



鲁邦通 S6000U


智能传感器

# 协议说明手册



版权所有©2024 广州鲁邦通物联网科技股份有限公司  
保留一切权利。

### 商标许可

 是广州鲁邦通物联网科技股份有限公司的商标。本手册中提及的其他商标和商业名称均属于各自持有者。

### 免责声明

未经版权拥有者允许，不得以任何形式复制该文档的任意部分。由于方法、设计、生产工艺的不断改进，文档内容可能在未预先通知的情况下进行更新或修订。因未使用该文档导致任何错误或损坏，鲁邦通概不负责。

### 技术支持

电话：400-987-3791

邮件：[support@robustel.com](mailto:support@robustel.com)

网址：[www.robustel.com.cn](http://www.robustel.com.cn)

### 版本历史

这里不断累积文档版本的更新记录。因此，最新版本的文档包含了所有历史版本的更新记录。

日期	版本号	修改说明	编制者
2024.06.27	V1.0.0	首次发布	王灏
2024.08.14	V1.0.1	1. 更新光照度等级指示。 2. 新增数据测量单位说明。	王灏

# 目录

<b>第 1 章</b>	<b>引言</b> .....	<b>5</b>
1.1	编写目的 .....	5
1.2	文档约定 .....	5
1.3	预期读者和阅读建议 .....	5
<b>第 2 章</b>	<b>综合描述</b> .....	<b>6</b>
1.1	产品描述 .....	6
1.2	通信规格 .....	6
1.3	功能码列表 .....	6
1.4	异常码列表 .....	6
1.5	系统配置类寄存器功能列表 .....	7
1.6	功能配置类寄存器功能列表 .....	8
1.7	数据采集类寄存器功能列表 .....	9
1.8	设备管理类寄存器功能列表 .....	10
1.9	设备事件类寄存器功能列表 .....	10
1.10	日志事件码列表 .....	10
<b>第 3 章</b>	<b>配置指引</b> .....	<b>12</b>
3.1	从站地址配置 .....	12
3.2	波特率配置 .....	12
3.3	加速度校准设置 .....	13
3.4	加速度输出类型配置 .....	13
3.5	原始数据加速度采样频率配置 .....	13
3.6	温度上下限配置 .....	14
	温度上限配置 .....	14
	温度下限配置 .....	14
3.7	气压上下限配置 .....	15
3.8	其它配置 .....	16
3.9	气压数据读取 .....	17
3.10	加速度数据 Buffer 数据长度读取 .....	17
3.11	加速度数据 Buffer 数据帧读取 .....	18
3.12	加速度数据 Buffer 读取 .....	18
3.13	Modbus OTA 升级 .....	19
<b>第 4 章</b>	<b>CRC 校验</b> .....	<b>21</b>
	术语表 .....	22

# 第1章 引言

## 1.1 编写目的

本文档主要描述了S6000U的使用说明，给相关使用者参考。

## 1.2 文档约定

在编制本文档时，将遵循公司发布的软件需求说明书模板，并严格遵守其中的约定。

## 1.3 预期读者和阅读建议

S6000U 产品的相关使用人员及开发人员。

## 第2章 综合描述

### 1.1 产品描述

S6000U支持温度,湿度,光照,噪音,气压等传感器的数据采集,并支持通过Modbus协议对传感器的数据进行读取,默认从站地址0x01,默认波特率115200bps。如需使用加速度监测,请安装后参考3.3先进行加速度校准。

### 1.2 通信规格

接口	RS-485
通信方式	RS-485(2线式半双工)
通信波特率	9600/38400/57600/115200(默认)
传送代码	RTU
起始位	1位
数据位	8位
中止位	1位
校验位	无

### 1.3 功能码列表

功能码	名称	作用	异常响应功能码
0x03	读保持寄存器	读多个寄存器的值	0x83
0x04	读输入寄存器	读取输入寄存器中的值	0x84
0x06	写单个保持寄存器	向单个保持寄存器写入值	0x86
0x10	写多个保持寄存器	向多个保持寄存器写入值	0x90
0x14	读文件记录	从设备读取文件记录	
0x15	写文件记录	向设备写入文件记录	

### 1.4 异常码列表

代码	名称	含义
0x01	非法功能	请求的操作码未被从机识别或不被支持。
0x02	非法地址	请求访问的地址不在从机的可访问范围内。

0x03	非法数据值	发送的数据或值无效，例如，尝试写入超出寄存器范围的值。
0x05	拒绝	从机已经接收到了请求，但无法执行主站设备发送的请求。

### 1.5 系统配置类寄存器功能列表

功能	寄存器功能	寄存器地址	寄存器类型	默认值	数据范围	备注
从站地址修改	从站地址寄存器	0x01	保持寄存器	0x01	0x01~0xF7	
波特率修改	RS485 波特率地址寄存器	0x02	保持寄存器	115200	9600/38400/57600/115200	
RTC-年修改	RTC-年地址寄存器	0x03	保持寄存器	2000	2000-2099	
RTC-月修改	RTC-月地址寄存器	0x04	保持寄存器	1	1~12	
RTC-日修改	RTC-日地址寄存器	0x05	保持寄存器	1	1~31	
RTC-时修改	RTC-时地址寄存器	0x06	保持寄存器	0	0~23	
RTC-分修改	RTC-分地址寄存器	0x07	保持寄存器	0	0~59	
RTC-秒修改	RTC-秒地址寄存器	0x08	保持寄存器	0	0~59	
加速度校准	加速度校准地址寄存器	0x09	保持寄存器	N/A	N/A	需垂直地面安装，首次使用/恢复出厂设置后需进行校准，参考 3.3
设备重启	设备重启地址寄存器	0x0A	保持寄存器	N/A	N/A	
恢复出厂设置	设备恢复出厂设置地址寄存器	0x0B	保持寄存器	N/A	N/A	事件、波特率、从站地址、RTC、加速度相关、已配置的上下限寄存器功能参数被清除，恢复完成后设备会重启

## 1.6 功能配置类寄存器功能列表

功能	寄存器功能	寄存器地址	寄存器类型	默认值	数据范围	备注
加速度输出类型修改	加速度输出类型地址寄存器	0x10	保持寄存器	倾斜数据	原始数据/ 倾斜数据	原始数据 6k66Hz (固定 10s 刷新) 倾斜 208Hz
原始数据加速度采样频率	原始数据加速度采样频率寄存器	0x11	保持寄存器	6k66	208-6k66Hz	0x10 寄存器为原始数据时生效
温度上限修改	温度上限地址寄存器	0x12	保持寄存器	70	最高 +70° C	设置数值应为实际温度*100
温度下限修改	温度下限地址寄存器	0x13	保持寄存器	-20	最低 -20° C	
湿度上限修改	湿度上限地址寄存器	0x14	保持寄存器	95	最高 95%RH	
湿度下限修改	湿度下限地址寄存器	0x15	保持寄存器	5	最低 5%RH	
光照上限修改	光照上限地址寄存器	0x16	保持寄存器	5	0/1/2/3/4/5	光照等级 L1~L5 对应信息请参考 <a href="#">3.9 光照数据读取</a>
光照下限修改	光照下限地址寄存器	0x17	保持寄存器	0		
噪音上限修改	噪音上限地址寄存器	0x18	保持寄存器	120	最高 120dB SPL	
噪音下限修改	噪音下限地址寄存器	0x19	保持寄存器	0	最低 0dB SPL	
气压上限修改	气压上限地址寄存器高位	0x1A	保持寄存器	126000.00	最高 126000.00Pa	气压值为浮点数
气压上限修改	气压上限地址寄存器低位	0x1B	保持寄存器			
气压下限修改	气压下限地址寄存器高位	0x1C	保持寄存器	26000.00	最低 26000.00Pa	气压值为浮点数
气压下限修改	气压下限地址寄存器低位	0x1D	保持寄存器			
TOF 上限修改	TOF 上限地址寄存器	0x1E	保持寄存器	360 cm	最远 360cm	
TOF 下限修改	TOF 下限地址寄存器	0x1F	保持寄存器	73 cm	最近 73cm	
倾斜上限修改	倾斜上限地址寄存器	0x20	保持寄存器	90°	90°	
倾斜下限修改	倾斜下限地址寄存器	0x21	保持寄存器	0°	0°	



## 1.7 数据采集类寄存器功能列表

功能	寄存器功能	寄存器地址	寄存器类型	默认值	数据范围	备注
采集温度数据	温度地址寄存器	0x100	输入寄存器	N/A	N/A	测量单位：℃ 数值为实际温度*100
采集湿度数据	湿度地址寄存器	0x101	输入寄存器	N/A	N/A	测量单位：% RH
采集光照数据	光照地址寄存器	0x102	输入寄存器	N/A	N/A	光照等级 L1~L5 对应信息请参考 <a href="#">3.9 光照数据读取</a>
采集噪音数据	噪音地址寄存器	0x103	输入寄存器	N/A	N/A	测量单位：dB
采集气压传感器数据	气压地址寄存器高位	0x104	输入寄存器	N/A	N/A	测量单位：hPa 气压值为浮点数
采集气压传感器数据	气压地址寄存器低位	0x105	输入寄存器	N/A	N/A	
采集 TOF 传感器数据	TOF 地址寄存器	0x106	输入寄存器	N/A	N/A	测量单位：cm
采集 Y 轴倾斜数据	Y 轴倾斜数据地址寄存器	0x107	输入寄存器	N/A	N/A	测量单位：° 针对 Y 轴的倾斜角
采集单个加速度 X 轴数据	单个加速度 X 轴地址寄存器高位	0x108	输入寄存器	N/A	N/A	加速度数据为浮点数 采集值转换公式： (采集值) / 1000 * 9.82 m/s <sup>2</sup>
采集单个加速度 X 轴数据	单个加速度 X 轴地址寄存器低位	0x109	输入寄存器	N/A	N/A	
采集单个加速度 Y 轴数据	单个加速度 Y 轴地址寄存器高位	0x10A	输入寄存器	N/A	N/A	
采集单个加速度 Y 轴数据	单个加速度 Y 轴地址寄存器低位	0x10B	输入寄存器	N/A	N/A	
采集单个加速度 Z 轴数据	单个加速度 Z 轴地址寄存器高位	0x10C	输入寄存器	N/A	N/A	
采集单个加速度 Z 轴数据	单个加速度 Z 轴地址寄存器低位	0x10D	输入寄存器	N/A	N/A	
读取缓存的加速度数据长度	缓存加速度 Z 轴地址寄存器	0x800	输入寄存器	N/A	N/A	
读取缓存的加速度数据标识	缓存加速度 Z 轴地址寄存器	0x801	输入寄存器	N/A	N/A	
采集缓存的加速度 X 轴数据	缓存加速度 X 轴地址寄存器	0x1000	输入寄存器	N/A	N/A	加速度数据为浮点数 采集值转换公式： (采集值) / 1000 * 9.82 m/s <sup>2</sup>
采集缓存的加速度 Y 轴数据	缓存加速度 Y 轴地址寄存器	0x3000	输入寄存器	N/A	N/A	
采集缓存的加速度 Z 轴数据	缓存加速度 Z 轴地址寄存器	0x5000	输入寄存器	N/A	N/A	

## 1.8 设备管理类寄存器功能列表

功能	寄存器功能	寄存器地址	寄存器类型	默认值	数据范围	备注
设备型号	设备型号寄存器	0x7020	输入寄存器	S6000U	N/A	从起始地址连续读 16 个寄存器的信息。读取的信息需进行 ASCII 字符转码
SN	设备序列号寄存器	0x7030	输入寄存器	随设备变化	N/A	
固件版本信息	固件版本信息寄存器	0x7040	输入寄存器	N/A	N/A	
OTA 状态标志位	OTA 状态标志位寄存器	0x7050	保持寄存器	0	0/1	
OTA 固件长度	OTA 固件长度寄存器	0x7051	保持寄存器	N/A	N/A	

## 1.9 设备事件类寄存器功能列表

功能	寄存器功能	寄存器地址	寄存器类型	默认值	数据范围	备注
采集事件个数	事件个数地址寄存器	0x7100	输入寄存器	N/A	N/A	ALARM 灯闪烁即存在事件。 先采集事件长度，如个数不为零，进行下一步读取
采集事件码	采集事件码寄存器	0x7101	输入寄存器	N/A	N/A	重启/恢复出厂后，等待 60s 开始记录事件。 调取采集事件时，连续采集从 0x7101 开始 5 个寄存器的内容
时间戳高 16 位	时间戳高 16 位寄存器		输入寄存器	N/A	N/A	
时间戳低 16 位	时间戳低 16 位寄存器		输入寄存器	N/A	N/A	
事件值	事件值寄存器高位		输入寄存器	N/A	N/A	
事件值	事件值寄存器低位		输入寄存器	N/A	N/A	

## 1.10 日志事件码列表

事件码	事件信息
01	温度高于设定阈值
02	温度低于设定阈值
03	湿度高于设定阈值
04	湿度低于设定阈值
05	光线强度高于设定阈值
06	光线强度低于设定阈值
07	噪音高于设定阈值

08	噪音低于设定阈值
09	气压高于设定阈值
0A	气压低于设定阈值
0B	ToF 距离高于设定阈值
0C	ToF 距离低于设定阈值
0D	倾斜高于设定阈值
0E	倾斜低于设定阈值

## 第3章 配置指引

### 3.1 从站地址配置

支持从站地址配置，从站地址寄存器为0x01，从站地址范围：0x01~0xF7，比如：从站旧地址为05，需要配置为新地址0x02，使用0x06命令，当前指令处理完后生效。

主机发送数据帧：

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器写入 值高字节	寄存器写入 值低字节	CRC 高字节	CRC 低字节
0x05	0x06	0x00	0x01	0x00	0x02		

从站响应数据帧：

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器值 高字节	寄存器值 低字节	CRC 高字节	CRC 低字节
0x05	0x06	0x00	0x01	0x00	0x02		

使用命令：05 06 00 01 00 02 CRCH CRCL

正常返回：05 06 00 01 00 02 CRCH CRCL

异常返回：05 86 03 CRCH CRCL

86：功能码，表示异常响应。在功能码前添加了0x80，表示异常。

03：异常码，表示主站请求的数据值非法。

### 3.2 波特率配置

从站地址为0x05，需要配置RS485波特率为9600，使用0x06命令，当前指令处理完后生效。

主机发送数据帧：

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器写入 值高字节	寄存器写入 值低字节	CRC 高字节	CRC 低字节
0x05	0x06	0x00	0x02	0x00	0x00		

从站响应数据帧：

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器值 高字节	寄存器值 低字节	CRC 高字节	CRC 低字节
0x05	0x06	0x00	0x02	0x00	0x00		

使用命令：05 06 00 02 00 00 CRCH CRCL

正常返回：05 06 00 02 00 00 CRCH CRCL

数值	波特率
0	9600
1	38400
2	57600
3	115200

### 3.3 加速度校准设置

首次使用或恢复出厂设置后，需重新校准加速度。

例如：从站地址默认为0x01，加速度校准寄存器为0x09，进行加速度校准，校准完成后，RUN灯+ALARM灯交替快闪3下。

主机发送数据帧：

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器写入 值高字节	寄存器写入 值低字节	CRC 高字节	CRC 低字节
0x01	0x06	0x00	0x09	0x00	0x01		

从站响应数据帧：

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器值 高字节	寄存器值 低字节	CRC 高字节	CRC 低字节
0x01	0x06	0x00	0x09	0x00	0x01		

使用命令：01 06 00 09 00 00 CRCH CRCL

正常返回：01 06 00 09 00 00 CRCH CRCL

### 3.4 加速度输出类型配置

从站地址为0x05，需要配置加速度输出类型为原始数据，使用0x06命令。

注：数据寄存器值固定10s刷新一次。

主机发送数据帧：

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器写入 值高字节	寄存器写入 值低字节	CRC 高字节	CRC 低字节
0x05	0x06	0x00	0x10	0x00	0x00		

从站响应数据帧：

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器值 高字节	寄存器值 低字节	CRC 高字节	CRC 低字节
0x05	0x06	0x00	0x10	0x00	0x00		

使用命令：05 06 00 10 00 00 CRCH CRCL

正常返回：05 06 00 10 00 00 CRCH CRCL

数值	单位
0	输出原始数据
1	输出倾斜数据

### 3.5 原始数据加速度采样频率配置

从站地址为0x05，需要配置原始数据加速度采样周期为6k66Hz，使用0x06命令。

主机发送数据帧：

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器写入 值高字节	寄存器写入 值低字节	CRC 高字节	CRC 低字节
------	-----	--------------	--------------	---------------	---------------	------------	------------

0x05	0x06	0x00	0x11	0x00	0x00		
------	------	------	------	------	------	--	--

从站响应数据帧:

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器值 高字节	寄存器值 低字节	CRC 高字节	CRC 低字节
0x05	0x06	0x00	0x11	0x00	0x00		

使用命令: 05 06 00 04 00 00 CRCH CRCL

正常返回: 05 06 00 04 00 00 CRCH CRCL

数值	单位
0	6k66Hz
1	208Hz
2	416Hz
3	833Hz
4	1k66Hz
5	3k33Hz

### 3.6 温度上下限配置

温度上限寄存器地址: 0x12

温度下限寄存器地址: 0x13

注:

(1) 温度上限设置值不能低于下限, 温度下限设置值不能高于上限, 设置错误会触发无法执行主站设备发送的请求错误码。

(2) 温度范围[-40, 85]摄氏度。

#### 温度上限配置

比如: 从站地址为0x05, 需要配置温度上限为25.2摄氏度, 使用0x06命令, 对应数据为 $25.2 * 100 = 2520 = 0x09D8$

主机发送数据帧:

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器写入 值高字节	寄存器写入 值低字节	CRC 高字节	CRC 低字节
0x05	0x06	0x00	0x12	0x09	0xD8		

从站响应数据帧:

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器值 高字节	寄存器值 低字节	CRC 高字节	CRC 低字节
0x05	0x06	0x00	0x12	0x09	0xD8		

使用命令: 05 06 00 12 09 D8 CRCH CRCL

正常返回: 05 06 00 07 09 D8 CRCH CRCL

异常返回1: 05 86 03 CRCH CRCL, 温度设定超过指定范围

异常返回2: 05 86 05 CRCH CRCL, 温度设定在指定范围内, 温度上限设置值低于下限, 返回无法执行主站设备发送的请求错误。

#### 温度下限配置

主机发送数据帧:

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器写入 值高字节	寄存器写入 值低字节	CRC 高字节	CRC 低字节
0x05	0x06	0x00	0x13	0xF9	0x70		

从站响应数据帧:

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器值 高字节	寄存器值 低字节	CRC 高字节	CRC 低字节
0x05	0x06	0x00	0x13	0xF9	0x70		

比如：需要配置温度下限为-16.8摄氏度，使用0x06命令，，对应数据为-16.8\*100 = -1680= 0xF970，补码表示

使用命令：05 06 00 13.F9 70 CRCH CRCL

正常返回：05 06 00 13 F9 70 CRCH CRCL

异常返回1：05 86 03 CRCH CRCL

异常返回2：05 86 05 CRCH CRCL，温度设定在指定范围内，温度下限设置值高于上限，返回无法执行主站设备发送的请求错误。

### 3.7 气压上下限配置

气压上限寄存器地址高位：0x1A

气压上限寄存器地址低位：0x1B

气压下限寄存器地址高位：0x1C

气压下限寄存器地址低位：0x1D

气压上下限为浮点数，从站地址为0x05，需要配置上限气压120000（0x47EA6000）帕斯卡，使用0x10命令。

主机发送数据帧:

从站地址	功能码	寄存器起始 地址高位	寄存器起始 地址低位	写入寄存器 数量高位	写入寄存器 数量低位	写入的字节 数	高位寄存器 写入值高位	高位寄存器 写入值低位	低位寄存器 写入值高位	低位寄存器 写入值低位	CRC 校验位
0x05	0x10	0x00	0x1A	0x00	0x02	0x60	0x00	0x47	0xEA	0xC0	

从站响应数据帧:

从站地址	功能码	寄存器起始 地址高位	寄存器起始 地址低位	写入寄存器 数量高位	写入寄存器 数量低位	写入的字节 数	高位寄存器 值高位	高位寄存器 值低位	低位寄存器 值高位	低位寄存器 值低位	CRC 校验位
0x05	0x10	0x00	0x1A	0x00	0x02	0x60	0x00	0x47	0xEA	0xC0	

使用命令：05 10 00 1A 00 02 04 60 00 47 EA CRCH CRCL

正常返回：05 10 00 1A 00 02 04 60 00 47 EA CRCH CRCL

从站地址为0x05，需要配置下限气压101000帕斯卡，使用0x06命令，对应数据为101000-101325=-325=0xFE8B。

主机发送数据帧:

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器写入 值高字节	寄存器写入 值低字节	CRC 高字节	CRC 低字节
0x05	0x06	0x00	0x13	0xFE	0x8B		

从站响应数据帧:

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器值 高字节	寄存器值 低字节	CRC 高字节	CRC 低字节
0x05	0x06	0x00	0x13	0xFE	0xBB		

使用命令：05 06 00 14 FE BB CRCH CRCL

正常返回：05 06 00 14 FE BB CRCH CRCL

### 3.8 其它配置

湿度、光照、噪音、TOF、倾斜、X/Y/Z轴加速度上下限均可参照配置指引进行配置，寄存器地址参考2.2章节中寄存器表，使用0x06命令对寄存器地址进行配置。



### 3.9 光照数据读取

光照等级数据对照表

光照等级	照度值
0	0~5 lux
1	6~50 lux
2	51~100 lux
3	101~500 lux
4	501~2000 lux
5	2000 lux 以上

对应寄存器为：0x102

主机发送数据帧：

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	读取寄存器数 量高位	读取寄存器数 量低位	寄存器读取指 令高字节	寄存器读取指 令低字节	CRC 高字节	CRC 低字节
0x05	0x04	0x01	0x02	0x00	0x02	0x00	0x01		

从站响应数据帧：

从站地址	功能码	寄存器值 字节数	寄存器数据字 节数	高位寄存器值 高字节	高位寄存器值 低字节	低位寄存器值 高字节	低位寄存器值 低字节	CRC 高字节	CRC 低字节
0x05	0x04	0x04	0x02	0x00	0x01	0x00	0x01		

使用命令：05 04 01 02 00 02 00 01 CRCH CRCL

正常返回：05 04 04 02 00 01 00 01 CRCH CRCL

### 3.10 气压数据读取

对应寄存器为：0x104, 0x105

主机发送数据帧：

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	读取寄存器数 量高位	读取寄存器数 量低位	寄存器读取指 令高字节	寄存器读取指 令低字节	CRC 高字节	CRC 低字节
0x05	0x04	0x01	0x04	0x00	0x02	0x00	0x01		

从站响应数据帧：

从站地址	功能码	寄存器值 字节数	寄存器数据字 节数	高位寄存器值 高字节	高位寄存器值 低字节	低位寄存器值 高字节	低位寄存器值 低字节	CRC 高字节	CRC 低字节
0x05	0x04	0x04	0x04	0x00	0x01	0xD4	0xC0		

使用命令：05 04 01 04 00 02 00 01 CRCH CRCL

正常返回：05 04 04 04 00 01 D4 C0 CRCH CRCL

### 3.11 加速度数据 Buffer 数据长度读取

对应寄存器为：0x800

主机发送数据帧：



### 3.14 Modbus OTA 升级

为提高设备升级效率，建议升级时将设备波特率设定为115200 bps。

需要配置设备OTA升级状态，使用0x10命令，设备开启OTA功能。

主机发送数据帧：

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器写入 值高字节	寄存器写入 值低字节	CRC 高字节	CRC 低字节
0x05	0x10	0x70	0x50	0x00	0x01		

从站响应数据帧：

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器值 高字节	寄存器值 低字节	CRC 高字节	CRC 低字节
0x05	0x10	0x70	0x50	0x00	0x01		

使用命令：05 10 70 40 00 01 CRCH CRCL

正常返回：05 10 70 40 00 01 CRCH CRCL

读取设备OTA升级状态，使用0x04命令，若设备准备就绪，读取设备OTA返回如下

主机发送数据帧：

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器写入 值高字节	寄存器写入 值低字节	CRC 高字节	CRC 低字节
0x05	0x04	0x70	0x50	0x00	0x01		

从站响应数据帧：

从站地址	功能码	寄存器值字 节数	寄存器值 高字节	寄存器值 低字节	CRC 高字节	CRC 低字节
0x05	0x04	0x02	0x00	0x01		

使用命令：05 04 70 50 00 01 CRCH CRCL

正常返回：05 04 02 00 01 CRCH CRCL

写固件长度，需要使用0x10命令

主机发送数据帧：

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器写入 值高字节	寄存器写入 值低字节	CRC 高字节	CRC 低字节
0x05	0x10	0x70	0x51	0x00	0xF0		

从站响应数据帧：

从站地址	功能码	寄存器地址 高字节	寄存器地址 低字节	寄存器值 高字节	寄存器值 低字节	CRC 高字节	CRC 低字节
0x05	0x10	0x70	0x51	0x00	0xF0		

使用命令：05 10 70 51 00 F0 CRCH CRCL

正常返回：05 10 70 51 00 F0 CRCH CRCL

读取固件长度，使用0x04命令，返回如下

主机发送数据帧：



## 第4章 CRC 校验

crc校验函数参考如下:

```
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;
}
```

## 术语表

缩写	解释参照
AC	Alternating Current
APN	Access Point Name of GPRS Service Provider Network
ASCII	American Standard Code for Information Interchange
CE	Conformité Européene (European Conformity)
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface for Batch scripting
CSD	Circuit Switched Data
CTS	Clear to Send
dB	DeciBel
dBi	DeciBel Relative to an Isotropic radiator
DC	Direct Current
DCD	Data Carrier Detect
DCE	Data Communication Equipment (typically modems)
DCS 1800	Digital Cellular System, also referred to as PCN
DI	Digital Input
DO	Digital Output
DSR	Data Set Ready
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi-frequency
DTR	Data Terminal Ready
EDGE	Enhanced Data rates for GloBal Evolution of GSM and IS-136
EMC	Electromagnetic CompatiBility
EMI	Electro-Magnetic Interference
ESD	Electrostatic Discharges
ETSI	European Telecommunications Standards Institute
FDD LTE	Frequency Division Duplexing Long Term Evolution
GND	Ground
GPRS	General Packet Radio Service
GRE	generic route encapsulation
GSM	GloBal System for MoBile Communications
HSPA	High Speed Packet Access
ID	identification data
IMEI	International MoBile Equipment Identification
IP	Internet Protocol
IPsec	Internet Protocol Security
kBps	kBits per second
L2TP	Layer 2 Tunneling Protocol
LAN	local area network

缩写	解释参照
LED	Light Emitting Diode
M2M	Machine to Machine
MAX	Maximum
Min	Minimum
MO	MoBile Originated
MS	MoBile Station
MT	MoBile Terminated
OpenVPN	Open Virtual Private Network
PAP	Password Authentication Protocol
PC	Personal Computer
PCN	Personal Communications Network, also referred to as DCS 1800
PCS	Personal Communication System, also referred to as GSM 1900
PDU	Protocol Data Unit
PIN	Personal Identity NumBer
PLCs	Program Logic Control System
PPP	Point-to-point Protocol
PPTP	Point to Point Tunneling Protocol
PSU	Power Supply Unit
PUK	Personal UnBlocking Key
R&TTE	Radio and Telecommunication Terminal Equipment
RF	Radio Frequency
RTS	Request to Send
RTU	Remote Terminal Unit
Rx	Receive Direction
SDK	Software Development Kit
SIM	suBscriBer identification module
SMA antenna	StuBBY antenna or Magnet antenna
SMS	Short Message Service
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TE	Terminal Equipment, also referred to as DTE
Tx	Transmit Direction
UART	Universal Asynchronous Receiver-transmitter
UMTS	Universal MoBile Telecommunications System
USB	Universal Serial Bus
USSD	Unstructured Supplementary Service Data
VDC	Volts Direct Current
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VSWR	Voltage Stationary Wave Ratio
WAN	Wide Area Network



**广州鲁邦通物联网科技股份有限公司**

**Guangzhou Robustel Co., Ltd.**

地址：广州市黄埔区永安大道 63 号 2 栋 501

电话：400-987-3791

邮箱：[info@robustel.com](mailto:info@robustel.com)

网址：[www.robustel.com.cn](http://www.robustel.com.cn)