CNS-RFID-01/1S

RFID Sensor

Instruction Manual（communication）

*Thankyou for using our products

*This manual explains how to use the product and safety matters.

* Read this manual thoroughly and pay attention to safety during use.

* Keep this manual in a suitable place for easy reference at anytime.

Guangdong Hinson Technology Co.Ltd.

Contents

Applicable version statement

Version	Increase or decrease information
V1.2	Change the description of RS485 wiring part

Safety attention

Please be sure to follow the precautions and major safety-related shown here.

Warning Violation of the content requirements shown in this warning during operation may result in death or serious injury.

Note Violation of the content requirements shown in this precaution during operation may result in personal injury or property damage.

Remind In order to enable you to use the product correctly, the relevant use items in the main text record the matters that the user must comply with.

1 SAFETY

1.1 SAFETY WARNINGS

The precautions suggested here are intended to enable you to use the product safely and correctly, so as not to cause harm and damage to you and others. Please fully understand its content before using this product.

Note

Do not use this product near explosive gas, flammable gas, corrosive, water-prone environment and combustible materials, otherwise it may cause fire or injury.

Setup, connection, operation, inspection and fault diagnosis should be carried out by appropriately qualified person, otherwise it may cause fire, injury or product damage.

Setting

Please install the sensor in the machine frame, otherwise the equipment may be damaged.

Connecting

The power input voltage must be controlled within the rated range, otherwise it may cause a fire.

Please connect according to the connection diagram, otherwise it may cause a fire.

Do not forcibly bend, pull or clamp the cable, otherwise it may cause a fire.

Please use the cable according to the specified size, otherwise it may cause a fire.

Maintenance and inspection

Maintenance and inspection must be performed after turning off the power, otherwise it may cause injury.

When conducting insulation resistance measurement and insulation withstand voltage test, please do not touch, otherwise it may cause electric shock.

Repair and disassembly

Do not disassemble or modify the sensor, otherwise it may cause injury or damage to the device. For internal inspection or repair, please contact our company.

2 FOREWORD

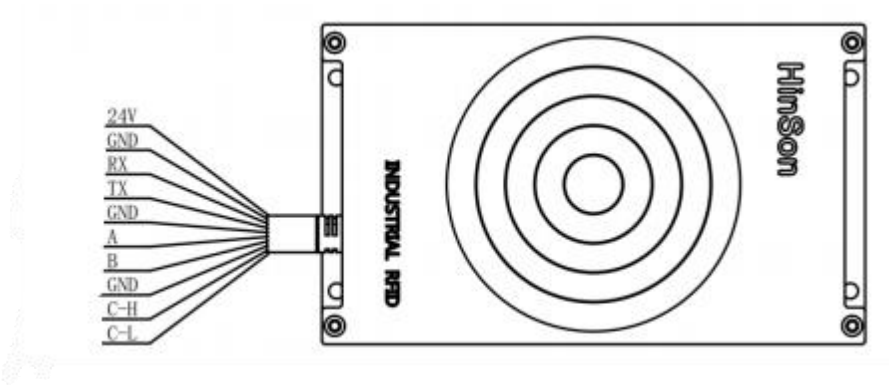
CNS-RFID-01/1S allows reading and writing operations through a variety of communication methods. This article will explain the communication methods in detail.

2.1 PRODUCT COMPOSITION

Model	Power input
CNS-RFID-01/1S	DC 24V

Please check if the model is the same

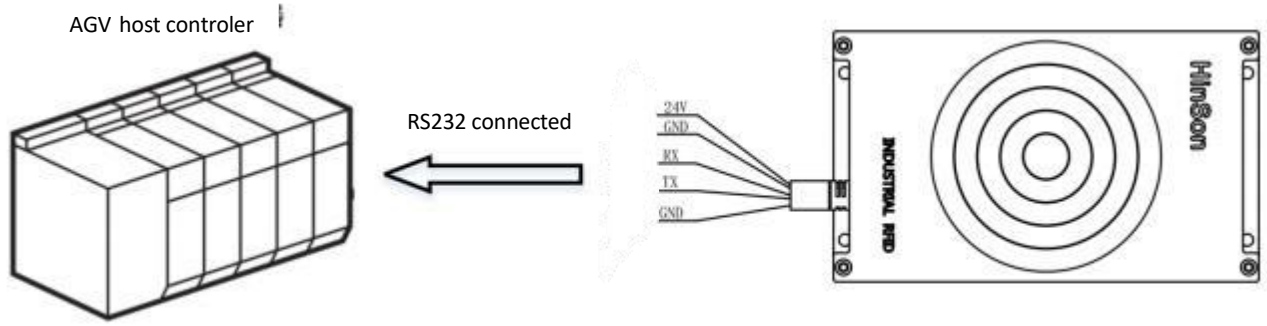
2.2 WIRE DEFINITION



3 RS-232 COMMUNICATION CONNECTION

3.1 CONNECTION

The host computer and the sensor are connected as follows.



3.2 COMMUNICATION SETTINGS

Use the RS232 communication HS protocol, after determining the protocol to be used, you need to set the CNS-RFID-01/1S before using it. Configure the parameters through the Hinson configuration software on the computer. For specific configuration connections, see <CNS-RFID-01/1S Usage>. The configuration parameters are as follows:

Parameter name	Parameter	Default parameters
Device interface and protocol	1：RS232-HS protocol 2：RS485-HS protocol 3：CAN Bus-HS protocol 4：RS485-Modbus protocol	RS232-HS protocol
Device address	1-127	127
RS232 communication baud rate	1：19200bps 2：115200bps	115200bps
RS232 reading mode	1： Query mode 2： Card reader trigger mode 3： Timed broadcast mode	Query mode
RS232 card reader trigger frame number	1：1 frame 2：2 frame 3：3 frame 4：4 frame 5： Continuous sending	1 frame
RS232 broadcast interval	1：5ms 2：10ms 3：20ms 4：50ms 5：100ms	5ms

3.3 COMMUNICATE WITH HS PROTOCOL

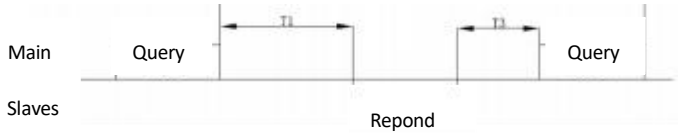
3.3.1 Communication specifications

Parameter	Parameter information	Default setting
Way of communication	Point to point	
Accept/send method	Full duplex communication mode	
Broadcast mode	5ms，10ms，20ms，50ms，100ms	Not broadcast
Communication ID	1 - 127	127
Communication rate	19200bps，115200bps	115200bps
Data bit	8 bit	8 bit
Check bit	No verification	No verification
Stop bit	1 bit	1 bit

3.3.2 Master-Slave Communication Sequence

Query mode

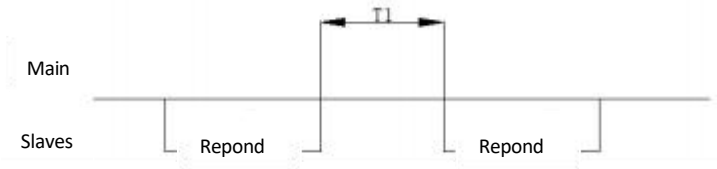
The master stationsends an inquiry to one slave station, and the slave station performs processing and responds.



Serial number	Name	Content
T1	Response waiting interval	Within 1ms
T3	Send waiting time	Recommended 5ms -30ms

Broadcast mode

The slave station automatically broadcasts according to the set time interval



Serial number	Name	Content
T1	Broadcast interval	Configure in Hinson configuration software

3.3.3 Communication protocol

The host control can read card data and write card data. The communication protocol includes two parts. The two operating protocols are described in detail below

.Read card data protocol

RFID-01 sensor return data mode includes inquiry mode, card reading trigger mode, and timed broadcast mode.

Query mode：After the RFID sensor receives the data from the host controler, it returns the data

Card reader trigger mode：The RFID sensor actively sends data after reading the card information

Timed broadcast mode：RFID sensor automatically sends data according to the set time interval

The master asks for data

Inquiry about the data format of the card reader

Flag	1Byte
	1Byte
	1Byte
	1Byte
	1Byte
Communication flag	1Byte
Check code	1Byte（Low）
	1Byte（High）

●Flag（5Byte） 0x52 0x43 0x6f 0x64 0x65

●Communication flag（1Byte）

RS232 free protocol mode: invalid data 0x00

●Check code（2Byte） 0x3F 0xFD

Return data from the station

The RFID sensor is in inquiry mode, card reading trigger mode, and timed broadcast mode, and the returned data grid is consistent.Response data format of slave sensor

Flag	1Byte
	1Byte
	1Byte
	1Byte
	1Byte
Communication flag	1Byte
Card reading status	1Byte
Card signal strength	1Byte
Card data	1Byte
	1Byte
	1Byte
	1Byte
	1Byte
	1Byte
	1Byte
	1Byte
Check code	1Byte（Low）
	1Byte（High）

●Flag（5Byte）

0x52 0x43 0x6f 0x64 0x65

●Communication flag（1Byte）

RS232-HS protocol mode: invalid data 0x00;

●Card reading status（1Byte）

0x00：RFID sensor is not card-reading status;

0x01：The RFID sensor is reading the card status;

●Card signal strength（1Byte）

0x00-0x07：Read the card signal strength, 0x00 signal strength is the weakest, 0x07 signal strength is the strongest;

●Card data（8Byte）

The RFID sensor will automatically record and save the data of the most recent card reading, so that the host computer can determine the landmark at anytime;

When the read data length is set to 4Byte: the first 4Bytes are valid data in the card, and the last 4bytes are invalid data 0x00;

When the read data length is set to 8Byte: all 8Byte data is valid;

●Check code（2Byte）

The result of the operation of CRC16. For details, please see the checksum calculation formula.

.Write card data protocol

Flag	1Byte
	1Byte
	1Byte
	1Byte
	1Byte
Communication flag	1Byte
Data input	1Byte
	1Byte
	1Byte
	1Byte
	1Byte
	1Byte
	1Byte
	1Byte
Check code	1Byte（Low）
	1Byte（High）

●Flag（5Byte）

0x57 0x43 0x6f 0x64 0x65

●Communication flag（1Byte）

RS232 free protocol mode: invalid data 0x00;

●Card data（8Byte）

When the read data length is set to 4Byte: the first 4Bytes are valid data in the card, and the last 4bytes are invalid data 0x00;

When the read data length is set to 8Byte: all 8Byte data is valid;

●Check code（2Byte）

The result of the operation of CRC16. For details, please see the checksum calculation formula.

Return data from the station

Flag	1Byte
	1Byte
	1Byte
	1Byte
	1Byte
Communication flag	1Byte
Write status	1Byte
Check code	1Byte（Low）
	1Byte（High）

●Flag（5Byte）

0x57 0x43 0x6f 0x64 0x65

●Communication flag（1Byte）

RS232 free protocol mode: invalid data 0x00;

●Write status（1Byte）

0x00：Write successfully;

0x01：Write error or the card is locked inside;

0x02：No card that can be written is detected;

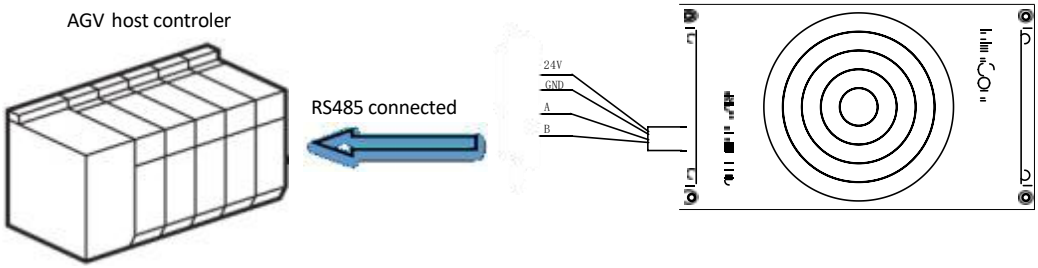
●Check code（2Byte）

The result of CRC16 operation. For details, please see the checksum calculation formula.

4 RS-485 COMMUNICATION CONNECTION

4.1 CONNECTION

Use the cable to connect the host computer and the sensor as follows



4.2 COMMUNICATION SETTINGS

The RS485 communication is divided into two protocols, namely the moudbus protocol and the HS protocol. After determining the protocol to be used, you need to set the CNS-RFID-01/1S before using it.

Since it is not possible to directly use RS485 to set the parameters of the device, it is necessary to configure the parameters through the Hinson configuration software on the computer side. Please refer to <CNS-RFID-01/1S Usage Part> for specific configuration and connection. The configuration parameters areas follows:

Parameter name	Parameter list	Setting parameters
Device interface and protocol	1：RS232-HS protocol 2：RS485-HS protocol 3：CAN Bus-HS protocol 4：RS485-modbus protocol	RS485-modbus protocol
Device address	1-127	127
RS485 communication baud rate	1：9600bps 2：19200bps 3：38400bps 4：57600bps	115200bps

	5：115200bps	
RS485 parity check	1： No verification 2： Odd parity 3： Even parity	No verification
RS485 Stop bit	1：1bit 2：1.5bit 3：2bit	1 bit

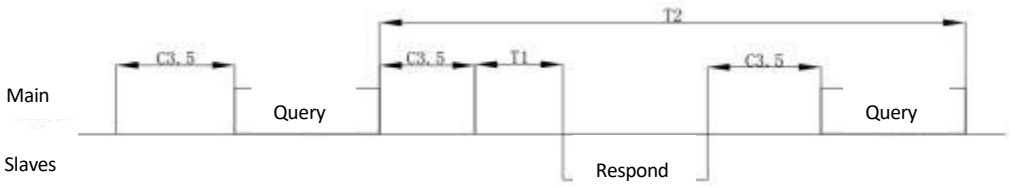
4.3 CONTROLLED BY MOUDBUS PROTOCOL

4.3.1 Communication specifications

	Parameter information	**Default setting**
way of communication	Single master/multi-slave mode	
Operating mode	Modbus RTU mode	RTU mode
Accept/send method	Half-duplex communication mode	
Communication ID	1-127 configurable	127
Communication rate	9600bps，19200bps，38400bps，576000bps，115200bps	115200bps
Data bit	8 bit	8 bit
Check Digit	No verification；Odd parity；Even parity	No verification
Stop bit	1 bit；2 bit	1 bit

4.3.2 Master-Slave Communication Sequence

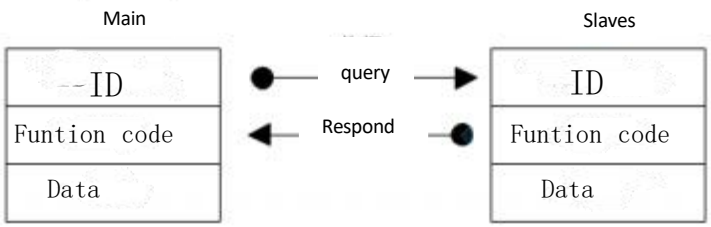
The communication mode of Modbus protocol is single-master station/multi-slave station mode. The master stationsends an inquiry to one slave station, and the slave station performs processing and responds.



Serial number	**Name**	**Content**
C3.5	Quiet interval	As the sending waiting time, please be sure to leave an interval of 3.5 words or more. If the number of words is not full, the sensor cannot respond. When the communication speed exceeds 19200 bps, please keep the interval at least 1.75 ms.
T1	Send waiting time	After receiving the inquiry from the master station, the slave station switches the communication line to the sending state, the time until it starts to reply to the response. In order to send a waiting time of 10 ms. The actual sending waiting time will become the static interval (C3.5) + command processing time + sending waiting time (T1)

4.3.3 Information

Information format



■ **Query information structure**

Slave address code	function code	Data
1 Bye	1 Bye	2Bye

●Slave address

The specified slave address is the address of the slave sensor configured by the configuration software.

●Function code

The function code information length supported by the sensor is as follows.

Function code	**Features**
04h	Read data from the save register
10h	Write multiple save registers

●Data

■ Data related to setting function codes.

■ Response information structure

After receiving the inquiry information from the station, there are three response states, namely, normal response, no response and abnormal response.

The information structure of the response is the same as the information structure of the query.

Slave address code	Function code	Data
1 Bye	1 Bye	2 Bye

●Normal response

After receiving the inquiry from the master station, the slave station will perform the required processing and reply with a response.

4.3.4 Register address

Write multiple registers Write card operation (16)

Register address	**Write value**	**Content**	
2000	0-255	RFID card first byte data	
2001	0-255	RFID card second byte data	
2002	0-255	RFID card 3rd byte data	
2003	0-255	RFID card 4th byte data	
2004	0-255	RFID card 5th byte data	The data can be read only when the read length is set to 8 bytes.
2005	0-255	RFID card 6th byte data	
2006	0-255	RFID card 7th byte data	
2007	0-255	RFID card 8th byte data	

The RFID sensor will automatically record and save the data of the mostrecent card reading so that the host controler can determine the landmark at anytime.

Register address	Read value	Content	
1000	0 - 2	Write status: 0：The data is written successfully; 1：Data writing fails or the card is locked; 2：No writable card is detected;	
1001	0 - 1	Reading status: 0：No card 1：Card reading status;	
1002	0 - 7	Card reading signal strength indicator; 0：The weakest signal; 7：The Strongest signal;	
1003	00-255	RFID card first byte data	
1004	00-255	RFID card second byte data	
1005	00-255	RFID card 3rd byte data	
1006	00-255	RFID card 4th byte data	
1007	00-255	RFID card 5th byte data	When the read length is set to 8 bytes, the data can be read, otherwise the data is 00;
1008	00-255	RFID card 6th byte data	
1009	00-255	RFID card 7th byte data	
1010	00-255	RFID card 8th byte data	

4.4 COMMUNICATION WITH HS PROTOCOL

4.4.1 Communication specifications

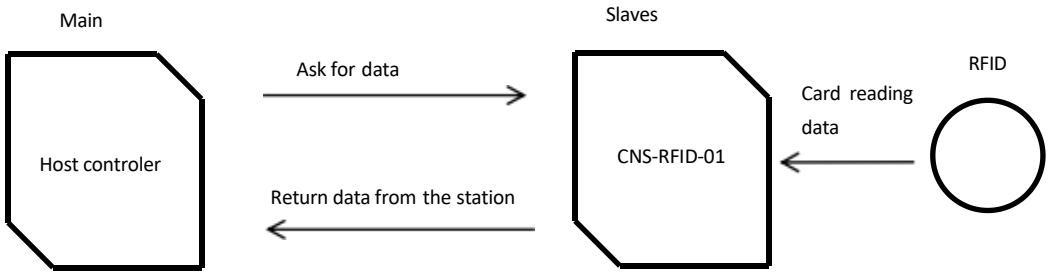
	Parameter information	Default setting
Communication way	Single master/multi-slave mode	
Accept/send method	Half-duplex communication mode	
Communication ID	1-127 configurable	127
Communication rate	9600bps， 19200bps， 38400bps， 576000bps，115200bps	115200bps
Data bit	8 bit	8 bit
Check Digit	No verification;Odd parity;Even parity	No verification
Stop bit	1 bit;2 bit	1 bit

4.4.2 Communication protocol

The host controler can read and write card operations on the card. The communication protocol includes two parts, read card data and write card data. The two operating protocols are described in detail below;

.Read card data protocol

Card reading operation data flow



In the RS485 mode, the RFID-1S sensor returns to the data mode only in the Query mode.

Query mode：After the RFID sensor receives the data from the host controler, it returns the data.

The master asks for data

Inquiry about the data format of the card reader

Flag	1Byte
	1Byte
	1Byte
	1Byte
	1Byte
Communication flag	1Byte
Check code	1Byte（Low）
	1Byte（High）

●Flag（5Byte）

0x52 0x43 0x6f 0x64 0x65

●Communication flag（1Byte）

Slave station RFID sensor address, the range is 0x01-0x7F;

●Check code（2Byte）

The result of the operation of CRC16. For details, please see the checksum calculation formula.

Return data from the station

RFID sensor returns data in Query mode

Flag	1Byte
	1Byte
	1Byte
	1Byte
	1Byte
Communication flag	1Byte
Card reading status	1Byte
Card signal strength	1Byte
Card data	1Byte
	1Byte

	1Byte
	1Byte
	1Byte
	1Byte
	1Byte
	1Byte
	1Byte
Check code	1Byte（Low）
	1Byte（High）

●Flag（5Byte）

0x52 0x43 0x6f 0x64 0x65

●Communication flag（1Byte）

Slave station RFID sensor address, the range is 0x01-0x7F;

●Card reading status（1Byte）

0x00：RFID sensor is not card-reading status;

0x01：The RFID sensor is reading the card status;

●Card signal strength（1Byte）

0x00-0x07：Read the card signal strength, 0x00 signal strength is the weakest, 0x07 signal strength is the strongest;

●Card data（8Byte）

The RFID sensor will automatically record and save the data of the most recent card reading so that the host controler can determine the landmark at anytime.

When the read data length is set to 4Byte: the first 4Bytes are valid data in the card, and the last 4bytes are invalid data 0x00;

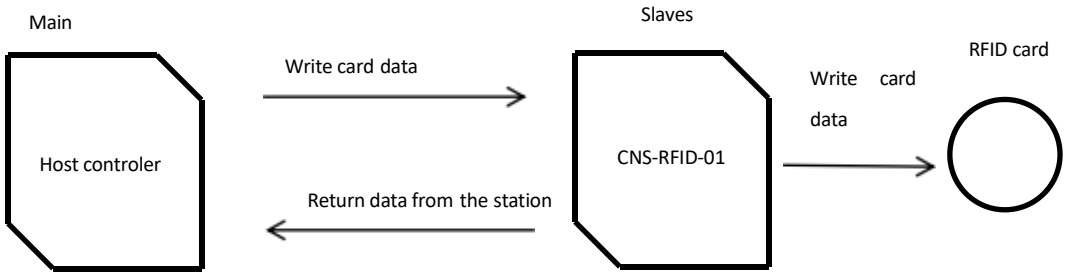
When the read data length is set to 8Byte: all 8Byte data is valid;

●Check code（2Byte）

The result of the operation of CRC16. For details, please see the checksum calculation formula.

.Write card data protocol

Card write operation data flow



Master stationsends data

Write card data format

Flag	1Byte
	1Byte
	1Byte
	1Byte
	1Byte
Communication flag	1Byte
Write card data	1Byte(Card data 1)
	1Byte(Card data 2)
	1Byte(Card data 3)
	1Byte(Card data 4)
	1Byte(Card data 5)
	1Byte(Card data 6)
	1Byte(Card data 7)
	1Byte(Card data 8)
Check code	1Byte（Low）
	1Byte（High）

●Flag bit（5Byte）

0x57 0x43 0x6f 0x64 0x65

●Communication flag（1Byte）

Slave station RFID sensor address, the range is 0x01-0x7F;

●Card data（8Byte）

When the read data length is set to 4Byte: the first 4Bytes are valid data in the card, and the last 4bytes are invalid data 0x00;

When the read data length is set to 8Byte: all 8Byte data is valid;

●Check code（2Byte）

The result of the operation of CRC16. For details, please see the checksum calculation formula.

Return data from the station

Return data from the station	1Byte
	1Byte
	1Byte
	1Byte
	1Byte
Communication flag	1Byte
Write status	1Byte
Check code	1Byte（Low）
	1Byte（High）

●Flag bit（5Byte）

0x57 0x43 0x6f 0x64 0x65

●Communication flag（1Byte）

Slave station RFID sensor address, the range is 0x01-0x7F;

●Write status（1Byte）

0x00：Write successfully;

0x01：Write error or the card is locked inside;

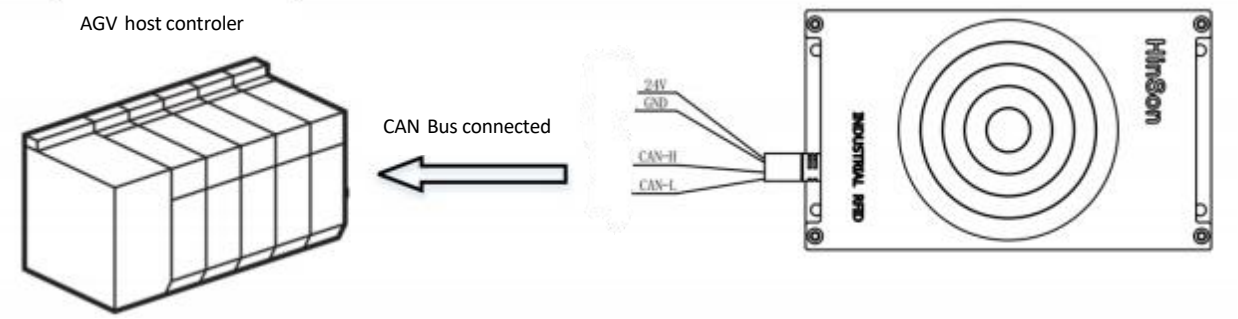
0x02：No card that can be written is detected;

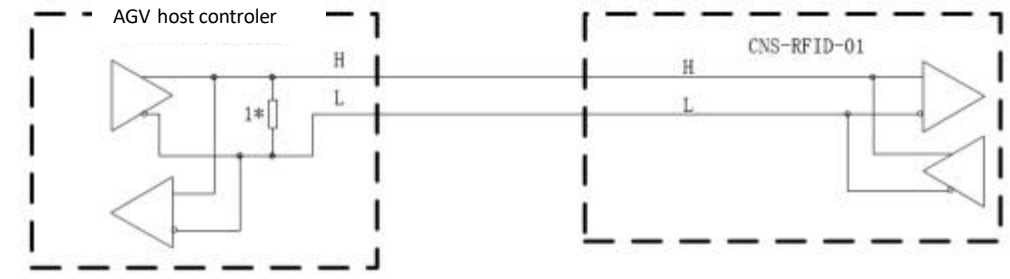
●Check code（2Byte）

The result of the operation of CRC16. For details, please see the checksum calculation formula.

5 CAN BUS COMMUNICATION

5.1 CONNECTION





5.2 COMMUNICATION SETTINGS

The CAN bus uses the HS protocol, and you need to set the CNS-RFID-01/1S before using it. Because it is not possible to directly use the CAN bus to set the parameters of the device, it is necessary to configure the parameters through the Hinson configuration software on the computer side. Please refer to <CNS-RFID-01/1S Usage Part> for specific configuration and connection. The configuration parameters areas follows:

Parameter name	Parameter list	Setting parameters
Device interface and protocol	1：RS232-HS protocol 2：RS485-HS protocol 3：CAN Bus-HS protocol 4：RS485-modbus protocol	CAN Bus-HS protocol
Device address	1-127	127

CAN bus baud rate	1：125K 2：250K 3：500K 4：1000K	1000K
CAN bus read mode	1： Query mode 2： Card reader trigger mode 3： Timed broadcast mode	Query mode
CAN bus card reader trigger frame number	1：1 frame 2：2 frame 3：3 frame 4：4 frame 5： Continuous sending	1 frame
CAN bus broadcast interval	1：5ms 2：10ms 3：20ms 4：50ms 5：100ms	5ms

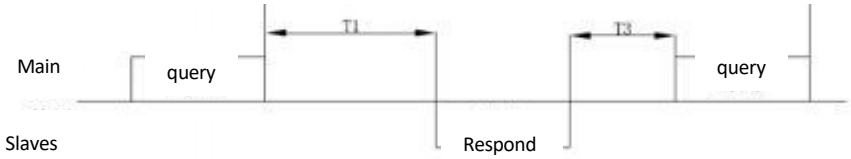
5.3 OMMUNICATION SPECIFICATIONS

Features	**Parameter**	**Default parameters**
Communication specifications	CAN BUS 2.0A	
Frame ID	1-127 configurable	127
Communication rate	Can choose from 125 Kbps; 250Kbps; 500Kbps; 1000Kbps	1000Kbps
Frame type	Standard frame	
Frame format	Data Frame	
Broadcast mode	Software configuration	

5.3.1 Master-Slave Communication Sequence

Query mode

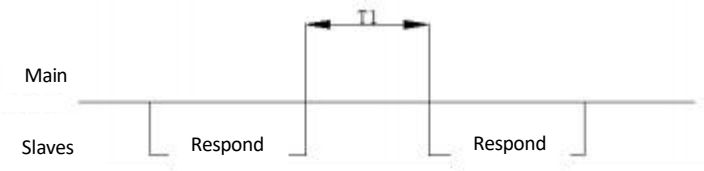
The master station sends an inquiry to one slave station, and the slave station performs processing and responds.



Serial number	**Name**	**Content**
T1	Response waiting interval	Within 1ms
T3	Send waiting time	Recommended 5ms -30ms

Broadcast mode

The slave station automatically broadcasts according to the set time interval



Serial number	Name	Content
T1	Broadcast interval	Configure in Hinson configuration software

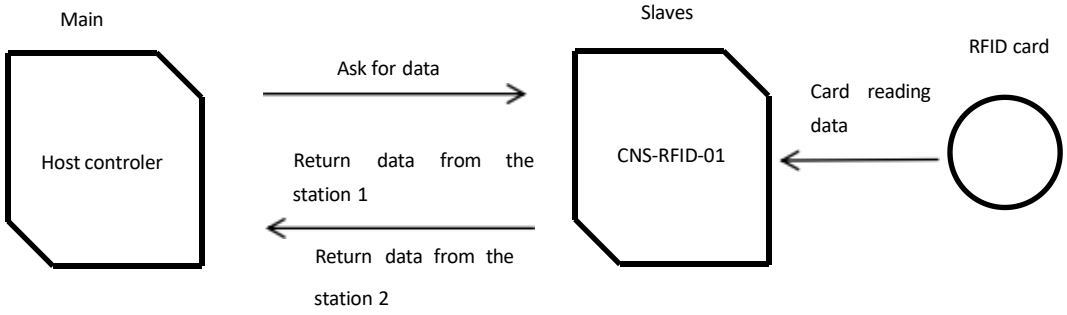
5.4 INFORMATION

5.4.1 The host controler can read and write card operations on the card. The communication protocol includes two parts, read card data and write card data. The two operating protocols are described in detail below;

5.4.2 Data protocol

The next return data in CAN bus mode is divided into two frames of data return.

Card reading operation data flow



RFID-01 sensor return data mode includes query mode, card reading trigger mode, and timed broadcast mode.

Query mode：After the RFID sensor receives the data from the host controler, it returns the data

Card reading trigger mode：The RFID sensor actively sends data after reading the card information

Timed broadcast mode：RFID sensor automatically sends data according to the set time interval

Reading card data frame

The query data can read card data and write data to the card, and realize the card reading and writing functions by sending two kinds of data to the slave RFID sensor.

Can ID	DLC	Data						
		0 Byte	1 Byte	2 Byte	3 Byte	4 Byte	5 Byte	6 Byte
Sensor setting address	7	Data						

- Data（1-7 Byte）

Card reading mode: send any data with a data length of 1-7Byte;

Write card data frame

The query data can read card data and write data to the card, and realize the card reading and writing functions by sending two kinds of data to the slave RFID sensor.

Can ID	DLC	Data							
		0 Byte	1 Byte	2 Byte	3 Byte	4 Byte	5 Byte	6 Byte	7 Byte
Sensor setting address	8	Data							

- Data（1-8 Byte）

  Write card mode: send data length 8Byte;

Card data 1 (1Byte)	Card data 2 (1Byte)	Card data 3 (1Byte)	Card data 4 (1Byte)	Card data 5 (1Byte)	Card data 6 (1Byte)	Card data 7 (1Byte)	Card data 8 (1Byte)

Return data frame

The RFID sensor will automatically record and save the data of the mostrecent card reading so that the host controler can determine the landmark at anytime.

The first frame of data

Can ID	DLC	Data							
		0 Byte	1 Byte	2 Byte	3 Byte	4 Byte	5 Byte	6 Byte	7 Byte
Sensor setting address	8	Data number	Card reading status	Card reading status	Card signal strength	Card data 1	Card data 2	Card data 3	Card data 4

Data number (1Byte)	Write status (1Byte)	Read status(1Byte)	Signal strength(1Byte)	Card data 1 (1Byte)	Card data 2 (1Byte)	Card data 3 (1Byte)	Card data 4 (1Byte)

- Data identification（1Byte）

  0x01：The first frame of data identification;

- rite status（1Byte）

  0x00：Write successfully;

  0x01：Write error or the card is locked inside;

  0x02：No card that can be written is detected;

- Read status（1Byte）

  0x00：RFID sensor is not card-reading status;

  0x01：The RFID sensor is reading the card status;

- Card signal strength（1Byte）

  0x00-0x07：Read the card signal strength, 0x00 signal strength is the weakest, 0x07 signal strength is the strongest;

- Card data 1（1Byte）;

- The first byte of data in the card;

Card data 2 (1Byte);

- The 2nd byte data in the card;
- Card data 3 (1Byte);

The 3rd byte data in the card;

- Card data 4 (1Byte);

The 4th byte data in the card;

The second frame of data

Can ID	DLC	Data							
		0 Byte	1 Byte	2 Byte	3 Byte	4 Byte	5 Byte	6 Byte	7 Byte
Sensor setting address	8	Data number	Write card status	Card reading status	Card signal strength	Card data 5	Card data 6	Card data 7	Card data 8

Data identification (1Byte)	Write status(1Byte)	Read status(1Byte)	Signal strength (1Byte)	Card data 5 (1Byte)	Card data 6 (1Byte)	Card data 7 (1Byte)	Card data 8 (1Byte)

- Data identification（1Byte）

0x02：The second frame of data identification;

- Write status（1Byte）

0x00：Write successfully;

0x01：Write error or the card is locked inside;

0x02：No card that can be written is detected;

- Read status（1Byte）

0x00：RFID sensor is not card-reading status;

0x01：The RFID sensor is reading the card status;

- Card signal strength（1Byte）

0x00-0x07：Read the card signal strength, 0x00 signal strength is the weakest, 0x07 signal strength is the strongest;

Card data 5 (1Byte);

The 5th byte data in the card;

- Card data 6 (1Byte);

The 6th byte data in the card;

- Card data 7 (1Byte);

The 7th byte data in the card;

- Card data 8 (1Byte);

The 8th byte data in the card;

6 AFTER-SALES AND TECHNICAL SUPPORT

6.1 WARRANTY PERIOD

CNS-RFID-01/1S provides a limited time warranty. If the product cannot be used normally due to quality problems, design defects and other reasons, we will carryout after-sales maintenance for free during the warranty period.

. Warranty period: 2 years from sale.

6.2 WARRANTY SCOPE

If the product is within the scope of the warranty during the warranty period, we will repair or replace it free of charge

- This product's warranty and after-sales service are only limited to mainland China;
- The product cannot be used normally when it is out of the box due to transportation;
- Failure to work normally caused by damage to the product's own components;
- Product design defects cannot be used normally;

6.3 EXEMPTION SCOPE

Please pay attention to the following conditions during the use of the product, we will not provide free after-sales and warranty.

. Failure to install the product according to the instructions correctly, causing damage to the product;
. Use this product under unsuitable environments and conditions, causing product damage;
. Damage to the product due to non-compliance with the product specification;
. Disassemble or repair the product without the permission of the company;
. Product damage caused by irresistible external forces such as natural disasters, fires, etc;

6.4 TECHNICAL SUPPORT

Guangdong Hinson Technology Co. Ltd. website：www.hinson-xs.com

Technical Support Wechat：13928672909
WhatApps: +86 13928672909

.Appendix I:

C language CRC check function

cBuffer：Calculate the array of CRC check codes.

iBufLen：The length of the array.

```
unsigned int CRC_Verify(unsigned char *cBuffer, unsigned int iBufLen)
{
    unsigned inti, j;                    //#define wPolynom 0xA001
    unsigned intwCrc = 0xffff;
    unsigned int wPolynom = 0xA001;
/*------------------------------------------------------------------------------*/
    for (i = 0; i < iBufLen; i++)
    {
        wCrc ^= cBuffer[i];
for (j = 0; j < 8; j++)
        {
            if (wCrc &0x0001)
            {   wCrc = (wCrc >> 1) ^ wPolynom;   }
            else
            {   wCrc = wCrc >> 1;   }
         }
     }
return wCrc;
}
```

PLC write CRC check function

The CRC-16 code is composed of two bytes. At the beginning, each bit of the CRC register is preset to 1 (0xffff), and then the CRC register is XORed with the 8-bit data, and then the CRC register is changed from high to Shift low, add zero at the position of the most significant bit (MSB), and the least significant bit (LSB), which has been moved out of the CRC register after shifting) If it is 1, put the register with the predefined polynomial code (16#A001) XOR is performed, otherwise if LSB is zero, XOR is not required. Repeat the above shift from high to low 8 times, the first 8-bit data is processed, use the value of the CRC register at this time and the next 8-bit data to XOR and perform 8 shifts like the previous data Bit. After all characters are processed, the value in the CRC register is the final CRC value.

he following is the calculation process of CRC:

Setup the CRC register and assign FFFF(hex) to it.

XOR the first 8-bit character of the data with the lower 8 bits of the 16-bit CRC register, and store the result in the CRC register.

The CRC register is shifted one bit to the right, the MSB is zeroed, and the LSB is shifted out and checked.

If the LSB is 0, repeat the third step; if the LSB is 1, the CRC register is XORed with the polynomial code.

Repeat steps 3 and 4 until all 8 shifts are completed. At this point, an 8-bit data has been processed.

Repeat steps 2 to 5 until all data is processed.

The content of the final CRC register is the CRC value.

Input parameters:

Pointer of the data area to be verified, the first byte is the data length

```
LD0          DataBuff          IN          DWORD
Network 1
 LD          SM0.0
 MOVW        16#FFFF, AC0                  // Initialize the CRC register
 BTI         *LD0, LW4                     // The first byte of the data buffer is the data length
 MOVD        LD0, LD6
 INCD        LD6                           // Pointer to the first byte to be processed
 Network 2
 LD          SM0.0
 FOR         AC2, +1, LW4                  // Start looping through each byte
 Network 3
 LD          SM0.0
 XORB        *LD6, AC0                     // The byte is first XORed with the low bit of the CRC register
 Network 4
 LD          SM0.0
 FOR         AC1, +1, +8                   // Shift processing loop, processing 8 bits of a byte
 Network 5
 LD          SM0.0
 SRW         AC0, 1                        // CRC register shifted one bit to the right
 Network 6
 LD          SM1.1                         // If the shift out bit is 0, then enter the next cycle
 XORW        16#A001, AC0                  // If the shifted out bit is 1, the CRC register is XORed with
polynomial 16#A001
 Network 7
 NEXT
 Network 8
 LD          SM0.0
 INCD        LD6                           // Pointer plus 1 points to the next byte
 Network 9
 NEXT
 Network 10
 LD          SM0.0
 SWAP        AC0                           // Exchange the high and low bytes of the CRC register
 MOVW        AC0, *LD6                     // CRC check value is written to the end of the data area
```

Remarks: After the PLC writes the CRC check function, use it to calculate the CRC check code, compare the check code with the CRC check code calculated by the SinloCRC16 check tool, if they are not the same, the CRC check written by the PLC The test function must be incorrect.