通讯协议

本产品的通讯协议为 Modbus RTU 协议，设备地址的有效范围为 0x01~0xFF；通讯波特率可选 1200bps、2400bps、4800bps、9600bps、19200bps、38400bps、57600bps、115200bps 等；串口通讯的帧格式为 1 个起始位、8 个数据位，校验位和停止位可选：偶校验+1 个停止位、奇校验+1 个停止位、无校验+1 个停止位或无校验+2 位停止位。

1.功能码描述

功能码	功能	备注
01(0x01)	读线圈	读继电器状态
02(0x02)	读离散量输入	读开关量输入状态
04(0x04)	读输入寄存器	读模拟量输入值
05(0x05)	写单个线圈	写单个继电器状态

2.寄存器地址分配

(1)继电器输出： 功能码 0x01（读多个）、0x05（写单个）
0x0000H 第 1 路继电器输出通道状态 0 表示 OFF，1 表示 ON

(2)开关量输入： 功能码 0x02（读多个）
0x0000H 第 1 路开关量输入通道状态 0 表示 OFF/低电平，1 表示 ON/高电平
0x0001H 第 2 路开关量输入通道状态 0 表示 OFF/低电平，1 表示 ON/高电平
0x0002H 第 3 路开关量输入通道状态 0 表示 OFF/低电平，1 表示 ON/高电平
0x0003H 第 4 路开关量输入通道状态 0 表示 OFF/低电平，1 表示 ON/高电平
0x0004H 第 5 路开关量输入通道状态 0 表示 OFF/低电平，1 表示 ON/高电平
0x0030H 第 1 路开关量输入报警标志 0 表示正常，1 表示报警
0x0031H 第 2 路开关量输入报警标志 0 表示正常，1 表示报警
0x0032H 第 3 路开关量输入报警标志 0 表示正常，1 表示报警
0x0033H 第 4 路开关量输入报警标志 0 表示正常，1 表示报警

注：只有在开关量输入通道报警使能的情况下，才可读开关量输入通道报警标志，否则按异常码 04 处理。

(3)模拟量输入： 功能码 0x04（读多个）
0x0000H 第 1 路模拟量输入通道值 数值范围（十进制）0~10000
0x0001H 第 2 路模拟量输入通道值 数值范围（十进制）0~10000
0x0002H 第 3 路模拟量输入通道值 数值范围（十进制）0~10000
0x0003H 第 4 路模拟量输入通道值 数值范围（十进制）0~10000
0x0004H 第 5 路模拟量输入通道值 数值范围（十进制）0~10000
0x0005H 第 6 路模拟量输入通道值 数值范围（十进制）0~10000
0x0006H 第 7 路模拟量输入通道值 数值范围（十进制）0~10000
0x0007H 第 8 路模拟量输入通道值 数值范围（十进制）0~10000

0x0030H 第 1 路模拟量输入报警标志
00：无报警；01：上限报警；
02：下限报警；03：上上限报警；
04：下下限报警

0x0031H 第 2 路模拟量输入报警标志 同上
0x0032H 第 3 路模拟量输入报警标志 同上
0x0033H 第 4 路模拟量输入报警标志 同上
0x0034H 第 5 路模拟量输入报警标志 同上
0x0035H 第 6 路模拟量输入报警标志 同上
0x0036H 第 7 路模拟量输入报警标志 同上
0x0037H 第 8 路模拟量输入报警标志 同上

注：只有在模拟量输入通道报警使能的情况下，才可读模拟量输入通道报警标志，否则按异常码 04 处理

支持的通道数量与产品型号相关，具体数量详见《KL-N7000 系列 GPRS 数据采集模块说明书》中的产品型号说明。

3.通讯命令

(1)读继电器通道状态
请求命令：

设备地址	0x01~0xF7	(Hex)	1 字节
功能码	0x01	(Hex)	1 字节
起始地址	0x0000~0xFFFF	(Hex)	2 字节
读取寄存器个数	0x0001~0x07D0	(Hex)	2 字节
CRC 校验	0x0000~0xFFFF	(Hex)	2 字节

响应：

设备地址	0x01~0xF7	(Hex)	1 字节
功能码	0x01	(Hex)	1 字节
字节计数	0x01	(Hex)	1 字节
输入状态		(Hex)	1 字节
CRC 校验	0x0000~0xFFFF	(Hex)	2 字节

异常响应：

设备地址	0x01~0xF7	(Hex)	1 字节
异常功能码	0x81	(Hex)	1 字节
异常码	01/02/03/04	(Hex)	1 字节
CRC 校验	0x0000~0xFFFF	(Hex)	2 字节

示例：读第 1 路继电器状态，假设当前设备地址为 0x01；

请求		响应	
字段名	十六进制	字段名	十六进制
设备地址	01	设备地址	01
功能	01	功能	01
起始地址 Hi	00	字节计数	01
起始地址 Lo	00	输出状态	01
输出数量 Hi	00	CRC 校验 Lo	90
输出数量 Lo	01	CRC 校验 Hi	48
CRC 校验 Lo	FD		
CRC 校验 Hi	CA		

其中，输出状态 0x01 为继电器输出通道的状态，其二进制数是 0000 0001，表明第 1 路继电器动作。

(2)读开关量通道状态

请求命令：

设备地址	0x01~0xF7	(Hex)	1 字节
功能码	0x02	(Hex)	1 字节
起始地址	0x0000~0xFFFF	(Hex)	2 字节
读取寄存器个数	0x0001~0x07D0	(Hex)	2 字节
CRC 校验	0x0000~0xFFFF	(Hex)	2 字节

响应：

设备地址	0x01~0xF7	(Hex)	1 字节
功能码	0x02	(Hex)	1 字节
字节计数	N*	(Hex)	1 字节
输入状态		(Hex)	N* x 1 字节
CRC 校验	0x0000~0xFFFF	(Hex)	2 字节

N* = 读取寄存器的个数

异常响应：

设备地址	0x01~0xF7	(Hex)	1 字节
异常功能码	0x82	(Hex)	1 字节
异常码	01/02/03/04	(Hex)	1 字节
CRC 校验	0x0000~0xFFFF	(Hex)	2 字节

示例：读 4 路开关量采集值，假设当前设备地址为 0x01；

请求		响应	
字段名	十六进制	字段名	十六进制
设备地址	01	设备地址	01
功能	02	功能	02
起始地址 Hi	00	字节计数	01
起始地址 Lo	00	输入状态	03
输出数量 Hi	00	CRC 校验 Lo	E1
输出数量 Lo	04	CRC 校验 Hi	89
CRC 校验 Lo	79		
CRC 校验 Hi	C9		

其中，输入状态 0x03 为开关量输入通道的状态，其二进制数是 00111110，表明第 1、2 路通道为高电平或悬空；3、4 路通道为低电平或对 GND 短接。

(3)读模拟量采集值

请求命令：

设备地址	0x01~0xF7	(Hex)	1 字节
功能码	0x04	(Hex)	1 字节
起始地址	0x0000~0xFFFF	(Hex)	2 字节
读取寄存器个数	0x0001~0x007D	(Hex)	2 字节
CRC 校验	0x0000~0xFFFF	(Hex)	2 字节

响应：

设备地址	0x01~0xF7	(Hex)	1 字节
功能码	0x04	(Hex)	1 字节
字节计数	2 x N*	(Hex)	1 字节
寄存器数据		(Hex)	N* x 2 字节
CRC 校验	0x0000~0xFFFF	(Hex)	2 字节

N* = 读取寄存器的个数

异常响应：

设备地址	0x01~0xF7	(Hex)	1 字节
异常功能码	0x84	(Hex)	1 字节
异常码	01/02/03/04	(Hex)	1 字节
CRC 校验	0x0000~0xFFFF	(Hex)	2 字节

示例：读第 1 和第 2 路模拟量采集值，假设当前设备地址为 0x01；

请求		响应	
字段名	十六进制	字段名	十六进制
设备地址	01	设备地址	01
功能	04	功能	04
起始地址 Hi	00	字节计数	04
起始地址 Lo	00	寄存器值 Hi(0)	00
输出数量 Hi	00	寄存器值 Lo(0)	25
输出数量 Lo	02	寄存器值 Hi(1)	10
CRC 校验 Lo	71	寄存器值 Lo(1)	33
CRC 校验 Hi	CB	CRC 校验 Lo	A7
		CRC 校验 Hi	9A

其中，第 1 路模拟量采集值为 0x0025，即 37(十进制)；第 2 路模拟量采集值为 0x1033，即 4147(十进制)。

(4)写单个继电器状态

请求命令：

设备地址	0x01~0xF7 (Hex)	1 字节
功能码	0x05 (Hex)	1 字节
寄存器地址	0x0000~0xFFFF (Hex)	2 字节
数值	0x0000 或 0xFF00 (Hex)	2 字节
CRC 校验	0x0000~0xFFFF (Hex)	2 字节

响应：

设备地址	0x01~0xF7 (Hex)	1 字节
功能码	0x05 (Hex)	1 字节
寄存器地址	0x0000~0xFFFF (Hex)	2 字节
数值	0x0000 或 0xFF00 (Hex)	2 字节
CRC 校验	0x0000~0xFFFF (Hex)	2 字节

异常响应：

设备地址	0x01~0xF7 (Hex)	1 字节
异常功能码	0x85 (Hex)	1 字节
异常码	01/02/03/04 (Hex)	1 字节
CRC 校验	0x0000~0xFFFF (Hex)	2 字节

示例：控制第 1 路继电器动作，使其 NO 端和 COM 端闭合，假设当前设备地址为 0x01；

请求		响应	
字段名	十六进制	字段名	十六进制
设备地址	01	设备地址	01
功能	05	功能	05
起始地址 Hi	00	起始地址 Hi	00
起始地址 Lo	00	起始地址 Lo	00
数值 Hi	FF	数值 Hi	FF
数值 Lo	00	数值 Lo	00
CRC 校验 Lo	8C	CRC 校验 Lo	8C
CRC 校验 Hi	3A	CRC 校验 Hi	3A

写入 0xFF00 表示使继电器动作；写入 0x0000 表示继电器恢复（不动作）。

(5)异常码说明

Modbus 异常码		
代码	名称	含义
01	非法功能	对于设备来说，询问中接收到的功能码是不准许的
02	非法数据地址	对于设备来说，询问中接收到的数据地址是不准许的地址。特别是寄存器编号和传输长度的组合是无效的。
03	非法数据值	对于设备来说，询问数据字段中包含的数不准许的值。它表示组合请求中剩余部分结构方面的错误，例如隐含长度不正确。它绝不表示寄存器中被提交存储的数据项有一个应用程序之外的值，因为 Modbus 协议并不知道任何特殊的寄存器的任何特殊值的具体含义。
04	从站设备故障	当设备正在试图执行所请求的操作时，产生不可恢复的差错。