indicates the reader current minimum frequency (maximum frequency >= minimum frequency).

Frequency Band:

MaxFre(Bit7)	MaxFre(Bit6)	MinFre(Bit7)	MinFre(Bit6)	FreqBand
0	0	0	0	User band
0	0	0	1	Chinese band2
0	0	1	0	US band
0	0	1	1	Korean band
0	1	0	0	RFU
0	1	0	1	RFU
…	…	…	…	…
1	1	1	1	RFU

Respond:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x22	0x00	——	LSB	MSB

Various frequency bands formula:

User band: Fs = 902.6 + N * 0.4 (MHz), N∈ [0, 62].

Chinese band2: Fs = 920.125 + N * 0.25 (MHz), N∈ [0, 19].

US band: Fs = 902.75 + N * 0.5 (MHz), N∈ [0, 49].

Korean band: Fs = 917.1 + N * 0.2 (MHz), N∈ [0, 31].

8.4.3 Set Address

The host sends this command to change the address (**Adr**) of the reader. The address data is stored in the reader's inner EEPROM and is nonvolatile after reader powered off. The default value of **Adr** is 0x00. The range of **Adr** is 0x00~0xFE. When the host tries to write 0xFF to **Adr**, the reader will set the value to 0x00 automatically.

Command:

Len	Adr	Cmd	Data[]	CRC-16	
			Address		
0x05	0xXX	0x24	0xXX	LSB	MSB

Respond:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x24	0x00	——	LSB	MSB

***Notes**: The **Adr** is old address, not new address.*

8.4.4 Set Scan Time

The host sends this command to change the value of InventoryScanTime of the reader. The value is stored in the reader's inner EEPROM and is nonvolatile after reader powered off.

Command:

Len	Adr	Cmd	Data[]	CRC-16	
			Scantime		
0x05	0xXX	0x25	0xXX	LSB	MSB

Parameter Connect:

Scantime: Inventory Scan Time. The default value is 0x0A (corresponding to 10*100ms=1s). The value range is 0x03~0xFF (corresponding to 3*100ms~255*100ms). When the host tries to set value 0x00~0x02 to InventoryScanTime, the reader will set it to 0x0A automatically. In various environments, the actual inventory scan time may be 0~75ms longer than the InventoryScanTime defined.

Respond:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x25	0x00	——	LSB	MSB

8.4.5 Set Band Rate

The host sends this command to change the value of band rate of the reader. The value is stored in the reader's inner EEPROM and is nonvolatile after reader powered off.

Command:

Len	Adr	Cmd	Data[]	CRC-16	
			BaudRate		
0x05	0xXX	0x28	0xXX	LSB	MSB

Parameter Connect:

BaudRate: The serial port baud rate default value is 57600 bps. Defined as follows:

BaudRate	Bps
0	9600bps
1	19200 bps
2	38400 bps
5	57600 bps
6	115200 bps

Respond:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x28	0x00	——	LSB	MSB

Notes: *The response of the baud rate for the original baud rate, and next command uses the new band rate.*

8.4.6 Set Power

The host sends this command to change the power of the reader. The value is stored in the reader's inner EEPROM and is nonvolatile after reader powered off.

Command:

Len	Adr	Cmd	Data[]	CRC-16	
			Pwr		
0x05	0xXX	0x2F	0xXX	LSB	MSB

Parameter Connect:

Pwr: New power. The default value is 30(about 30dBm), it range is 0~30.

Respond:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x2F	0x00	——	LSB	MSB

8.4.7 Set Wiegand

The host sends this command to change Wiegand parameter of the reader. The value is stored in the reader's inner EEPROM and is nonvolatile after reader powered off.

Command:

Len	Adr	Cmd	Data[]				CRC-16	
			Wg_mode	Wg_Data_Inteval	Wg_Pulse_Width	Wg_Pulse_Inteval		
0x08	0xXX	0x34	0xXX	0xXX	0xXX	0xXX	LSB	MSB

Parameter Connect:

Wg_mode: Bit0: Select Wiegand format interface.

=0 Wiegand 26bits format interface.

=1 Wiegand 34bits format interface.

Bit1: High-bit first or Low-bit first.

=0 High-bit first.

=1 Low-bit first.

Bit2~Bit7: RFU. Default value is zero.

Wg_Data_Inteval: Sending Data Delay (0 ~255)*10ms, the default value is 30.

Wg_Pulse_Width: Data pulse width (1 ~255)*10us, the default value is 10.

Wg_Pulse_Inteval: Data pulse interval width (1 ~255)*100us, the default value is 15.

Respond:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x34	0x00	——	LSB	MSB

8.4.8 Set WorkMode

The host sends this command to set the reader's in Scan Mode or Trigger Mode. The host can also use this command to define the reader's output data content and format.

In Scan Mode or Trigger Mode, the reader can still accept commands from the host. But it will only respond to reader-defined commands. Other commands can not be executed when the reader in Scan Mode or Trigger Mode.

Command:

Len	Adr	Cmd	Data[]	CRC-16	
			Parameter		
0x0a	0xXX	0x35	6Bytes	LSB	MSB

Respond:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x35	0x00	——	LSB	MSB

Note: Scan Mode configuration words **Parameter** will be stored in reader's EEPROM and be effective until changed explicitly. Defined as follows:

Byte1	Byte2	Byte3	Byte4	Byte5	Byte6
Read_mode	Mode_state	Mem_Inven	First_Adr	Word_Num	Tag_Time

Parameter Connect:

Read_mode:

Bit1	Bit0	Work Mode
0	0	Answer Mode
0	1	Scan Mode
1	0	Trigger Mode(Low)
1	1	Trigger Mode(High)

Bit2~Bit7: RFU. Default value is zero.

Notes: *Answer mode, the following parameter is invalid.*

Mode_state: Bit0: Protocol bit.

=0 the reader support 18000-6C protocol.

=1 the reader support 18000-6B protocol.

Bit1: Output mode bit.

=0 Wiegand output.

=1 RS232/RS485 output.

Bit2: Beep Enable.

=0 on

=1 off

Bit3: Wiegand output, 18000-6C protocol. **First_Adr** is byte address or word address.

=0 word address.

=1 bytes address.

Bit4: Syris485 Enable. It is invalid when Bit1 is zero.

=0 Common 485

=1 Syris 485

When Bit4 = 1:

Validity: 18000-6C protocol: Read accesses Password, EPC, TID, User memory, Inventory Single.

18000-6B protocol: validity.

Bit5~Bit7: RFU. Default value is zero.

Mem_Inven: It is valid when the reader supports 18000-6C protocol. It specifies whether the Read accesses Password, EPC, TID, User memory, Inventory multiple, Inventory Single, EAS Alarm. 0x00: Password memory; 0x01: EPC memory; 0x02; TID memory; 0x03: User memory; 0x04 Inventory multiple; 0x05 Inventory Single; 0x06: EAS Alarm. Otherwise, it returns the parameters error message.

First_Adr: It specifies the starting data address for the memory read.

Support 18000-6C: **First_Adr** = 0x00 specifies the first 16-bit memory word, **First_Adr** = 0x01 specifies the second 16-bit memory word, etc.

Support 18000-6B: **First_Adr** = 0x00 specifies the first 8-bit memory byte, **First_Adr** = 0x01 specifies the second 8-bit memory byte, etc.

Word_Num: Only RS232 RS232/RS485 output, it is valid. It specifies the number of word for the memory read. The value range is 1~32. Syris 485 Mode, the value range is 1~4.

Tag_Time: Read Single Tag Delay (0 ~255)*1s. The default value is zero.

Validity: 18000-6C protocol: Read accesses Password, EPC, TID, User memory, Inventory Single.

18000-6B protocol: validity.

Output Format Connect In The Scan Mode Or Trigger Mode:

RS232/RS485, serial output format is as follows:

Notes: *RS232/RS485 serial output mode, these must be no tag in the effective field when set reader parameter.*

1.18000-6C Protocol, Mem_Inven is 0x00~0x03:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0xXX	0xXX	0xee	0x00	Word1，Word2,…	LSB	MSB

Parameter Connect:

Word1, Word2….: In word units, one word is two bytes. High-byte is first. **Word1** is the word which reads from the start address, **Word2** is the word which reads from the second address, etc.

2.18000-6C Protocol, Mem_Inven is 0x04 or 0x05:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0xXX	0xXX	0xee	0x00	EPC ID	LSB	MSB

Parameter Connect:

EPC ID: G2 tag's **ECP**, The most significant word (EPC C1 G2 data in word units) of **EPC** is transmitted first and the most significant byte of word is transmitted first.

3.18000-6C Protocol, Mem_Inven is 0x06:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0xXX	0xXX	0xee	0xee	——	LSB	MSB

4.18000-6B Protocol:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0xXX	0xXX	0xee	0x00	Word1，Word2,…	LSB	MSB

Parameter Connect:

Data []: 6B tag's UID. UID length is 8 bytes. The least significant byte of UID is transmitted first.

8.4.9 Get WorkMode

The host sends this command to get the reader's information including reader's Wiegand parameter, WorkMode parameter.

Command:

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x36	——	LSB	MSB

Respond:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x11	0xXX	0x36	0x00	Wg_mode，Wg_Data_Inteval，Wg_Pulse_Width，Wg_Pulse_Inteval，Read_mode，Mode_state，Mem_Inven，First_Adr，Word_Num，Tag_Time，accuracy，OffsetTime	LSB	MSB

Parameter Connect:

Wg_mode, Wg_Data_Inteval, Wg_Pulse_Width, Wg_Pulse_Inteval: Wiegand parameters.

Read_mode, Mode_state, Mem_Inven, First_Adr, Word_Num, Tag_Time: Work Mode parameters.

Accuracy: EAS Alarm accuracy.

OffsetTime: Syris485 response offset time.

8.4.10 SetRelay

The host sends this command to set ralay status.

Command:

Len	Adr	Cmd	Data[]	CRC-16	
			Relaystatus		
0x05	0xXX	0x3c	0xXX	LSB	MSB

Relaystatus: one byte, relay status, bit0=1, relay active;bit0=0,relay release

Respond:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x3c	0x00	——	LSB	MSB

8.4.11 Set query tags parameter

The host sends this command to set avalue and session on active mode

Command:

Len	Adr	Cmd	Data[]		CRC-16	
			QValue	Session		
0x06	0xXX	0x3d	0xXX	0xXX	LSB	MSB

QValue: one byte.tag number=$2^{Q,}$ range is 0 to 15.

Session: one byte.
0x00 session is S0;
0x01 session is S1;
0x02 session is S2;
0x03 session is S3;

Respond:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x3d	0x00	——	LSB	MSB

8.4.12 Get query tags parameter

The host sends this command to get avalue and session on active mode.

Command:

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x3e	0xXX	LSB	MSB

Respond:

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x07	0xXX	0x3e	0x00	QValue ,Session	LSB	MSB

QValue: one byte.tag number=$2^{Q,}$ range is 0 to 15.

Session: one byte.
0x00 session is S0;
0x01 session is S1;
0x02 session is S2;
0x03 session is S3;