Communication Protocol Instruction

1. Communication Protocol Design

Communication protocol is a communication agreement which a host PC can communicate with a reader/writer via RS-232 communication interfaces.

RS-485 communication interface support RS-232 communication protocol in the data link layer, but there is a protocol extension.

USB and RS-485 communication interface abide by the same communication protocol as RS-232 in the data link layer.

Communication protocol adopts byte-oriented asynchronous data communication protocol format. It's stipulated that the data frame which is transferred from PC to reader/writer is called Command, and the data frame return to PC(from reader/writer) is called Response. Command or response frame is variable-length bytes, which is using group packet method and conduct after error detection by checksum method.

The max byte for command or response data is 256bytes.

1. 1 Communication Protocol Structure

Communication protocol including the following hierarchical Structure: physical Layer, link layer and application layer.

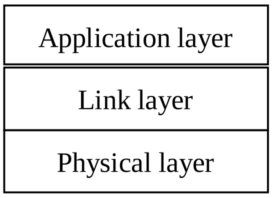

Figure 1: Communication protocol diagram

1. 1. 1 Physical Layer

The physical layer completes the signal transmission and reception of bit data.
Physical layer should comply with corresponding communication interfaces requirements.

1. 1. 1. 1 RS-232 Physical Layer Regulation Data Link Layer

- 1 start bit, 8 data bits, 1 stop bit, no parity checking
- The communication baud rate is set to be 2400bps, 4800bps, 9600bps, 19200bps, 38400bps, 57600bps, 115200bps

optional. The initial baud rate is 9600bps after the reader power on or reset, it can be changed by the command of PC. The baud rate will back to 9600bps in case the PC and reader transmission error occurs.

1． 1． 2 Data Link Layer

Data link layer specified command, response frame types and data formats. Frame type including command frame, response frame, and response frames completion from readers to confirm commands.

1． 1． 2． 1 Definition of Command Frame Format

Command frame is a kind of data frame which is transferred between PC and reader. As shown in the following table,

Packet Type	Station Num	Length	Command Code	Command Data	…	Command Data	Command Data	Checksum
0xA5	0xFF	n+2	1 byte	Byte 1		Byte n-1	Byte n	cc

- Packet Type is the domain of packet type, it is fixed for 0xA5.
- Station Num is the domain of station address, it represents the unique identification of reader in the BUS network.. 0xFF means an arbitrary station, 0x00 means broadcast address, 0x01~0xFE mean any independent station.
- Length is the domain of packet length, it represents the total byte number of frame after length domain.
- Command Code is the domain of command code.
- Command Data is the parameter domain of command frame.
- Checksum is the domain of Checksum, it stipulates that the checking range is the checksum of all bytes from packet type field to the last byte of parameter domain. Reader is required to calculate checksum for error detection after receiving the command frame. (Checksum=0-all bytes from packet type field to the last byte of parameter domain.)

To illustrate this algorithm, here we take the following command frame for example to explain,

Packet Type	Station Num	Length	Command Code	Command Data	Checksum
0xA5	0x00	3	0x92	04	cc

Caculating process of the command frame CheckSum as below,

1. A5+0+3+92+4=0x17E;
2. 0x17E extract 0x7E to transfrom binary system as 01111110, extract the inverse number and add 1, then transform HEX as 0xC2;
3. Complete command frame is A5 00 03 92 04 C2.

1． 1． 2． 2 Definition of Response Frame

Response frame is data frame which is returned from reader, it contains the data or status value that reader should return to PC.

The definition is as shown in the table below,

Packet Type	Station Num	Length	Response Code	Response Data	…	Response Data	Response Data	Checksum

0xE5	0xFF	n+2	1 byte	Byte 1		Byte n-1	Byte n	cc

- Packet Type is the domain of packet type, it is fixed for 0xE5.
- Station Num is the domain of station address, it represent the unique identification of reader in the BUS network.
- Length is the domain of packet length, it represents the total byte number of frame behind the length domain.
- Response Code is the domain of response code, the value is the command code of the responsive comamnd frame.
- Response Data is the parameter domian of response frame.
- Checksum is the domain of Checksum, it stipulates that the checking range is the checksum of all bytes from packet type field to the last byte of parameter domain. PC is required to calculate checksum for error detection after receiving the command frame. Station Num is participate in the calculation checksum, the calculation method is the same as the method of command frame.

1．1．2．3 The format definition of the response frames completion from readers to confirm commands.

Response frame of reader command completion is data frame of fixed length, as shown in the following table,

Packet Type	Station Num	Length	Command Code	Status	Checksum
0xE9	0xFF	0x03	1 byte	1 Byte	cc

- Packet Type is the domain of packet type, packet type of command frame is fixed for 0xE9.
- Station Num is the domain of station address, it represent the unique identification of reader in the BUS network.
- Length is the domain of packet length, represents the byte number of frame behind the length domain, and fixed for 0x03.
- Command Code is the domian of command code.
- Status is the domain of status.
- Checksum is the domain of Checksum, it stipulates that the checking range is the checksum of all bytes from packet type field to the last byte of parameter domain. Reader is required to calculate checksum for error detection after receiving the command frame. Station Num is participate in the calculation checksum, the calculation method is the same as the method of command frame.

1. 2 Definition of Command Frame in Data Link Layer

Data link layer protocol specified the communication format, command and command parameter between reader and host pc. According to functon of different communication protocol, command frame in data link layer contains communication protocol of reader operation and communication protocol of tag operation.

1．2．1 Cmmunication protocol of reader operation

Cmmunication protocol of reader operation specified the basic function of reader and data communication formate of setting.

1．2．1．1 Set Parameter

Set up configuring parameter of reader

Length	Command Code	Parameter Count	AddrH	AddrL	Parameter	Checksum
n+5	0x72	n	1 byte	1 byte	n Bytes	cc

- Parameter Count is the byte number of parameter needs to be set.
- AddrH means the high byte of address for the first byte of configurating parameter in the EEPROM.
- AddrH means the low byte of address for the first byte of configurating parameter in the EEPROM.
- Parameter is the parameter data needs to be set.

The reader will write the configurating parameters into EEPROM after receiving this command frame, and return the command completing frame.

1．2．1．2 Get Parameter

Reading configuring parameter value EEPROM.

Length	Command Code	Parameter Count	AddrH	AddrL	Checksum
5	0x73	n	1 byte	1 byte	cc

- Parameter count is the reading byte number of parameters.
- AddrH means the high byte of address for the first byte of reading parameter in the EEPROM.
- AddrH means the low byte of address for the first byte of reading parameter in the EEPROM.

The reader will read the configurating parameters after receiving this command frame, and return the command completing frame. The format for command frame is as below table,

Length	Command Code	Parameter Count	AddrH	AddrL	Parameter	Checksum
n+5	0x73	n	1 byte	1 byte	n Bytes	cc

- Parameter count is the reading byte number of parameters.
- AddrH means the high byte of address for the first byte of reading multi-parameter in the EEPROM.
- AddrH means the low byte of address for the first byte of reading multi-parameter in the EEPROM.
- Parameter is the “n” byte parameters data when reading

1．2．1．3 Set Baud Rate

Set the communication baud rate of reader by RS-232 or RS-485 interface.

Length	Command Code	Command Data	Checksum
3	0x74	Baud Rate	cc

- Baud Rate is the baud rate parameter needs to be set. The specific parameter defined as 0x00，2400bps；0x01，4800bps；0x02，9600bps；0x03，19200bps；0x04，38400bps；0x05，57600bps；0x06，115200bps。

When host set up baud rate of reader, it is only apply to change current baudrate while communicating with reader using RS-232 or RS-485. After receiving the command, readers will return the response frame completion back to the host and the new Baud Rate will be used for the communication.

1．2．1．4 Reset Reader

Reset the command frame of reader

Length	Command Code	Checksum
2	0x75	cc

After receiving this command, reader will return the response frame completion back to the host and the reader will be reset.

1．2．1．5 Stop RF Work

Stoping reads tag automatically.

Length	Command Code	Checksum
2	0x60	cc

After receiving this command frame, reader will stop to identify tag automatically. According to different working mode of reader, this command frame has different effect on reader. Under auto working mode or triggering working mode that is valid trigger, reader will stop to identify tag automatically; Under master-slave mode, it won't effect the working condition of reader.

Reader will return the command completion frame.

1．2．1．6 Start RF Work

Starting reads tag automatically.

Length	Command Code	Checksum
2	0x62	cc

After receiving this command frame, reader will start to identify tag automatically. According to different working mode of reader, this command frame has different effect on reader. Under auto working mode or triggering working mode that is valid trigger, reader will start to identify tag automatically; Under master-slave mode, it won't effect the working condition of reader.

Reader will return the command completion frame.

1．2．1．7 Get Firmware Version

Reading the firmware version of reader software.

Length	Command Code	Checksum
2	0x7A	cc

After receiving this command, the reader will return the response frame. The command data in response frame is BootLoader or the firmware version of the reader software. The format of response frame is as the table below:

Length	Response Code	Response Data	Response Data	Response Data	Response Data	Checksum
6	0x7A	Firmware Flag	Firmware Major	Firmware Minor	Firmware Release	cc

- Firmware Flag is the mark of reader firmware program.
- Firmware Major is the chief version of reader firmware program.
- Firmware Minor is the secondary version of reader firmware program.
- Firmware Release is the release time of reader firmware program under the current chief and secondary version.

Calling this communication protocol can test the communication interface staus of reader and aware of the firmware version, so as to avoid the wrong firmware to cause uncertainty of products function.

1．2．1．8 ID Match Start

Reader support ID match function. Before using this function, all the ID data should be written into reader and the entire operation should to be an atomic operation. It’s designed for 3 command packets which support ID match function.

ID Match Start command means starting ID matching

Length	Command Code	Command Data	Command Data	Command Data	Checksum
2	0x40	Order	Length	Count 4Byte	cc

- Order is the order of ID match.
- Length is the byte number needs to be matched.
- Count is the ID number of matching tag.

After receiving the command, the reader start ID matching, initialize the store data and return the command completing frame.

1．2．1．9 ID Match Data

Starting writes the ID data to the reader which needs to be matched.

Length	Command Code	Command Data	Command Data	Command Data	Checksum
n+4	0x41	Tag Type	Length n	Data nByte	cc

- Tag Type is tag type is the type of tag..
- Length is length is the length of tag ID.
- Data is the ID code of tag.

After receiving the command, the reader will write tag ID into the relevant ID matching stock area and return the command completing frame.

1．2．1．10 ID Match End

End imputing the ID matching data.

Length	Command Code	Checksum
2	0x42	cc

After receiving the command, the readers return the command completing frame.

1．2．1．11 Set Date Time

Set current date and time for reader.

Length	Command Code	Command Data	Command Data	Command Data	Command Data	Command Data	Command Data	Checksum
8	0x48	Year	Month	Day	Hour	Minute	Second	cc

- Year is year of reader needs to be set, the actual vaule have the deviation of 2008, for example, 0 means 2008 year.
- Month is month of reader needs to be set, and the vaule is from 1~12.
- Day is day of reader needs to be set.
- Hour is the hour of reader needs to be set.
- Minute is minute of reader needs to be set.
- Second is second of reader needs to be set.

After receiving this command frame, it can update the date and time of reader, and return command completion frame.

1．2．1．12 Get Date Time

Check current date and time of reader.

Length	Command Code	Checksum
2	0x49	cc

After receiving this command, the reader will return response frame. The format of response frame is as below,

Length	Response Code	Response Data	Response Data	Response Data	Response Data	Response Data	Response Data	Checksum
8	0x49	Year	Month	Day	Hour	Minute	Second	cc

- Year stands for reader date of the year.
- Month stands for reader date of the Month.
- Day stands for reader date of the days.
- Hour stands for reader time of the hours.
- Minute stands for reader time of minute.
- Second stands for reader time of second..

1．2．1．13 Get Trig State

Check trigger/input state command frame

Length	Command Code	Checksum
2	0x56	cc

After receiving this command, the reader will return response frame. The format of response frame is as below,

Length	Response Code	Response Data	Checksum
3	0x56	state	Cc

- State stands for trigger input state.

1. 2. 1. 14 Set Relay State

Setup relay working state command frame.

Length	Command Code	Command Data	Command Data	Checksum
4	0x57	Mask	State	cc

- Mask is the bit mask of relay which needs to set. D0 stands for operating relay. The State value will effect the relay status if the DO is 1. It won’t effect if it is 0. The definition for D1-D3 is the same as D0, it respectively stands for operation of relay 2~relay 4.
- State is the bit mask of relay status which needs to change. The relay is closed if it is 1 and it’s open if it is 0. When the relay is closed and it has configured as open automatically, it will automatically open once it has over the time of relay delay.

After receiving this command, the reader will set the relay status and return the command completing frame.

1. 2. 1. 15 Get Relay State

Check relay working state command frame.

Length	Command Code	Checksum
2	0x58	cc

After receiving this command, the reader will return the response frame. The format of response frame is as below,

Length	Response Code	Response Data	Checksum
3	0x58	state	cc

- State stands for the relay working state.

1. 2. 1. 16 Get ID Buffer

Reading ID data command frame.

Length	Command Code	Command Data	Command Data	Checksum
0x04	0x3C	Operation Type	Count	cc

- Operation Type stands for method of operation , 02 stands for reading data of tag.
- Count stands for expect number of identified tag.

After receiving this command, the reader will return the command response frame. The format of response frame is as below,

Length	Response Code	Response Data	Response Data	Response Data	Response Data	Checksum
k*n+5	0x3C	Operation Type	Count n	More Id	ID Data k*n Bytes	cc

- Operation Type is the method of operation, 01 means reading the data of tag. Count stands for the number of IDs in the response frame.
- More Ids means whether tag data is available or not, if the value is "1", that means ID data is available. "0" means no tag data.
- ID Data is the data of tag, it is k*n bytes in total. "N" stands for tag count, "K" stands for every tag's bytes. "K" will be different in according to different tag type. The first byte of "K" is the type of tag. The second (K-2) bytes stands for tag ID. Both k-1 and k bytes stands for tag state. Different types of tags, the definition will be different.

1. 2. 1. 17 Master Acknowledge

Master acknowledge of ID data command frame.

Length	Command Code	Checksum
2	0x80	cc

After receiving this command, the reader will delete the ID data that is sent by the reader last time.

No response frame returns from this command.

1. 2. 2 Tag basic operation of the communication procotol

Tag basic operation communication protocol is valid for all tags of NFC serials, which including regulating management tag and configuring the operating function of tag.

1. 2. 2. 1 Set Tag Parameter

Set tag parameter command frame.

Length	Command Code	Command Data	Command Data	Checksum
11	0x23	ID 4	Parameter 5	cc

- ID is the four byte of specified tag, if the coding is 0xFFFFFFF or 0x00000000, it will be arbitrary tag.
- Parameter stands for tag working parameter. The first byte is tag transmission interval; the second byte is tag power; the third to five bytes means reverve.

After receiving this command, reader will setup parameter for specified tag. If it is successful, it will return response frame; If it is failed, reader will return command completing frame. The format of response frame is as below:

Length	Response Code	Response Data	Response Data	Checksum

7	0x23	ID 4	Status	cc

- ID stands for the ID of specified tag.
- Status stands for the operation result of the specified tag.

1．2．2．2 Get Tag Parameter

Reading tag parameter command frame.

Length	Command Code	Command Data	Checksum
6	0x22	ID 4	cc

- ID is the four byte of specified tag, if it is 0xFFFFFFF or 0x00000000, it will be arbitrary tag.

After receiving this command, reader will read parameter for specified tag. Normally, the response frame will be returned, if the parameter is correctly read. Otherwise, command completing frame will be returned.

Length	Response Code	Response Data	Response Data	Response Data	Response Data	Checksum
15	0x22	ID 4	Status	Parameter 5	Product 4	cc

- ID stands for the ID of specified tag.
- Status stands for the operation result of specified tag.
- Parameter stands for the parameter of tag.
- Product stands for relevant information of tag.

1．2．3 Communication protocol for reading and writing tag

Communication protocol for reading and writing tag is only valid for read & write type tag, which regulates data communication format for reading and writing tag operation.

1．2．3．1 Set Tag Password

Set tag password command frame.

There is colsely relation between tag password and user area, the area of reading and writing needs tag password.

Length	Command Code	Command Data	Command Data	Checksum
10	0x2D	ID 4	Password 4	cc

- ID stands for the four byte of specified tag. If the coding is 0xFFFFFFFF or 0x00000000, the ID is random tag.
- Password stands for 4 bytes password needs to be set.

If the tag password was setted successfully by reader, the reader will return response frame , otherwise, will return command completing frame. The format of response frame is as below table,

Length	Response Code	Response Data	Response Data	Checksum
7	0x2D	ID 4	Status	cc

- ID stands for the ID of tag..
- Status is the executing result.

1．2．3．2 Enter Tag Password

Entering tag password command frame into reader.

Length	Command code	Command Data	Checksum
6	0x26	Password 4	cc

- Password stands for the input tag password. The password will be stored in the reader and you should enter the password again when the read in reset case or power off.

1．2．3．3 Read Tag User

Reading user data command frame of random tag.

Length	Command code	Command Data	Command Data	Command Data	Checksum
5	0x2A	Length	AddrH	AddrL	cc

- Length is the number of data needs to be read.
- AddrH is the high byte of data address needs to be read.
- AddrL is the low byte of data address needs to be read.

The response frame will be returned, if the tag data is successfully read. Otherwise, command completing frame will be returned. The format of response command is as below table:

Length	Response Code	Response Data	Response Data	Response Data	Response Data	Response Data	Checksum
9+n	0x2A	ID 4	Length	AddrH	AddrL	Data n	cc

- ID is the ID code of tag.
- Length is the length of data has been read.
- The high byte of data address has been read.
- The low byte of data address has been read.
- Data is the data of tag has been read.

1．2．3．4 Read Tag User With ID

Reading user data command frame of appointed tag.

Length	Command code	Command Data	Command Data	Command Data	Command Data	Checksum
9	0x29	ID 4	Length	AddrH	AddrL	cc

- ID is the tag code needs to be read.
- Length is the number of data needs to be read.

- AddrH is the high byte of data address needs to be read.
- AddrL is the low byte of data address needs to be read.

The response frame will be returned, if the tag data is successfully read. Otherwise, command completing frame will be returned. The format of response command is as below table:

Length	Response Code	Response Data	Response Data	Response Data	Response Data	Response Data	Checksum
9+n	0x29	ID 4	Length	AddrH	AddrL	Data n	cc

- ID is the ID code of tag.
- Length is the length of data has been read.
- AddrH is the high byte of data address has been read.
- AddrL is the low byte of data address has been read.
- Data is the data of tag has been read.

1．2．3．5 Write Tag User

Wring user data command frame of random tag..

Length	Command code	Command Data	Command Data	Command Data	Command Data	Checksum
5+n	0x27	Length	AddrH	AddrL	Data n	cc

- Length is the number of data needs to be written.
- AddrH is the high byte of data address needs to be written.
- AddrL is the low byte of data address needs to be written.
- Data is the data connent needs to be written.

The response frame will be returned, if the tag data is successfully written. Otherwise, command completing frame will be returned. The format of response command is as below table,

Length	Response Code	Response Data	Response Data	Checksum
7	0x27	ID	Status	cc

- ID is the ID code of tag.
- Status is the status of writing tag.

1．2．3．6 Write Tag User With ID

Writing user data command frame of appointed tag.

Length	Command code	Command Data	Command Data	Command Data	Command Data	Checksum
9	0x28	ID 4	Length	AddrH	AddrL	cc

- ID is the coding of tag needs to be written.
- Length is the number of data needs to be written.
- AddrH is the high byte of data address needs to be written.
- AddrL is the low byte of data address needs to be written.

The response frame will be returned, if the tag data is successfully written. Otherwise, command completing frame will be returned. The format of response command is as below table,

Length	Command code	Response Data	Response Data	Checksum
7	0x28	ID	Status	cc

- ID is the ID code of tag.
- Status is the status of writing tag.