robustel | Software Manual

S6000U Smart Sensor Software Manual

Guangzhou Robustel Co., Ltd.
www.robustel.com

Technical Support
Tel: +86-20-82321505
Email: support@robustel.com
Web: www.robustel.com

Document History

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Date	Firmware Version	Document Version	Change Description
October 24, 2024	1.1.0	1.0.0	Initial release.

Contents

Chapter 1 About This Document

1.1. Purpose

This document describes the S6000U Smart Sensor in terms of its specifications, functions and configurations.

1.2. Document Conventions

This document uses Robustel's Software Manual typographic conventions, and observes the requirements stated in the specifications document.

1.3. Intended Audience and Reading Suggestions

The document is intended for engineers, developers and project managers. Before reading this document, it is highly recommended to obtain an overview of the product.

Chapter 2 Overview

2.1. Product Overview

The S6000U Smart Sensor (hereinafter referred to as the "S6000U") is an all-in-one industrial smart sensor for temperature, humidity, light, noise, air pressure etc., and supports reading sensor data via Modbus protocol. Its default slave address is 0x01, and default baud rate is 115200bps. For further details regarding the acceleration monitoring, please refer to "Chapter 3.3 Acceleration Calibration Settings" after installation.

2.2. Communication Specifications

Interface	RS-485
Communication mode	RS-485 (2-wire half-duplex mode)
Communication baud rate	9600/38400/57600/115200 (default)
Transmission code	RTU
Start bit	1 bit
Data bit	8 bit
Stop bit	1 bit
Parity bit	N/A

2.3. Function Code List

Function Code in Request	Name	Description	Function Code in Exception Response
0x03	Read Holding Register	This function code is used to read the binary contents of multiple holding registers.	0x83
0x04	Read Input Registers	This function code is used to read the binary contents of input registers.	0x84
0x06	Write Single Holding Register	This function code is used to write a single holding register in a remote device.	0x86
0x10	Write Multiple Holding Register	This function code is used to write multiple holding registers in a remote device.	0x90
0x14	Read File Record	This function code is used to read file record from devices.	
0x15	Write File Record	This function code is used to write file record to devices.	

2.4. Exception Code List

Exception Code	Name	Description
0x01	Illegal function	The function code received in the query is not an allowable action for the slave.
0x02	Illegal Data Address	The data address received in the query is not an allowable address for the slave.
0x03	Illegal Data Value	A value contained in the query data field is not an allowable value for the slave, such as that the tried value is out of the register range.
0x05	Negative acknowledge	The slave has accepted the request, but cannot perform the program function received in the query.

2.5. System Configuration Register List

Function	Register Function	Register Address	Register Type	Default	Data Range	User Notes
Changing slave address	Slave address register	0x01	Holding register	0x01	0x01~0xF7	
Changing baud rate	RS485 baud rate address register	0x02	Holding register	115200	9600/38400/ 57600/ 115200	
RTC-year setting	RTC-year address register	0x03	Holding register	2000	2000-2099	
RTC-month setting	RTC-month address register	0x04	Holding register	1	1~12	
RTC-day setting	RTC-day address register	0x05	Holding register	1	1~31	
RTC-hour setting	RTC-hour address register	0x06	Holding register	0	0~23	
RTC-minute setting	RTC-minute address register	0x07	Holding register	0	0~59	
RTC-second setting	RTC-second address register	0x08	Holding register	0	0~59	
Acceleration calibration	Acceleration calibration address register	0x09	Holding register	N/A	N/A	Should be installed vertically to the ground, and be calibrated after first use or factory reset. Please refer to Chapter 3.3.
Device reboot	Device reboot address register	0x0A	Holding register	N/A	N/A	

Function	Register Function	Register Address	Register Type	Default	Data Range	User Notes
Restore factory setting	Restore factory settings address register	0x0B	Holding register	N/A	N/A	Parameters like event, baud rate, slave address, RTC, acceleration, configured upper and lower limit registers will be cleared, and the device rebooted after Factory Reset is complete.

2.6. Feature Configuration Register List

Function	Register Function	Register Address	Register Type	Default	Data Range	User Notes
Change acceleration output type	Acceleration output type address register	0x10	Holding register	Skewed data	Raw data/ skewed data	Raw data 6k66Hz (refresh every 10 seconds); skewed data 208Hz
Acceleration sampling frequency for raw data	Acceleration sampling frequency for raw data register	0x11	Holding register	6k66	208-6k66Hz	The value is only effective if register 0x10 is set to the raw data.
Change temperature upper limit	Temperature upper limit address register	0x12	Holding register	70	Maximum +70°C	The setting value should be 100 times the actual temperature value.
Change temperature lower limit	Temperature lower limit address register	0x13	Holding register	-20	Minimum -20°C	
Change humidity upper limit	Humidity upper limit address register	0x14	Holding register	95	Maximum 95% RH	
Change humidity lower limit	Humidity lower limit address register	0x15	Holding register	5	Minimum 5% RH	
Change light upper limit	Light upper limit address register	0x16	Holding register	5	0/1/2/3/4/5	Light level L1~L5 Refer to Chapter 3.9 for further information.
Change light lower limit	Light lower limit address register	0x17	Holding register	0		
Change noise	Noise upper limit	0x18	Holding	120	Maximum	

Function	Register Function	Register Address	Register Type	Default	Data Range	User Notes
upper limit	address register		register		120dB SPL	
Change noise lower limit	Noise lower limit address register	0x19	Holding register	0	Minimum 0dB SPL	
Change air pressure upper limit	Air pressure upper limit address register high	0x1A	Holding register	126000.00	Maximum 126000.00Pa	The value of air pressure is a floating-point number.
Change air pressure upper limit	Air pressure upper limit address register low	0x1B	Holding register			
Change air pressure lower limit	Air pressure lower limit address register high	0x1C	Holding register	26000.00	Minimum 26000.00Pa	The value of air pressure is a floating-point number.
Change air pressure lower limit	Air pressure lower limit address register low	0x1D	Holding register			
Change TOF upper limit	TOF upper limit address register	0x1E	Holding register	360 cm	Furthest 360cm	
Change TOF lower limit	TOF lower limit address register	0x1F	Holding register	73 cm	Nearest 73cm	
Change tilt angle upper limit	Tilt angle upper limit address register	0x20	Holding register	90°	90°	
Change tilt angle lower limit	Tilt angle lower limit address register	0x21	Holding register	0°	0°	

2.7. Data Acquisition Register List

Function	Register Function	Register Address	Register Type	Default	Data Range	User Notes
Temperature data acquisition	Temperature address register	0x100	Input register	N/A	N/A	Unit: °C (100 times the actual value)
Humidity data acquisition	Humidity address register	0x101	Input register	N/A	N/A	Unit: % RH
Light data acquisition	Light address register	0x102	Input register	N/A	N/A	Light level L1~L5 Refer to Chapter

Function	Register Function	Register Address	Register Type	Default	Data Range	User Notes
						3.9 for further information.
Noise data acquisition	Noise address register	0x103	Input register	N/A	N/A	Unit: dB
Air pressure sensor data acquisition	Air pressure address register high	0x104	Input register	N/A	N/A	Unit: hPa The value of air pressure is a floating-point number.
Air pressure sensor data acquisition	Air pressure address register low	0x105	Input register	N/A	N/A	
TOF sensor data acquisition	TOF address register	0x106	Input register	N/A	N/A	Unit: cm
Y-axis skewed data acquisition	Y-axis skewed data address register	0x107	Input register	N/A	N/A	Unit: ° Tilt angle for the Y-axis
Single acceleration X-axis data acquisition	Single acceleration X-axis address register high	0x108	Input register	N/A	N/A	The acceleration value is a floating-point number. Value conversion formula: (result value)/1000*9.82 m/s^2
Single acceleration X-axis data acquisition	Single acceleration X-axis address register low	0x109	Input register	N/A	N/A	
Single acceleration Y-axis data acquisition	Single acceleration Y-axis address register high	0x10A	Input register	N/A	N/A	
Single acceleration Y-axis data acquisition	Single acceleration Y-axis address register low	0x10B	Input register	N/A	N/A	
Single acceleration Z-axis data acquisition	Single acceleration Z-axis address register high	0x10C	Input register	N/A	N/A	
Single acceleration Z-axis data acquisition	Single acceleration Z-axis address register low	0x10D	Input register	N/A	N/A	
Reading the length of the cached acceleration	Cached acceleration Z-axis address register	0x800	Input register	N/A	N/A	

Function	Register Function	Register Address	Register Type	Default	Data Range	User Notes
data						
Reading the marker of the cached acceleration data	Cached acceleration Z-axis address register	0x801	Input register	N/A	N/A	
Cached acceleration X-axis data acquisition	Cached acceleration X-axis address register	0x1000	Input register	N/A	N/A	The acceleration value is a floating-point number. Value conversion formula: (acquired value)/1000*9.82 m/s^2
Cached acceleration Y-axis data acquisition	Cached acceleration Y-axis address register	0x3000	Input register	N/A	N/A	
Cached acceleration Z-axis data acquisition	Cached acceleration Z-axis address register	0x5000	Input register	N/A	N/A	

2.8. Device Management Register List

Function	Register Function	Register Address	Register Type	Default	Data Range	User Notes
Device model	Device model register	0x7020	Input register	S6000U	N/A	Read 16 consecutive register values from the start address. The reading information must be converted into a valid ASCII format.
SN	Device SN register	0x7030	Input register	Vary depending on the device	N/A	
Firmware version	Firmware version register	0x7040	Input register	N/A	N/A	
OTA status marking	OTA status marking register	0x7050	Holding register	0	0/1	
OTA firmware length	OTA firmware length register	0x7051	Holding register	N/A	N/A	

2.9. Device Event Register List

Function	Register Function	Register Address	Register Type	Default	Data Range	User Notes
Fetch event counter	Event counter address register	0x7100	Input register	N/A	N/A	A blinking ALARM light means an event occurred. First, fetch the event length, if the counter is non-zero, then perform the next step.
Fetch event code	Event code register	0x7101	Input register	N/A	N/A	After rebooting or resetting to factory settings, wait 60 seconds to start recording events. Collect 5 consecutive register content from 0x7101 when calling to collect events.
Timestamp 16-bit high	Timestamp 16-bit high register		Input register	N/A	N/A	
Timestamp 16-bit low	Timestamp 16-bit low register		Input register	N/A	N/A	
Event value	Event value register high		Input register	N/A	N/A	
Event value	Event value register low		Input register	N/A	N/A	

2.10. Log Event Code List

Event Code	Event Meaning
01	Temperature value above the maximum setting
02	Temperature value below the minimum setting
03	Humidity value above the maximum setting
04	humidity value below the minimum setting
05	Light level value above the maximum setting
06	Light level value below the minimum setting
07	Noise value above the maximum setting
08	Noise value below the minimum setting
09	Air pressure value above the maximum setting
0A	Air pressure value below the minimum setting
0B	ToF distance value above the maximum setting
0C	ToF distance value below the minimum setting
0D	Tilt angle value above the maximum setting
0E	Tilt angle value below the minimum setting

Chapter 3 Configuration Guidelines

3.1. Slave Address Settings

The initial slave address register is 0x01, the address range is from 0x01 to 0xF7. For example, if the old slave address is 0x05, and you want to configure the new address to 0x02, the command is 0x06. The new address is applied after the command is sent.

The master sending a request frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Write Value High	Register Write Value Low	CRC High	CRC Low
0x05	0x06	0x00	0x01	0x00	0x02		

The slave returning a response frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Value High	Register Value Low	CRC High	CRC Low
0x05	0x06	0x00	0x01	0x00	0x02		

Command messages: 05 06 00 01 00 02 CRCH CRCL
Normal response: 05 06 00 01 00 02 CRCH CRCL
Exception response: 05 86 03 CRCH CRCL
86: Function code, indicates the response is an error response (called an exception response). Exceptions are indicated by adding a value 0x80 before the function code field of the response.
03: Exception code, indicates the data value requested by the master is illegal.

3.2. Baud Rate Settings

If the slave address is 0x05, and you want to configure the RS485 baud rate to 9600, the command is 0x06. The new parameter is applied after the command is sent.

The master sending a request frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Write Value High	Register Write Value Low	CRC High	CRC Low
0x05	0x06	0x00	0x02	0x00	0x00		

The slave returning a response frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Value High	Register Value Low	CRC High	CRC Low
0x05	0x06	0x00	0x02	0x00	0x00		

Command messages: 05 06 00 02 00 00 CRCH CRCL
Normal response: 05 06 00 02 00 00 CRCH CRCL

Value	Baud Rate
0	9600
1	38400
2	57600
3	115200

3.3. Acceleration Calibration Settings

You should recalibrate the acceleration before first use or after restoring to factory settings.
For example, the default slave address is 0x01 and the acceleration calibrating register is 0x09. After the calibration is completed, the RUN and ALARM indicators will alternately flash quickly 3 times .

The master sending a request frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Write Value High	Register Write Value Low	CRC High	CRC Low
0x01	0x06	0x00	0x09	0x00	0x01		

The slave returning a response frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Value High	Register Value Low	CRC High	CRC Low
0x01	0x06	0x00	0x09	0x00	0x01		

Command messages: 01 06 00 09 00 00 CRCH CRCL
Normal response: 01 06 00 09 00 00 CRCH CRCL

3.4. Acceleration Output Type Settings

Use slave address 0x05, to configure the acceleration output type to raw data, the command is 0x06.
Note: The value of data register refreshes every 10 seconds.

The master sending a request frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Write Value High	Register Write Value Low	CRC High	CRC Low
0x05	0x06	0x00	0x10	0x00	0x00		

The slave returning a response frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Value High	Register Value Low	CRC High	CRC Low
0x05	0x06	0x00	0x10	0x00	0x00		

Command messages: 05 06 00 10 00 00 CRCH CRCL
Normal response: 05 06 00 10 00 00 CRCH CRCL

Value	Unit
0	Input raw data
1	Input skewed data

3.5. Raw Acceleration Data Sampling Frequency Settings

Use slave address 0x05, if you want to set the raw acceleration data sampling frequency to 6k66Hz, the command is 0x06.

The master sending a request frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Write Value High	Register Write Value Low	CRC High	CRC Low
0x05	0x06	0x00	0x11	0x00	0x00		

The slave returning a response frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Value High	Register Value Low	CRC High	CRC Low
0x05	0x06	0x00	0x11	0x00	0x00		

Command messages: 05 06 00 04 00 00 CRCH CRCL
Normal response: 05 06 00 04 00 00 CRCH CRCL

Value	Unit
0	6k66Hz
1	208Hz
2	416Hz
3	833Hz
4	1k66Hz
5	3k33Hz

3.6. Temperature Upper/Lower Limit Settings

Temperature upper limit register address: 0x12
Temperature lower limit register address: 0x13
Note:
(1) The temperature upper limits setting cannot be less than the lower limits setting, and the lower cannot be greater than the upper. Incorrect setting will trigger an error code that cannot execute the request sent by the master device.
(2) The temperature range is from -40° to 85° C.

Temperature Upper Limit Settings

For example, the slave address is 0x05, and you want to set the temperature limit to 25.2 degrees Celsius, the command is 0x06 which corresponds to the data 25.2 * 100 = 2520 = 0x09D8.

The master sending a request frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Write Value High	Register Write Value Low	CRC High	CRC Low
0x05	0x06	0x00	0x12	0x09	0xD8		

The slave returning a response frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Value high	Register Value low	CRC High	CRC Low
0x05	0x06	0x00	0x12	0x09	0xD8		

Command messages: 05 06 00 12 09 D8 CRCH CRCL
Normal response: 05 06 00 07 09 D8 CRCH CRCL
Exception response 1: 05 86 03 CRCH CRCL, the temperature setting exceeds the specified range.

Exception response 2: 05 86 05 CRCH CRCL, the temperature setting is within the specified range. The temperature upper value is less than the lower setting, and an error that unable to execute request sent by the master device is returned.

Temperature Lower Limit Settings

The master sending a request frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Write Value High	Register Write Value Low	CRC High	CRC Low
0x05	0x06	0x00	0x13	0XF9	0x70		

The slave returning a response frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Value high	Register Value low	CRC High	CRC Low
0x05	0x06	0x00	0x13	0XF9	0x70		

For example, if you want to set the temperature lower limit to -16.8 degrees Celsius, the command is 0x06 which corresponds to the data -16.8*100 = -1680= 0xF970.

Command messages: 05 06 00 13 F9 70 CRCH CRCL
Normal response: 05 06 00 13 F9 70 CRCH CRCL
Exception response 1: 05 86 03 CRCH CRCL
Exception response 2: 05 86 05 CRCH CRCL, the temperature setting is within the specified range. The temperature lower value is greater than the upper setting, and an error that unable to execute request sent by the master device is returned.

3.7. Air Pressure Upper/Lower Limit Settings

Air pressure upper limit register address high: 0x1A
Air pressure upper limit register address low: 0x1B

Air pressure lower limit register address high: 0x1C
Air pressure lower limit register address low: 0x1D

The upper and lower air pressure limits are floating-point numbers. The slave address is 0x05, and you want to configure the upper air pressure to 120,000 (0x47EA6000) pascals, the command is 0x10.

The master sending a request frame:

Slave Address	Function Code	Register Starting Address High	Register Starting Address Low	Number of Write Registers High	Number of Write Registers Low	Byte Count	Data, High Word, High Byte	Data, High Word, Low Byte	Data, Low Word, High Byte	Data, Low Word, Low Byte	CRC Check
0x05	0x10	0x00	0x1A	0x00	0 x 02	0 x 60	0 x 00	0 x 47	0 x EA	0 x C0	

The slave returning a response frame:

Slave Address	Function Code	Register Starting Address High	Register Starting Address Low	Number of Write Registers High	Number of Write Registers Low	Byte Count	Data, High Word, High Byte	Data, High Word, Low Byte	Data, Low Word, High Byte	Data, Low Word, Low Byte	CRC Check
0x05	0x10	0x00	0x1A	0x00	0 x 02	0 x 60	0 x 00	0 x 47	0 x EA	0 x C0	

Command messages: 05 10 00 1A 00 02 04 60 00 47 EA CRCH CRCL
Normal response: 05 10 00 1A 00 02 04 60 00 47 EA CRCH CRCL

The slave address is 0x05, and you want to configure the lower air pressure to 101000 pascals, the command is 0x06 which corresponds to the data 101000-101325= -325=0xFEBB.

The master sending a request frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Write Value High	Register Write Value Low	CRC High	CRC Low
0x05	0x06	0x00	0x13	0xFE	0xBB		

The slave returning a response frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Value high	Register Value low	CRC High	CRC Low
0x05	0x06	0x00	0x13	0xFE	0xBB		

Command messages: 05 06 00 14 FE BB CRCH CRCL
Normal response: 05 06 00 14 FE BB CRCH CRCL

3.8. Other Settings

Other parameters like humidity, light, noise, TOF, tilt, X/Y/Z-axis acceleration upper and lower limits can be configured by referring to the configuration guidelines. For the register address table see chapter 2.2, using 0x06 command to configure the register address.

3.9. Light Data Reading

The following table shows the light level and related lux level.

Light Level	Light Lux Level
0	0~5 lux
1	6~50 lux
2	51~100 lux
3	101~500 lux
4	501~2000 lux
5	More than 2000 lux

The corresponding register is 0x102.

The master sending a request frame:

Slave Address	Function Code	Register Address High	Register Address Low	Number of Read Registers High	Number of Read Registers Low	Register Read Instruction High	Register Read Instruction Low	CRC High	CRC Low
0x05	0x04	0x01	0x02	0x00	0x02	0x00	0x01		

The slave returning a response frame:

Slave Address	Function Code	Register Value Byte	Register Data Byte	Data, High Word, High Byte	Data, High Word, Low Byte	Data, Low Word, High Byte	Data, Low Word, Low Byte	CRC High	CRC Low
0x05	0x04	0x04	0x02	0x00	0x01	0x00	0x01		

Command messages: 05 04 01 02 00 02 00 01 CRCH CRCL
Normal response: 05 04 04 02 00 01 00 01 CRCH CRCL

3.10. Air Pressure Data Reading

The corresponding registers are 0x104 and 0x105.

The master sending a request frame:

Slave Address	Function Code	Register Address High	Register Address Low	Number of Read Registers High	Number of Read Registers Low	Register Read Instruction High	Register Read Instruction Low	CRC High	CRC Low
0x05	0x04	0x01	0x04	0x00	0x02	0x00	0x01		

The slave returning a response frame:

Slave Address	Function Code	Register Value Byte	Register Data Byte	Data, High Word, High Byte	Data, High Word, Low Byte	Data, Low Word, High Byte	Data, Low Word, Low Byte	CRC High	CRC Low
0x05	0x04	0x04	0x04	0x00	0x01	0xD4	0xC0		

Command messages: 05 04 01 04 00 02 00 01 CRCH CRCL
Normal response: 05 04 04 04 00 01 D4 C0 CRCH CRCL

3.11. Buffer Length Reading of Acceleration Data

The corresponding register is 0x800.

The master sending a request frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Read Instruction High	Register Read Instruction Low	CRC High	CRC Low
0x05	0x04	0x08	0x00	0x00	0x01		

The slave returning a response frame:

Slave Address	Function Code	Register Value Byte	Register Value high	Register Value low	CRC High	CRC Low
0x05	0x04	0x02	0x04	0x00		

Command messages: 05 04 08 00 00 01 CRCH CRCL
Normal response: 05 04 02 04 00 CRCH CRCL
From the above return information, we know that the length of X/Y/Z-axis acceleration data in the current acceleration Buff is 0x400=1024 respectively.

3.12. Buffer Frame Reading of Acceleration Data

The corresponding register is 0x801.

The master sending a request frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Read Instruction High	Register Read Instruction Low	CRC High	CRC Low
0x05	0x04	0x08	0x01	0x00	0x01		

The slave returning a response frame:

Slave Address	Function Code	Register Value Byte	Register Value high	Register Value low	CRC High	CRC Low
0x05	0x04	0x02	0x00	0x09		

Command messages: 05 04 08 01 00 01 CRCH CRCL
Normal response: 05 04 02 00 09 CRCH CRCL
From the above table, we know that the current acceleration data frame is 9. With this information, we'll avoid reading acceleration buffer data across frames. If the frame number is 0 means that the acceleration data is being collected, avoid reading at this time. The frame number cycle increments from 1 to 100.

3.13. Buffer Reading of Acceleration Data

S6000U supports register cache, with built-in 1024 X/Y/Z-axis acceleration data (floating point number, refreshed every minute).
Note: Due to the limitation of Modbus protocol, the max number of registers that can be read in a single query is 125 (63 acceleration data) and the acceleration data is 1024 (1024*2=2048 registers), which need to be read 17 times.

The corresponding register address start space is: X-axis - 0x1000, Y-axis - 0x3000, Z-axis - 0x5000, which can be read consecutively.

For example:
Read 16 consecutive X-axis data from 0x1000 (format EFGHABCD floating-point number)
Request: 05 04 10 00 00 20 CRCH CRCL
Respond: 05 04 40 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 CRCH CRCL

Read 16 consecutive X-axis data from 0x1010
Request: 05 04 10 10 00 10 40 87
Respond: 05 04 40 C6 A8 BF F9 C6 A8 BF F9 C6 A8 BF F9 C6 A8 BF F9 C6 A8 BF F9 C6 A8 BF F9 C6 A8 BF F9 C6 A8 BF F9 C6 A8 BF F9 C6 A8 BF F9 C6 A8 BF F9 C6 A8 BF F9 C6 A8 BF F9 C6 A8 BF F9 C6 A8 BF F9 C6 A8 BF F9 CRCH CRCL

3.14. Modbus OTA Upgrade

To increase device upgrade performance, it is advisable to set the baud rate of the S6000U to 115,200 bits per second prior to upgrading. You need to configure the OTA upgrade status of the device, and use the command 0x10 to enable the OTA function for device.

The master sending a request frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Write Value High	Register Write Value Low	CRC High	CRC Low
0x05	0x10	0x70	0x50	0x00	0x01		

The slave returning a response frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Value high	Register Value low	CRC High	CRC Low
0x05	0x10	0x70	0x50	0x00	0x01		

Command messages: 05 10 70 40 00 01 CRCH CRCL
Normal response: 05 10 70 40 00 01 CRCH CRCL

If you want to read the OTA upgrade status of device, the command is 0x04. If the device is ready, the following response returns the device OTA as:
The master sending a request frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Write Value High	Register Write Value Low	CRC High	CRC Low
0x05	0x04	0x70	0x50	0x00	0x01		

The slave returning a response frame:

Slave Address	Function Code	Register Value Byte	Register Value high	Register Value low	CRC High	CRC Low
0x05	0x04	0x02	0x00	0x01		

Command messages: 05 04 70 50 00 01 CRCH CRCL
Normal response: 05 04 02 00 01 CRCH CRCL

If you want to write the firmware length, the command is 0x10.

The master sending a request frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Write Value High	Register Write Value Low	CRC High	CRC Low
0x05	0x10	0x70	0x51	0x00	0xF0		

The slave returning a response frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Value high	Register Value low	CRC High	CRC Low
0x05	0x10	0x70	0x51	0x00	0xF0		

Command messages: 05 10 70 51 00 F0 CRCH CRCL
Normal response: 05 10 70 51 00 F0 CRCH CRCL

If you want to read the firmware length, the command is 0x04. The following response returns as:
The master sending a request frame:

Slave Address	Function Code	Register Address High	Register Address Low	Register Write Value High	Register Write Value Low	CRC High	CRC Low
0x05	0x04	0x08	0x01	0x00	0x01		

The slave returning a response frame:

Slave Address	Function Code	Register Value Byte	Register Value high	Register Value low	CRC High	CRC Low
0x05	0x04	0x02	0x00	0xF0		

Command messages: 05 04 70 51 00 01 CRCH CRCL
Normal response: 05 04 02 00 F0 CRCH CRCL

Use the command 0x15 to write file and send cyclic packets according to the size until the sending is complete.
05 15 40 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 28 F6 3F 79 9F E3

Once the packet sending is done, the device upgrade is completed.
When reading the status of the device OTA upgrade again, use the command 0x03. If the device has been successfully upgraded, the following response returns the device OTA as:
Command messages: 05 04 70 40 00 01 CRCH CRCL
Normal response: 05 04 02 00 00 CRCH CRCL

Chapter 4 CRC Checking

Here is the CRC checksum for reference.

```
uint16_t GenCRC16(byte* buff, uint16_t len)
{
    uint16_t crc = 0xFFFF;
    uint16_t pos = 0;
    uint8_t i = 0;
    uint8_t lo = 0;
    uint8_t hi = 0;

    for (pos = 0; pos < len; pos++)
    {
        crc ^= buff[pos];

        for (i = 8; i != 0; i--)
        {
            if ((crc & 0x0001) != 0)
            {
                crc >>= 1;
                crc ^= 0xA001;
            }
            else
                crc >>= 1;
        }
    }
    lo = crc & 0xFF;
    hi = (crc >> 8) & 0xFF;

    buff[len++] = lo;
    buff[len++] = hi;

    return len;
}
```

Glossary

Abbr.	Description
ASCII	American Standard Code for Information Interchange
dB	Decibel
CRC	Cyclic Redundancy Check
RTC	Real Time Clock
RTU	Remote Terminal Unit
OTA	Over-The-Air
TOF	Time-of-Flight

Guangzhou Robustel Co., Ltd.
Add: 501, Building#2, 63 Yongan Road, Huangpu District, Guangzhou, China 511350
Email: info@robustel.com
Web: www.robustel.com