

STA IR0507 E READER COMMUNICATION PROTOCOL

1. COMMUNICATION PROTOCOL STRUCTURE.....	1
1.1 PHYSICAL LAYER	错误！未定义书签。
1.2 DATA LINK LAYER	错误！未定义书签。
2. COMMAND FRAME DEFINITION	2
2.1 CONFIGURATION COMMAND.....	2
2.2 ISO18000-6B TAG COMMAND	6
2.3 EPC GEN2 TAG COMMAND	9
2.4 BUFFER MANAGEMENT COMMAND	12
3. TECHNICAL SUPPORT	15
4. COMMAND APPENDIX	15

Communication protocol explanation

Command Frame is defined as PC send data frame to the reader, and Response frame is defined as reader returns data frame to PC. Command frame or Response frame is the byte count with variable-length, uses Group packet method as well as with Checksum method for backward error detection.

252bytes are the longest command frame or response frame.

1 Communication Protocol Structure

1.1 Command frame's Format definition

Command frame is the data frame for PC to control reader, and the frame format is below like

Head	Addr	Len	Cmd	Parameter	...	Parameter	Check
0x0A	1 byte	n+2	1 byte	Byte 1		Byte n	cc

- Head is the symbol of frame head, defined as 0x0A.
- Addr is reader address, general address is from 0 to 240bytes, 255 (0xFF) is the public address, 254 (0xFE) is the broadcast address
- Len is Packet Length field, means the byte count of the length field back frame.
- Cmd is the Command field.
- Parameter is the parameter field of the command frame
- Check is the Checksum field, prescribed the checksum is the sum of bytes from frame head field to parameter field. (sum of all bytes, then XOR, then plus 1, for example: $0x0A + 0x2E + 0x1F = XX \text{ xor } +1$), Reader need to do Checksum for the error detection when received the command frame.

1.2 Response frame format definition

Response frame is the data frame return from reader to PC. Response frame includes reader collected data, the format definition is below like:

Head	Addr	Len	Status	Response	...	Response	Check
0x0B	1 byte	n+2	1 byte	Byte 1		Byte n	cc

- Head is the packet type field, response frame packet type is fixed to 0x0B
- Addr is the reader address
- Len is Packet Length field, means the byte count of the length field back frame.
- Status is the result of executing the command frame, '0' means correct operation, others mean operation abnormal.
- Response is the return data from the response frame.
- Check is the Checksum field, prescribed the checksum is the sum of bytes from frame head field to parameter field. (sum of all bytes, then XOR, then plus 1, for example: $0x0A + 0x2E + 0x1F = XX \text{ xor } +1$), Reader need to do Checksum for the error detection when received the command frame.

Status field value prescribed like the below table

No.	Value	Name	Description
1	0x00	ERR_NONE	successful command completion
	0x01	ERR_GENERAL_ERR	General error
	0x02	ERR_PAR_SET_FAILED	Set Parameter failed
	0x03	ERR_PAR_GET_FAILED	Get Parameter failed
	0x04	ERR_NO_TAG	No tag.
	0x05	ERR_READ_FAILED	Read tag failed
	0x06	ERR_WRITE_FAILED	write tag failed
	0x07	ERR_LOCK_FAILED	Lock tag failed
	0x08	ERR_ERASE_FAILED	Erase tag failed
	0x09		
	0x0A		
	0xFE	ERR_CMD_ERR	command does not support or exceed parameter range.
	0xFF	ERR_UNDEFINED	undefined error

2 Command frame definition

2.1 System configuration command

2.1.1 Set Baud Rate

Set reader's RS232 Serial port communication Baud Rate

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x03	0x20	baudrate	cc

Baudrate is parameter that need to config. The specific Baudrate parameter definition are:

0x00, 9600bps; 0x01, 19200bps; 0x02, 38400bps; 0x03, 57600bps; 0x04, 115200bps.

When received the above command frame, reader returns a no data response frame with the previous baudrate, then revises the reader parameter with new baudrate for the communication.

2.1.2 Reset Reader

Reset Reader command frame

Head	Addr	Len	Cmd	Check
------	------	-----	-----	-------

0x0A		0x02	0x21	cc
------	--	------	------	----

When received the above command frame, reader returns a no data response frame first, then reset the reader.

2.1.3 Get Firmware Version

Get reader Firmware version command frame

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x22	cc

When received the above command frame, reader returns a response frame, in this response frame, the command data is BootLoader or reader's firmware version, the response frame format is below like:

Head	Addr	Len	Status	Response	Response	Check
0x0B		0x04	0x00	Major	Minor	cc

Major is the firmware's Main version

Minor is the firmware's Minor version.

2.1.4 Set Rf Power

Set reader's RF Power

Head	Addr	Len	Cmd	Par1	Par2	Par3	Par4	Check
0x0A		0x06	0x25	Pwr1	Pwr2	Pwr3	Pwr4	cc

Pwr 1-4 are the 4 antennas' RF power

When received this command frame, reader revises the RF power value, and returns no data response frame.

2.1.5 Get Rf Power

Get Reader's RF Power

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x26	cc

Response frame is below like

Head	Addr	Len	Status	Par1	Par2	Par3	Par4	Check
0x0B		0x06	00	Pwr1	Pwr2	Pwr3	Pwr4	cc

2.1.6 Set Frequency

Set reader's Frequency

Head	Addr	Len	Cmd	Par1	Par2	Check
0x0A		XX	0x27	Freq num(n)	Freq points(n bytes)	cc

Freq num: Frequency number, if Freq num≠0, Frequency of reader is the fixed frequency point listed in the Freq points, if Freq num=0, then Frequency of reader is a byte of Freq points, represents a certain area frequency:

0: China

1: North American

2: European

Self defined frequency range in the Freq points is from 900MHz to 930MHz, progressively increased by 250 KHz.

2.1.7 Get Frequency

Get reader frequency

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x28	cc

Reader response frame is below like:

Head	Addr	Len	Status	Par1	Par2	Check
0x0B		XX	00	Freq num	Freq points(n bytes)	cc

2.1.8 Set Antenna

Set reader antenna

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x03	0x29	Work ant	cc

Work ant is the working antenna, represented in mask. 4 low bits correspond with 4 antennas' status, '1' means antenna open, '0' means antenna no open, 4 high bits have not meaning.

When received the above command frame, reader returns no data response frame.

2.1.9 Query Antenna

Query Antenna working status

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x2A	cc

Reader returns below like response frame:

Head	Addr	Len	Status	Response	Response	Check
0x0B		0x04	0x00	Work ant	Ant Status	cc

Work ant is the working antenna, represented in mask.

Ant Status represents the available working antennas, represented in mask, '1' means antenna open, '0' means antenna no open

2.1.10 Set Single Fast Tag Mode

Tag reading mode setting

Head	Addr	Len	Cmd	Parameters	Check
0x0A		0x03	0x15	Mode	cc

If mode = '0', it's favor speed reading mode for single tag (as well as few tags) fast reading, if mode≠0, it's favor quantity reading mode for multi tags reading.

When received the above command frame, reader returns no data response frame.

2.1.11 Get Single Fast Tag Mode

Get Tag reading mode

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x16	cc

Reader returns below like response frame:

Head	Addr	Len	Status	Response	Check
0x0B		0x03	0x00	Modulate_type	cc

2.1.12 Set Test Mode

Reader Test Mode setting

Head	Addr	Len	Cmd	Mode	Check
0x0A		0x03	0x2F	Mode	cc

Mode: '00' open Amplifier;

'01' close Amplifier

'02' Antenna adjustment, Antenna adjustment is begin when 4 antennas are disconnected.

2.1.13 Set OutPort

Set IO Output (when reader is turn on, the default IO output is High level voltage)

Head	Addr	Len	Cmd	Parameter	Parameter	Check
0x0A		0x04	0x2D	Num	level	cc

Num is IO port number, 00 & 01 are two sets output port, 02 is relay output.

Level is output voltage, '0' is low level voltage, and '1' is high level voltage.

2.1.14 Set IP

IP address setting

Head	Addr	Len	Cmd	IP	PORT	Check
0x0A		0x10	0x2C		AA+BB	cc

IP: 4bytes IP address;

4bytes Subnet Mask

4bytes Gateway

Port: Port number, 2bytes, AA is Little Endian, BB is Big Endian

Take the below example for the reference of reader config:

If IP is 192.168.1.200, port is: 100 and the command is below like:

0A FF 10 2C C0 A8 01 C8 FF FF FF 00 C0 A8 01 01 64 00 BF

C0 A8 01 C8 = 192.168.1.200

FF FF FF 00 = 255.255.255.0

C0 A8 01 01 = 192.168.1.1

Port: 64 =100

2.1.15 Get IP

Get IP address

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x2B	cc

Returns

Head	Addr	Len	Status	Response	Check
0x0B		0x10	0x00	IP	cc

IP: 4bytes IP address;

4bytes Subnet Mask

4bytes Gateway

Port: Port number, 2bytes, AA is Little Endian, BB is Big Endian

2.1.16 Update reader parameter

Update all of the reader parameter and refresh the reader (Note: difference to the reset)

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x03	0x2F	05	cc

2.1.17 Set LED & Buzzer ON/OFF

LED & Buzzer ON/OFF Setting

Head	Addr	Len	Cmd	Parameter	Parameter	Check
0x0A		0x04	0x23	1B	level	cc

Level: ON/OFF Control Level, 00---OFF LED&Buzzer, 03---Open LED&Buzzer.

2.2 ISO18000-6B tag operation command

2.2.1 Iso Multi Tag Identify

ISO18000-6B tag Multi tag identify

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x60	cc

Reader starts multi tags identify when received the above command frame, and returns the identified tag number, tag information is stored in the reader buffer. The Response frame is below

like:

Head	Addr	Len	Status	Response	Check
0x0B		0x03	0x00	TagCount	cc

TagCount is tags' number.

2.2.2 Iso Multi Tag Read

ISO18000 multi tag information data read

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x03	0x61	Start Addr	cc

Start Addr is the starting address of to be USER data

Reader starts the multi tags identify when received the above command frame and identifies each tag's 8bits data from the start addr. The reader returns the multi tag account when finish the multi tags identify, tag data is stored in the reader buffer. The response frame is below like:

Head	Addr	Len	Status	Response	Check
0x0B		0x03	0x00	TagCount	cc

2.2.3 Iso Write

ISO18000-6B tags write in one byte.

Head	Addr	Len	Cmd	Parameter	Parameter	Check
0x0A		0x04	0x62	Addr	Value	cc

Addr is the address of the writing tag.

Value is the writing value

Reader returns a no data response frame.

2.2.4 Iso Read with UID

Read data with the ISO18000-6B Tag UID

Head	Addr	Len	Cmd	Parameter	Parameter	Check
0x0A		0x0B	0x63	UID(8byte)	Addr	cc

Addr is the starting address; UID is the ISO18000-6B Tag unique ID; Reader returns a 9bytes value.

Head	Addr	Len	Status	Response	Check
0x0B		0x0B	0x00	9 字节	cc

In this return value, the 1st byte is antenna No., other 8bytes are the tag data.

2.2.5 Iso Write with UID

ISO18000-6B writing with UID

Head	Addr	Len	Cmd	Parameter	Parameter	Parameter	Check
0x0A		0x0B	0x64	UID(8byte)	Addr	Value	cc

Addr is the address of the writing tag.

Value is the writing value

UID is the ISO18000-6B tag Unique ID

Reader returns a no data response frame.

2.2.6 Iso Lock

ISO18000-6B tag data lock

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x03	0x65	Addr	cc

Addr is the locking address of the ISO18000-6B tag.

2.2.7 Iso Query Lock

ISO18000-6B tag querying lock

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x03	0x66	Addr	cc

Addr is the address of the querying tag.

Response frame is below like:

Head	Addr	Len	Status	Response	Check
0x0B		0x03	0x00	Lock Status	cc

Lock Status: '0' means unlocked, '1' means locked

2.2.8 Iso Lock with UID

ISO18000-6B tag lock with UID

Head	Addr	Len	Cmd	Parameter	Parameter	Check
0x0A		0x0B	0x69	UID(8byte)	Addr	cc

Addr is the address of the locking tag

UID is the ISO18000-6B tag Unique ID.

Reader returns a no data response frame.

2.2.9 Iso Query Lock With UID

ISO18000-6B tag query lock with UID

Head	Addr	Len	Cmd	Parameter	Parameter	Check
0x0A		0x0B	0x6A	UID(8byte)	Addr	cc

Addr is the address of the querying tag.

UID is the ISO18000-6B tag Unique ID

Response frame is below like:

Head	Addr	Len	Status	Response	Check
0x0B		0x03	0x00	Lock Status	cc

Lock Status: '0' means unlocked, '1' means locked.

2.2.10 Iso Single Tag Read

ISO18000-6B single tag read

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x03	0x68	Addr	cc

Addr is the tag starting address, if Addr is '0', reads UID and reader return 9bytes tag data.

Head	Addr	Len	Status	Response	Check
0x0B		0x0B	0x00	9 字节	cc

In this return data, the 1st byte is antenna No., other 8bytes are the tag data.

2.3 EPC Class1 Gen2 Tag Command

2.3.1 Gen2 Multi Tag Inventory

EPC Gen2 Multi Tag inventory

Head	Addr	Len	Cmd	Par	Check
0x0A		0x03	0x80	01	cc

If Par=00, reader starts the first EPC Gen2 multi tag read,

If Par=01, reader starts the active reading, and returns the tag number when finished this

identify, tag data is stored in the reader buffer. Response frame is below like:

Head	Addr	Len	Status	Response	Check
0x0B		0x03	0x00	TagCount(2 bytes)	cc

TagCount is the identified tag number, display in two bytes, big endian.

2.3.2 Gen2 Multi Tag Inventory Stop

EPC Gen2 multi tag inventory stop

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x81	cc

Reader stops the EPC Gen2 multi tag inventory when received the above command frame.

2.3.3 Gen2 Multi Tag Read Settings

EPC Gen2 Multi Tag Read Setting is to define and set EPC Tag's Membank, the first addr and

the length of the Address.

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x0B	0x84	Wordptr&length(9bytes)	cc

9bytes Wordptr&Length is defined as the following 9 definitions:

1. MasMembankMask: from 1 to 4 are Reserve Membank, EPC Membank, TID Membank and User Membank.
2. ReserveWordPtr: Set the first reading address of the Reserve Membank.
3. ReserveWordCnt: The word count of the Reserve Membank
4. EpcWordPtr: Set the first reading address of the EPC Membank
5. EpcWordCnt: The word count of the EPC Membank
6. TidWordPtr: Set the first reading address of the TID Membank
7. TidWordCnt: The word count of the TID Menbank
8. UserWordPtr: Set the first reading address of the User Membank
9. UserWordCnt: The word count of the User Membank

Attention: The EPC Membank is read on default, and the reading length of default EPC reading is based on the PC, while if the EPC default reading is longer than PC requirement, using this command frame to get EPC reading.

When reader receives the above command frame, the reader will start the reading with the pre-setting to read tags' multi Membank, the Membank's first reading address, and the length of the Membank. It can read multi Membank at the same time. Tag data is stored in the reader buffer, and via *Get Tag Data* command to get buffer data. The response frame is below like:

Head	Addr	Len	Status	Response	Check
0x0B		0x04	0x00	TagCount(2 bytes)	cc

2.3.4 Gen2 Muti Tag Write

EPC Gen2 Multi Tag Write

Head	Addr	Len	Cmd	Parameter	Parameter	Parameter	Parameter	Check
0x0A		0xXX	0x85	Membank	Word Addr	len	Data	cc

WorldAddr is the address of the encoding word

Data means the encoding data, encoding length is Len*2

When reader received the above command frame, it will start the qualified multi tags encoding in the reader's radiation range, and returns the success encoding tags' number, the success encoding tags' EPC data is stored in the reader buffer, and get these tags data via *Get Tag Data* command.

2.3.5 Gen2 Kill

Epc Gen2 Tag kill

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x06	0x83	Password	cc

Password is EPC Gen2 Tag 4bytes Kill Password.

Reader returns a no data response frame

2.3.6 Gen2 Secured Read

Head	Addr	Len	Cmd	Parameter	Parameter	Parameter	Parameter	Check
0x0A		0x09	0x88	Acc Pwd(4Bytes)	Membank	Word Addr	WordCnt	cc

Acc Pwd: EPC Gen2 Tag 4bytes Access Password

Membank is the reading Membank

WordAdr is the starting reading address of the Membank.(word unit)

WordCnt is word count

Attention: If access password is 0, the password is considered as not encrypted, and the reader executes the normal reading of the EPC tag.

2.3.7 Gen2 Secured Write

Head	Addr	Len	Cmd	Parameter	Parameter	Parameter	Parameter	Check
0x0A		0x0A	0x89	Acc Pwd(4Bytes)	Membank	World Addr	Value (2bytes)	cc

Acc Pwd: EPC Gen2 Tag 4bytes Access Password

World Addr is the encoding word address (from 0-5)

Value is 2bytes encoding data.

When received the above command frame, reader encodes a word (2bytes) into the specified address of the tag, and returns a no data response frame.

Attention: If access password is 0, the password is considered as not encrypted, and the reader executes the normal encoding of the EPC tag.

2.3.8 Gen2 Secured Lock

Head	Addr	Len	Cmd	Parameter	Parameter	Parameter	Check
0x0A		0x08	0x8A	Acc Pwd(4Bytes)	MemBank	Level	cc

Acc Pwd: EPC Gen2 Tag 4bytes Access Password

Membank is the EPC tag's to be locked MemBank, from 0 to 4 are: User Membank, TID

Membank, EPC Membank, Access Password Membank, Kill Password Membank.

Lock Level: '0'---unlock; '1'---unlock forever; '2'---secure lock; '3'---Lock forever

Attention: If access password is 0, the password is considered as not encrypted, and the reader executes the normal single EPC tag lock.

2.3.9 Gen2 Select Config

EPC Gen2 Select Config

Head	Addr	Len	Cmd	Parameter	Parameter	Parameter	Parameter	Parameter	Check
0x0A		0xXX	0x8F	Action	Membank	Bit Ptr (2bytes)	Length	Mask(Nb ytes)	cc

Action: '0'---Matched tag, '1'---mismatched tag

Membank is the Matched Membank

Bit Ptr is bit address, for example, EPC first word's bit address is 0x20

Length: the comparison bit length;

Mask: the comparison data, biggest 16bytes.

2.3.10 Set Gen2 Parameters

Set Reader's EPC Gen2 related Parameters:

Head	Addr	Len	Cmd	Par1	Par2	Par3	Par4	Check
0x0A		0x06	0x8E	Session	Rsv	Rsv	Rsv	cc

Session: used for EPC Gen2 inventory

Rsv: reserved for the future purpose.

2.4 Buffer Management command

2.4.1 Get ID and Delete

Get tag's EPC code (or ISO18000-6B Tag's ID code) from reader buffer, and then delete buffer data.

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x03	0x40	Count	cc

Count is the tag number, biggest 18bytes. And the response frame is below like:

Head	Addr	Len	Status	Response	Response	Check
0x0B		14*n+3	0x00	Count	Data(14*n)	cc

Count is the uploaded tag number, Data is the tag code, 14bytes a set, the first byte of the 14bytes is the tag type, the second byte is the antenna number, and the left 12bytes are the EPC code.

2.4.2 Get Tag Data

Get tag data from reader buffer.

Head	Addr	Len	Cmd	Parameter	Check
0x0A		0x03	0x41	Count	cc

Count is the downloaded tag number, 16bytes biggest, (not exceed the limits of the biggest frame requirement), the response frame is below like:

Head	Addr	Len	Status	Response	Response	Check
0x0B			0x00	Count	Data	cc

Count is the upload data count, data is the tag data.

Data unit is set, the first byte of each set is the length of this set (exclude the first byte), and the left bytes are the valid tag data. The following are the common data set of the return data:

ISO18000-6B tag Identify

Len	ant	ID
9	1byte	8bytes

EPC Tag Identify

Len	ant	EPC
13	1byte	12 bytes EPC code

Attention: Depends on different EPC tag Chip, the EPC code can be more than 12bytes.

EPC Read

Len	ant	EPC+DATA
n	1byte	EPC Code + other Membank data

n= the total reading bytes of the data + EPC length. EPC length is variable; the length of EPC code in return is according to the n minus the length of the total reading Membank data.

2.4.3 Query ID Count

Query buffer data count.

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x43	cc

Reader response frame is below like.

Head	Addr	Len	Status	Response	Check
0x0B		0x03	0x00	Count (2Bytes)	cc

Count is the tag number in the buffer.

2.4.4 Clear ID Buffer

Clear ID buffer

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x44	cc

No data response frame from the reader

- ✧ Each time, when send Identify, read or write command to the reader, reader buffer will automatically empty buffer data
- ✧ In Trigger reading mode, the data is saved in nonvolatile data storage with power-down data protection.

2.4.5 Clear Buffer

Empty the external memory

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x48	cc

No data response frame from the reader

Data is saved in nonvolatile data storage with power-down data protection.

2.4.6 Get Buffer Count

Query the external memory tag number:

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x49	cc

Reader response frame is below like:

Head	Addr	Len	Status	Response	Check
0x0B		0x04	0x00	Count (2Bytes)	cc

Count is the tag number in the buffer

2.4.7 Get Buffer Data

Get tag data from the external memory:

Head	Addr	Len	Cmd	Check
0x0A		0x02	0x4A	cc

Response frame is below like:

Head	Addr	Len	Status	Response	Response	Check
0x0B			0x00	Count	Data	cc

Count is the total uploaded sets of tag data, data is the tag data.

Data unit is set, the first byte of each set is the length of this set (exclude the first byte), and the left bytes are the valid tag data. The following are the common data sets of the return data:

ISO18000-6B Tag Identify

Len	ant	ID
9	1byte	8bytes

EPC Tag Identify

Len	ant	EPC
13	1byte	12bytes EPC code

Attention: Depends on different EPC tag Chip, the EPC code can be more than 12bytes.

EPC read

Len	ant	EPC+DATA
n	1byte	EPC code+ Other Membanks' data

n= the total reading bytes of the data + EPC length. EPC length is variable; the length of EPC code in return is according to the n minus the length of the total reading Membank data.

Data is saved in nonvolatile data storage with power-down data protection.

3. Technical Support

If you are requesting support for reader product, please have your reader's model number, serial number and firmware revision ready. Stallion is committed to providing rapid and effective support to its customers and partners.

4. Command Appendix
