科创仪表局

KC9532 1MHz…4GHz

Quad-channel Synchronous Sampling Power Meter

Communication Protocol

Version V1.1

科新社

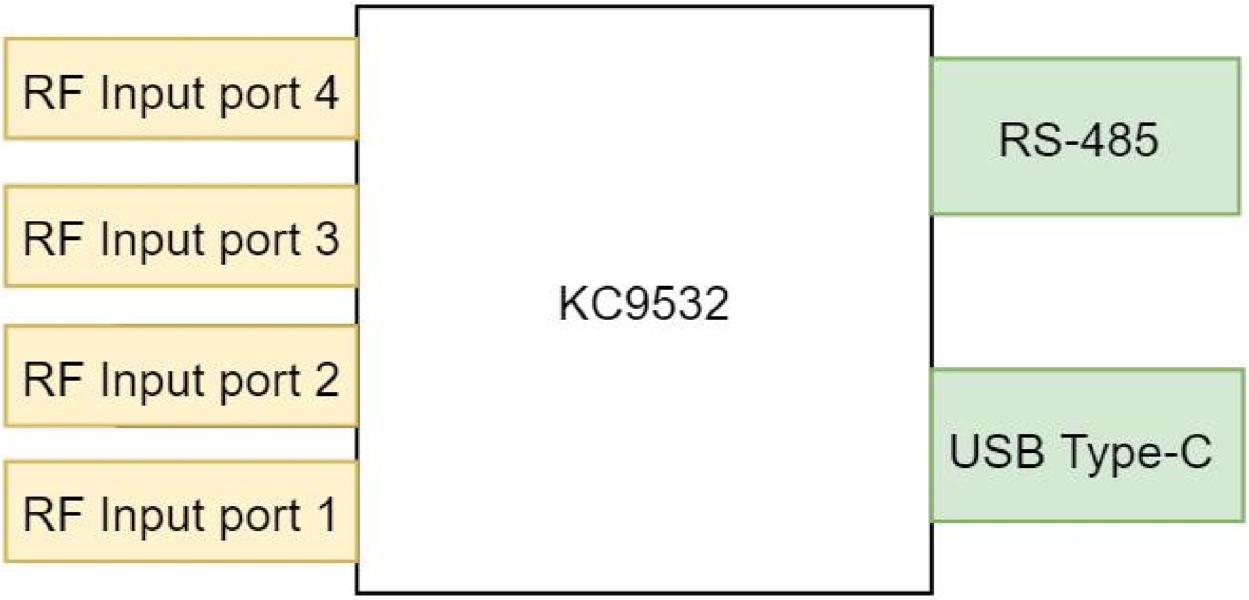
二〇二二年四月

目录

1 Overview

1.1 Ports

Pic 1-1 shows the ports' logic of KC9532.



Pic 1-1

KC9532 comes with a RS-485 port and an USB Type-C port. (Abbreviated as 485 and USB)

The 485 port utilises Modbus-RTU protocol to communicate with the host computer. KC9532 plays the role of the slave machine waiting for commands from the host before matching the address and returning the corresponding data. The adjustable Baud rate range of the 485 port is 9600-460800, and the default is 115200.

USB port is mainly used to acquire system information, connecting the host computer and remote upgrading. Since the communication address and the Baud rate of 485 port is adjustable, the Baud rate of USB port is fixed to 115200 to acquire the information like the adjusted address as well as the new Baud rate.

1.2 Protocol Format

KC9532's 485 port obeys standard Modbus-RTU protocol format, as shown in Pic 1-2.

1 Byte	1 Byte	0~252 Bytes	2 Bytes
Address domain	Function domain	Data domain	CRC check

Pic 1-2

1.2.1 Address Domain

Address domain is mainly used by the host computer to select equipment. The default address of KC9532 is 0x01.

1.2.2 Function Domain

Function domain is mainly used for those specific functions of the equipment. The list below shows the function domains supported by KC9532.

Code (Hexadecimal)	Function	Description
0x03	Read holding register	Acquire option values
0x04	Read input register	Acquire measured values
0x06	Write single register	Configure a certain setting

List 1-1 Function domains supported by KC9532

When an unsupported function code is sent, KC9532 sets the highest bit of function code to 1 and sets 0x01 in the data domain, to represent an error.

For example, the host computer sends 01 01 00 00 00 08 3D CC , yet KC9532 doesn't support this function, so 01 81 01 81 90 will be returned.

1.2.3 Data Domain

Data domain comprises of option address and option content, as shown in Pic 1-3.

2 Bytes	0~250 Bytes
Option address	Option data

Pic 1-3

Currently, all the option data the option address (register address) correspond to are multiple of 2 Bytes.

Whenever the address sent by the user is mistaken, KC9532 sets the highest bit of function domain to be 1, and returns 0x02 to represent an address error.

For example, the host computer sends 01 04 01 0A 00 02 50 35, yet KC9532 cannot find 0x010A data address in input register, in this case it returns 01 84 02 C2 C1.

When the user sends a mistaken option data, KC9532 will set the highest bit of the function domain to be 1 and will return 0x03 to represent a parameter error.

For example, the host computer sends 01 04 01 01 00 01 61 F6 , yet KC9532 requires a minimum amount of register requested to be 2. So it returns 01 84 03 03 01 .

1.2.4 Big Endian or Small Endian

KC9532 adopts big-endian mode to return data. Data 0x1234 would be returned as 0x12, 0x34.

2 Protocol Format Details

2.1 Acquire Current Settings

Every time KC9532 is booted, it returns the information about the equipment through USB. User can acquire it with normal serial port software.

To acquire system info, connect USB port with serial port software and set parameters as below.

Baud rate: 115200

Stop bit: 1

Data bit: 8

Parity bit: None

KC9532 return the info as below after connected to power:

==================================

product: KC9532

Version:1.3

Address:0x1

RS485 baud rate:115200

==================================

Product name, software version, address and 485 port's baud rate are returned, and user can connect 485 port precisely with this info.

2.2 Acquire the Measured Values

Each channel of KC9532 returns data as it's shown below.

Data	Description	Unit	Data Type
Peak value	Max power within a unit sampling time	dBm/mW	Single-precision floating point
Average Value	Average power within a unit sampling time	dBm/mW	Single-precision floating point
Mean square root value	Effective power within a unit sampling time	dBm/mW	Single-precision floating point
Peak-to-average ratio	The ratio of peak value to mean square root value within a unit sampling time	/	Single-precision floating point
Pulse width	The duration time of high signal within a single pulse period	us	Single-precision floating point
Duty ratio	The ratio of high signal duration time to period time within a single pulse period	%	Single-precision floating point
Repeat cycle	The duration time of a single pulse period	us	Single-precision floating point

List 2-1 Measured Data Types

To acquire measured data in the channel, 0x04 function domain (read input register) is uniformly adopted. Note that a specific address is bound to each data value in each channel. Below describes the detail of acquiring the data in channel 1, and the method of acquiring other channels' data resembles this one.

The default unit for peak value, average value and mean square root value is dBm, to change unit please refer to chapter 2.3.3.

2.2.1 Command Format for Reading Input Register

According to standard Modbus-RTU protocol format, the command format of reading input register is shown below.

Data domain

1 Byte	1 Byte	2 Bytes	2 Bytes	2 Bytes
Address domain	Function domain	Register address	Request size of data	CRC check

Pic 2-1 Request Format of Host Computer

Data domain

1 Byte	1 Byte	1 Byte	0~251 Bytes	2 Bytes
Address domain	Function domain	Return size of data	Data contents	CRC check

Pic 2-2 Response Format

Note: The size of request data from the host computer refers to the amount of 2-Byte data requested. A request size value of 2 represents the host computer will get a 4-Byte return.

A single measured data in KC9532 would be stored as single-precision floating point, whose size is 4 Byte. **For this reason, the user must specify the request data size to be 2,**otherwise a warning for parameter error would be returned.

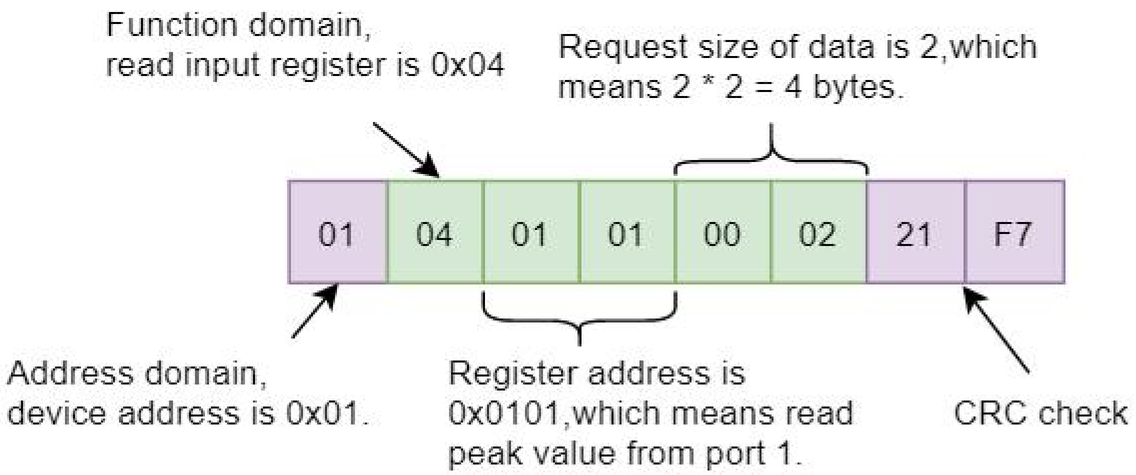
2.2.2 Acquire Measured Data in Channel 1

The addresses of data registers of channel 1 are shown below.

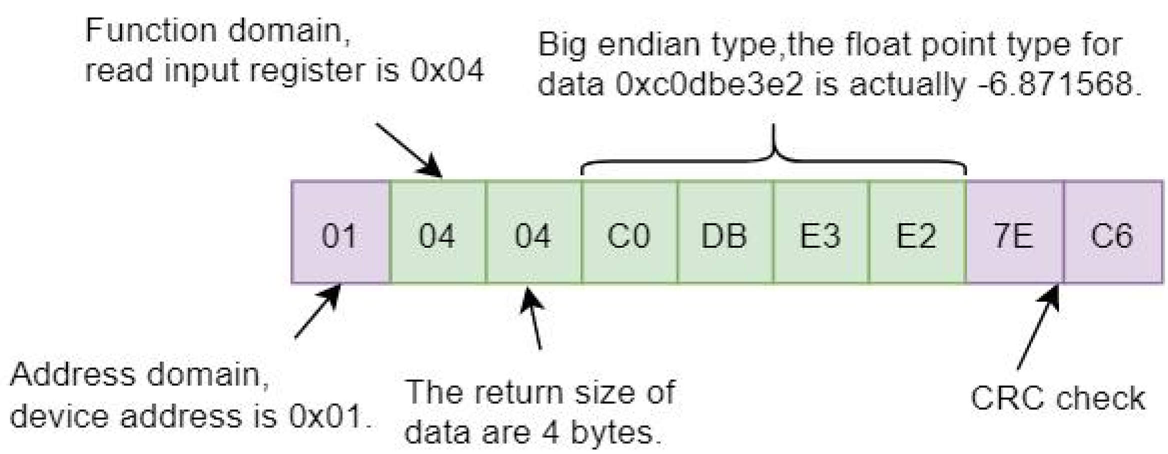
Data	Data register address
Peak value	0x0101
Average value	0x0102
Mean square root value	0x0103
Peak-to-average ratio	0x0104
Pulse width	0x0105
Duty ratio	0x0106
Repeat cycle	0x0107

List 2-2 Addresses of Data Registers in Channel 1

For example, the peak value in channel 1 is desired, the request from the host and the return from the slave would be like this:



Pic 2-3 Request from the host for peak value in channel 1



Pic 2-4 The returned data of peak value request in channel 1

As shown above, the peak value of channel 1 is -6.871568 dBm.
User can probably figure out the resemblance between this example and requesting other data in channel 1, since the only difference is the data register's address.
As for the data content, it's worth noting that pulse width, duty ratio and repeat cycle would only return valid data when a pulse signal is detected. Otherwise, 0xffffffff would be returned, representing no pulse signal is present.

2.2.3 Acquire Measured Data in Channel 2

The data in channel 2 and their addresses is shown below:

Data	Data Register Address
Peak value	0x0201
Average value	0x0202
Mean square root value	0x0203
Peak-to-average ratio	0x0204
Pulse width	0x0205
Duty ratio	0x0206
Repeat cycle	0x0207

List 2-3 Addresses of Data Registers in Channel 2

As for the format of requesting and returning of the data in channel 2, please refer to chapter 2.2.1.

2.2.4 Acquire Measured Data in Channel 3

The data in channel 3 and their addresses is shown below:

Data	Data Register Address
Peak value	0x0301
Average value	0x0302
Mean square root value	0x0303
Peak-to-average ratio	0x0304

Pulse width	0x0305
Duty ratio	0x0306
Repeat cycle	0x0307

List 2-4 Addresses of Data Registers in Channel 3

As for the format of requesting and returning of the data in channel 3, please refer to chapter 2.2.1.

2.2.5 Acquire Measured Data in Channel 4

The data in channel 4 and their addresses is shown below:

Data	Data Register Address
Peak value	0x0401
Average value	0x0402
Mean square root value	0x0403
Peak-to-average ratio	0x0404
Pulse width	0x0405
Duty ratio	0x0406
Repeat cycle	0x0407

List 2-5 Addresses of Data Registers in Channel 4

As for the format of requesting and returning of the data in channel 4, please refer to chapter 2.2.1.

2.3 Acquiring and Adjusting the Settings

Acquiring and adjusting the settings can be done by function domain 0x03 (read holding registers) and 0x06(write a single register).

Adjustable parameters in each channel of KC9532 is shown below:

Parameter	Description	Unit	Default Value	Adjustable Range	Data Type
Central frequency	The frequency of the external signal to be measured	MHz	2450 MHz	1~4000 MHz(1MHz stepping)	Signed 16 bits integer
External attenuators or amplifiers	External attenuators or amplifiers for compensation	dB	0 dB	-200~+200 dB(0.1dB stepping)	Signed 16 bits integer
Cable power dissipation	To compensate power dissipation caused by cable	dB	0 dB	-200~0dB(0.1dB stepping)	Signed 16 bits integer

Cable frequency dissipation	The frequency at which cable dissipation occurs	MHz	2450 MHz	1~4000 MHz(1MHz stepping)	Signed 16 bits integer
Sampling time of peak sampling	Time duration for each peak sampling	s	180 ms	10ms~10s (10ms stepping)	Signed 16 bits integer
Sampling time of average sampling	Time duration for each average sampling	s	180 ms	10~10s (10ms stepping)	Signed 16 bits integer
Sampling time of mean-square-root sampling	Time duration for each mean-square-root sampling	s	180 ms	10~10s (10ms stepping)	Signed 16 bits integer
Single pulse sampling time	Time duration for each pulse sampling	s	100 ms	1ms~3s (1ms stepping)	Signed 16 bits integer
Power threshold of pulse	A pulse signal whose power is greater than this value would be deemed as valid	dBm	-20 dBm	-51~+9 dBm(1dBm stepping)	Signed 16 bits integer
Power unit	The unit of the returned data can be set	/	0 (dBm as default)	0 : dBm 1 : mW	Signed 16 bits integer

List 2-6 Adjustable Parameters of Each Channel

Parameters for measuring are identical between each channel. Below would show the detailed settings in channel 1.

Note: When step is 0.1dB, the value should multiply by 10.

For example, user send 50 for "External attenuators or amplifiers" parameter means the actually value is 5dB.

2.3.1 Command Format for Reading Holding Register

According to standard Modbus-RTU protocol, the command format for reading holding register is shown below.

Data domain

1 Byte	1 Byte	2 Bytes	2 Bytes	2 Bytes
Address domain	Function domain	Register address	Request size of data	CRC check

Pic 2-5 Request from Host

Data domain

1 Byte	1 Byte	1 Byte	2 Bytes	2 Bytes
Address domain	Function domain	Return size of data	Data contents	CRC check

Pic 2-6 Response

Note: The size of request data from the host computer refers to the amount of 2-Byte data requested. A request size value of 2 represents the host computer will get a 4-Byte return.

The data stored in each register is of the size of 2 Byte. For this reason the data request from the host needs to be size 1, so that to obtain a size 2 data response in response frame from KC9532.

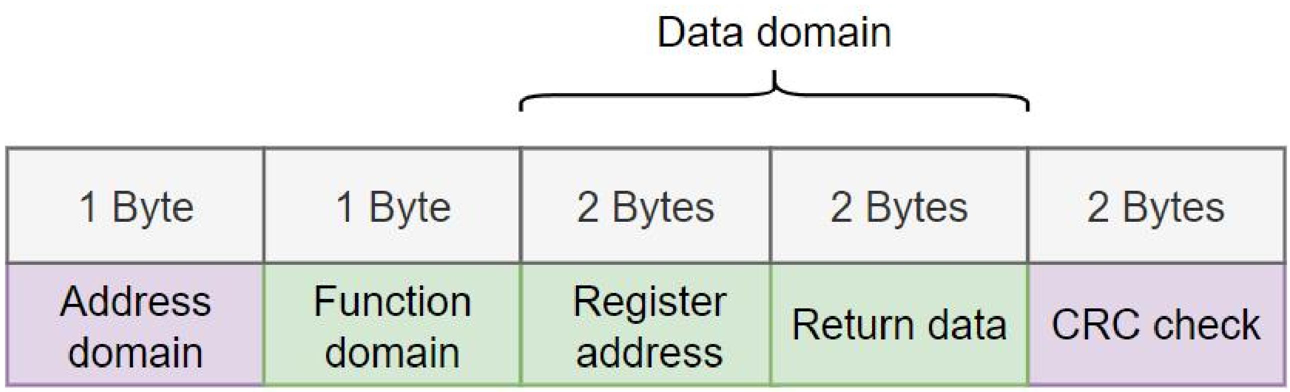
2.3.2 Command Format for Writing a Single Register

According to standard Modbus-RTU protocol format, the command format for writing a single register is shown below.

Data domain

1 Byte	1 Byte	2 Bytes	2 Bytes	2 Bytes
Address domain	Function domain	Register address	Write data	CRC check

Pic 2-7 Request from host



Pic 2-8 Response

The resemblance between the request and the response is clear, which can serve as an echo.

Likewise, the data written is also 2-Byte.

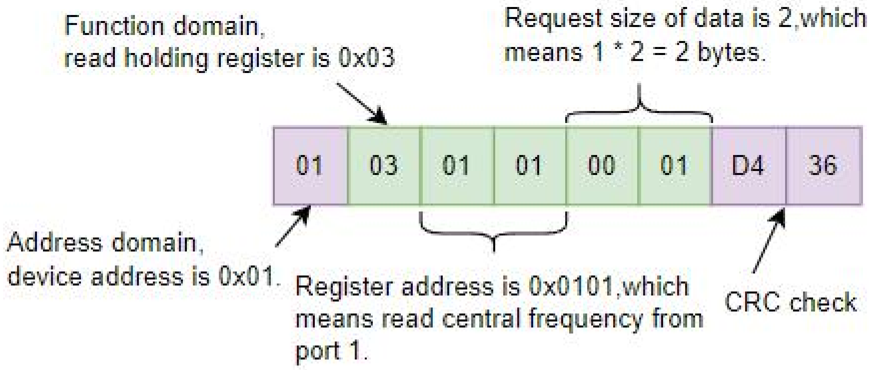
2.3.3 Acquire and adjust measuring parameters in channel 1

The addresses of measuring parameters of channel 1 is shown in the list below.

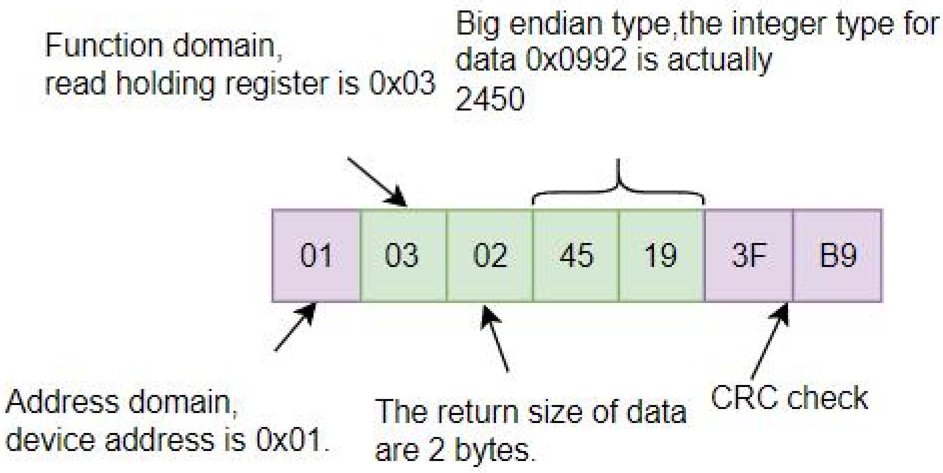
Parameter	Parameter register address
Central frequency	0x0101
External attenuator	0x0102
Cable power dissipation	0x0103
Cable frequency dissipation	0x0104
Single peak sampling time	0x0105
Single average sampling time	0x0106
Single mean-square-root sampling time	0x0107
Single pulse sampling time	0x0108
Pulse power threshold	0x0109
Unit of power	0x010A

List 2-7 Addresses of adjustable parameters in channel 1

Acquire central frequency in channel 1:



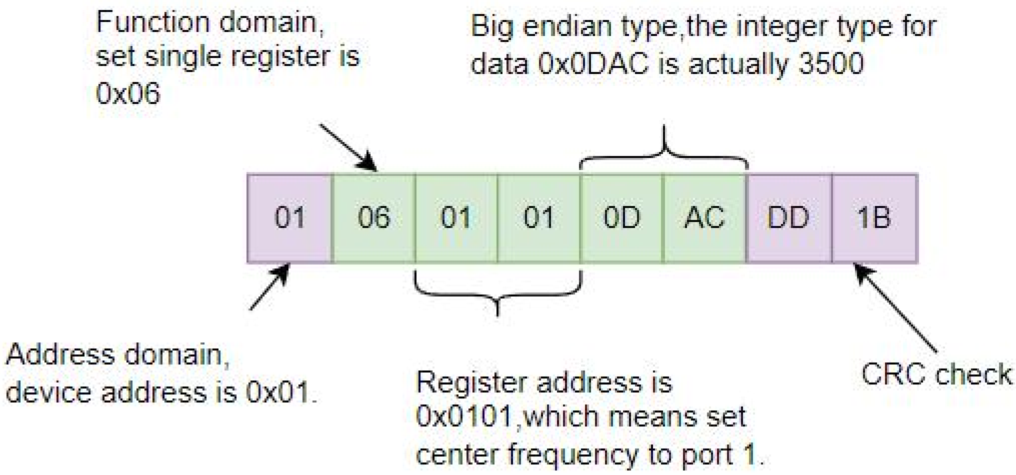
Pic 2-9 Host request for central frequency



Pic 2-10 Response

Adjust central frequency of channel 1:

Assume that the central frequency of channel 1 is 3500MHz, then the data would look like this.



Pic 2-11 Request and Response

The process of acquiring and adjusting other parameter registers resemble the process above.

2.3.4 Acquire and adjust measuring parameters in channel 2

The addresses of measuring parameters of channel 2 is shown in the list below.

Parameter	Parameter register address
Central frequency	0x0201
External attenuator	0x0202
Cable power dissipation	0x0203
Cable frequency dissipation	0x0204
Single peak sampling time	0x0205
Single average sampling time	0x0206
Single mean-square-root sampling time	0x0207
Single pulse sampling time	0x0208
Pulse power threshold	0x0209

Unit of power	0x020A

List 2-8 Addresses of adjustable parameters in channel 2

As for the protocol format of the measuring parameters in channel 2, please refer to chapter 2.3.3.

2.3.5 Acquire and adjust measuring parameters in channel 3

The addresses of measuring parameters of channel 3 is shown in the list below.

Parameter	Parameter register address
Central frequency	0x0301
External attenuator	0x0302
Cable power dissipation	0x0303
Cable frequency dissipation	0x0304
Single peak sampling time	0x0305
Single average sampling time	0x0306
Single mean-square-root sampling time	0x0307
Single pulse sampling time	0x0308
Pulse power threshold	0x0309
Unit of power	0x030A

List 2-9 Addresses of adjustable parameters in channel 3

As for the protocol format of the measuring parameters in channel 3, please refer to

chapter 2.3.3.

2.3.6 Acquire and adjust measuring parameters in channel 4

The addresses of measuring parameters of channel 4 is shown in the list below.

Parameter	Parameter register address
Central frequency	0x0401
External attenuator	0x0402
Cable power dissipation	0x0403
Cable frequency dissipation	0x0404
Single peak sampling time	0x0405
Single average sampling time	0x0406
Single mean-square-root sampling time	0x0407
Single pulse sampling time	0x0408
Pulse power threshold	0x0409
Unit of power	0x040A

List 2-10 Addresses of adjustable parameters in channel 4

As for the protocol format of the measuring parameters in channel 4, please refer to chapter 2.3.3.

2.4 Acquire the Auxiliary Info of Equipment

The auxiliary info of KC9532 is shown below.

Info	Description	Unit	Data Type
Temperature of the equipment	Since the equipment produces heat itself, this info is for reference only.	℃	Single-precision floating point
Software version	The info can also be acquired from USB port.	/	Unsigned 32-bit integer
Serial number	The info can also be acquired from USB port.	/	Unsigned 32-bit integer
USB voltage	The supply voltage of USB port.	V	Single-precision floating point
485 voltage	The supply voltage of 485 port.	V	Single-precision floating point

List 2-11 Auxiliary info list

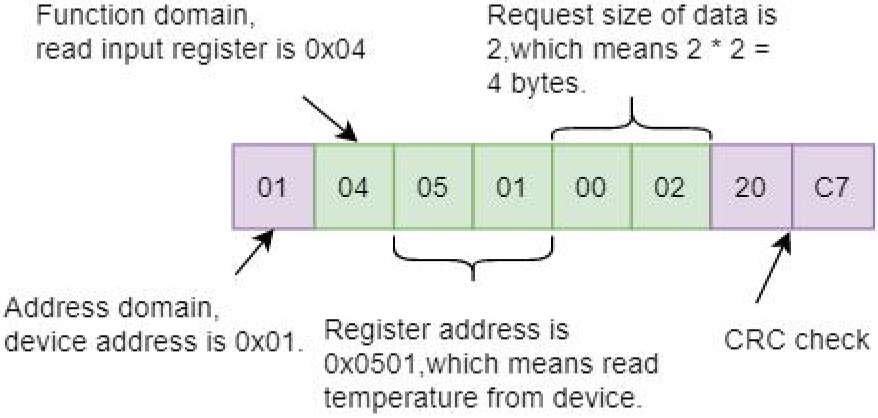
The acquisition of auxiliary info is achieved by reading the input registers, the addresses are shown below.

Info	Register address
Equipment temperature	0x0501
Software version	0x0502
Serial number	0x0503
USB Voltage	0x0504
485 Voltage	0x0505

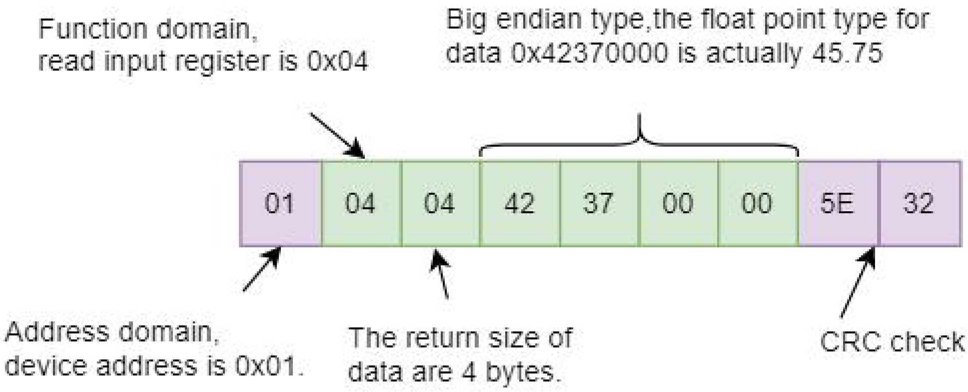
List 2-12 Auxiliary info registers addresses

The data length of the auxiliary info is 4 Byte as well, so the length of the request should be of 2 registers.

2.4.1 Acquire the temperature of the equipment



Pic 2-12 Request temperature



Pic 2-13 Response of the temperature

The returned temperature data is 45.75℃.

2.4.2 Acquire software version

The response data of software version is a 32-bit unsigned integer. To get the real version, user needs to divide this response value by 10.

For example:

Request: 01 04 05 02 00 02 D0 C7

Response: 01 04 04 00 00 00 0D 3A 41

The version data is 0x0000000D, which means 13 in decimal. Make this value divided by 10, that is 1.3, which means the current version is V1.3

2.4.3 Acquire serial number

The serial number data of KC9532 is an unsigned 32-bit integer. User can directly deem this value as the serial number.

2.4.4 Acquire USB and 485 voltage

The data of USB and 485 voltage are both floating point, user should just treat them with the floating-point way.

2.5 Adjust Auxiliary Parameters

The adjustable auxiliary parameters of KC9532 are listed below.

Parameter	Description	Data Type
Address of equipment	The range is 1-247. After reboot, USB port will output the new address as string.	Signed 16 bits integer
485 port baud rate	Designed to be adjustable to fit in different industrial environments with a maximum value of 460800. After reboot, USB port will output the new baud rate as string.	Signed 16 bits integer

Restore to factory	Restore all the settings to default.	/

List 2-13 Auxiliary parameters list

Likewise, the adjustment of the auxiliary parameters are achieved by writing a single register. The list of registers is shown below.

Parameter	Registers' address	Adjustable range
Address of equipment	0x0501	1-247
485 port baud rate	0x0502	See the list below
Restore to factory	0x0503	/

List 2-14 Auxiliary parameters' register

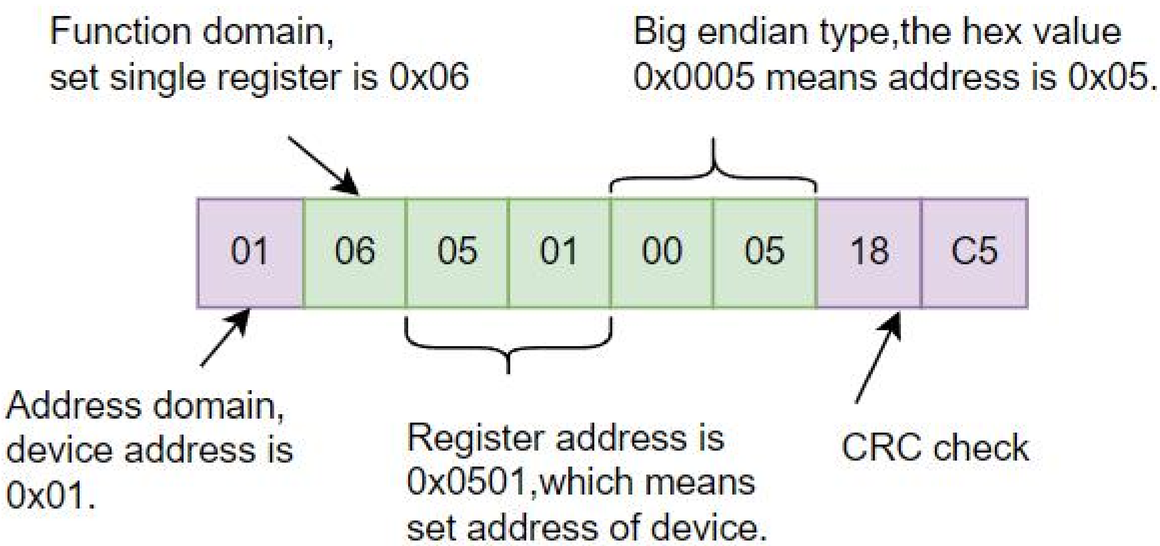
The data length of these registers is 4 Byte, so the request length made by user should be 2 registers.

2.5.1 Adjust the address of equipment

The new address becomes valid after rebooting.

For example:

change the equipment's address to 0x05.



Pic 2-14 Request and Response

The address becomes 0x05 after next boot.

2.5.2 Adjust 485 port's baud rate

The list below shows the available baud rate values.

Data value	Corresponding baud rate
0x0000	9600
0x0001	14400
0x0002	19200
0x0003	38400
0x0004	57600

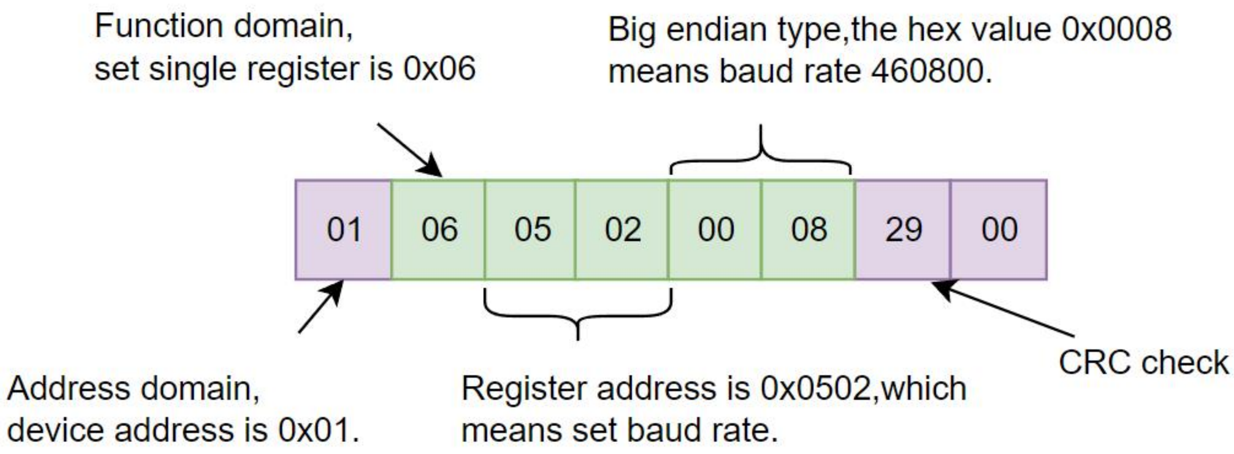
0x0005	115200
0x0006	128000
0x0007	256000
0x0008	460800

List 2-15 Data values and their corresponding baud rate

New baud rate setting becomes valid after next boot.

For example,

set the baud rate to 460800 would be like,



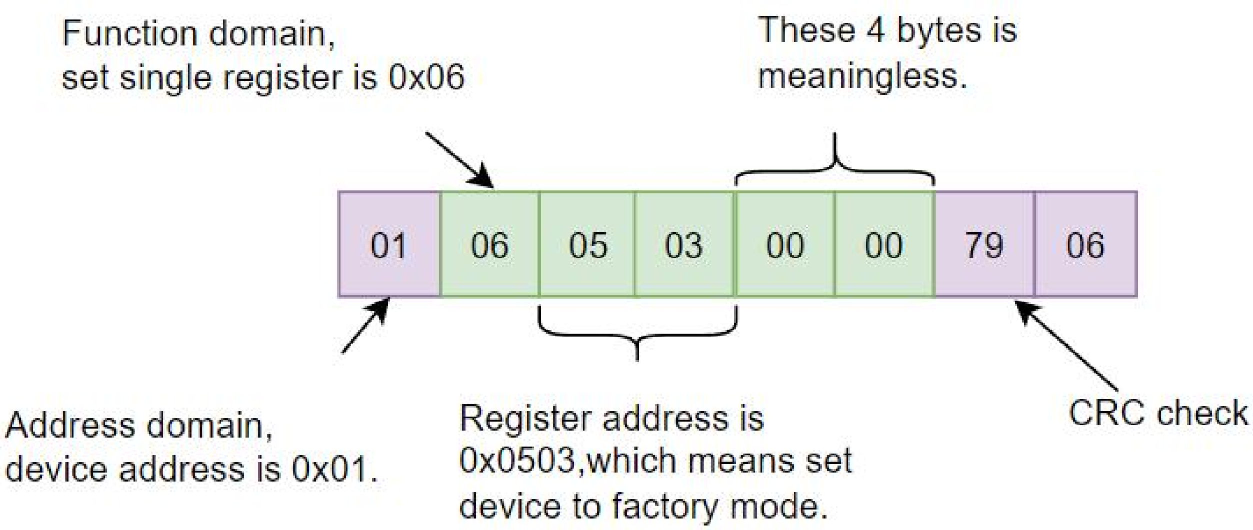
Pic 2-15 Request and Response of setting baud rate 460800

Next time it boots, the baud rate will become 460800.

2.5.3 Restore to Factory

After sending restore to factory request, **the equipment would restore all the settings to default and reboot immediately.**

Pay attention: **There will not be any response** since the equipment reboots itself immediately.



Pic 2-16 Request for restoring to factory sent by the host

[The END]