1. 引言

本文档描述了KSTAR GP800 UPS Modbus协议，适用于三/单进单出UPS通讯。

本协议引用了《GBT 19582 -2008 基于Modbus协议的工业自动化网络规范》。

本文档在《GP800 modbus通讯协议V1.3》基础上修订。

2. 硬件设置

物理接口：RS232 或 RS485

波特率：2400/4800/9600 bps

起始位：1；　数据位：8；　停止位：1；　奇偶校验位:无

3. MODBUS 协议描述

3.1 Modbus 协议帧

Modbus协议帧由地址域、功能码、数据域、校验码组成。

表 3.2.1 通用 Modbus 帧

地址域	功能码	数据域	校验码

本 Modbus 协议帧采用 RTU 传输模式。

RTU报文帧包含：从机地址、功能码、数据域、CRC校验。

RTU报文帧最大为256字节，其中数据域最大长度为252字节。

表 3.2.1a RTU 报文帧

格式	从机地址	功能码	数据	CRC 校验	
字节数	1 字节	1 字节	0~252 字节	2 字节	
备注				低字节	高字节

在 RTU 模式中，时长至少为 3.5 个字符时间的空闲间隔将报文帧区分开。
必须以连续的字符流发送整个报文帧。

如果两个字符之间的空闲间隔大于 1.5 个字符时间，则认为报文帧不完整，接收端应该丢弃这个报文帧。

表 3.2.1b RTU 报文帧发送顺序

	Modbus 报文				
起始	从站地址	功能码	数据	CRC 校验	结束
≥3.5 字符时间	8 位	8 位	N*8 位	16 位	≥3.5 字符时间

3.1 Modbus 地址规则

Modbus为主从通讯模式，通讯由主机发起，对应地址的从机应答。

主机无地址，从机地址范围为：1~247；0为广播地址。

在Modbus串行总线上从机地址是唯一的。

GP800系列UPS为从机，等待MODBUS主机来查询。

3.2 CRC 校验

CRC 包含两个 8 位字节组成的一个 16 位值。
CRC 字段作为报文的最后字段附加到报文上。先低字节，后高字节（L-H）。

CRC 的计算：

1）预置 1 个 16 位的寄存器为十六进制 FFFF（即全为 1）；称此寄存器为 CRC 寄存器；
2）把第一个 8 位二进制数据（既通讯信息帧的第一个字节）与 16 位的 CRC 寄存器的低 8 位相异或，把结果放于 CRC 寄存器；
3）把 CRC 寄存器的内容右移一位（朝低位）用 0 填补最高位，并检查右移后的移出位；
4）如果移出位为 0：重复第 3 步（再次右移一位）；
如果移出位为 1：CRC 寄存器与多项式 A001（1010 0000 0000 0001）进行异或；
5）重复步骤 3 和 4，直到右移 8 次，这样整个 8 位数据全部进行了处理；
6）重复步骤 2 到步骤 5，进行通讯信息帧下一个字节的处理；
7）将该通讯信息帧所有字节按上述步骤计算完成后，得到的 16 位 CRC 寄存器的高、低字节进行交换；
8）最后得到的 CRC 寄存器内容即为：CRC 码。

3.3 功能码

表 2.5.1 仅列出本协议应用的功能码

表 3.4.1 功能码列表

序号	功能码	说明	备注
1	01H	读输出状态	本协议未涉及
2	**02H**	**读输入状态**	
3	03H	读保持寄存器	本协议未涉及
4	**04H**	**读输入寄存器**	
5	05H	写单个输出状态	本协议未涉及
6	06H	写单个寄存器	本协议未涉及
7	0FH	写多个输出状态	本协议未涉及
8	**10H**	**写多个寄存器**	
9	14H	读文件记录	本协议未涉及
10	**2BH**	**读设备识别码**	

3.4 异常码

表 3.4.1 异常码明细表

代码	说明	备注
01H	非法功能码	询问中接收到的功能码是不可允许的操作
02H	非法数据地址	询问中接收到的数据地址是不可允许的地址
03H	非法数据值	询问中包括的值是不可允许的值
06H	从属设备忙	
07H	CRC 校验错误	
08H	数据长度错误	

3.5 寄存器地址划分

本协议对寄存器地址进行了分组，有以下几种地址：1XXXX、2XXXX、3XXXX、4XXXX，分组规则见表3.5.1。

表3.5.1 存储区地址标识分组规则

寄存器地址	名称	类型	读/写	存储单元地址	功能码
1XXXX	输入状态	位	只读	10001 ~ 1XXXX	02H
2XXXX	输出寄存器	字	只写	20001 ~ 2XXXX	10H
3XXXX	输入寄存器	字	只读	30001 ~ 3XXXX	04H
4XXXX	输入寄存器	字	只读	40001 ~ 4XXXX	2BH

3.6 MODBUS 通讯

3.6.1 读取输入状态(功能码：0x02)

读取输入状态-请求

从机地址	1 字节	1~247(0xF7)
功能码	1 字节	0x02
起始地址	2 字节	0x0000~0xFFFF
输入状态数量	2 字节	1~2000(0x7D0)
CRC 校验码	2 字节	-计算-

读取输入状态-响应

从机地址	1 字节	1~247(0xF7)
功能码	1 字节	0x02
字节计数	1 字节	N *
输入状态值	N *字节	
CRC 校验码	2 字节	-计算-
* N=输出状态数量/8，若余数不为 0，则 N=N+1		

读取输入状态-错误响应

从机地址	1 字节	1~247(0xF7)
异常功能码	1 字节	0x82
异常码	1 字节	见《异常码明细表》
CRC 校验码	2 字节	-计算-

示例：请求读取输入状态

ID 号 01 从机，寄存器地址 10001~10022(0x2711~0x2726),共 22(0x16)个。

请求		响应	
字段名	十六进制	字段名	十六进制
从机地址	01	从机地址	01
功能码	02	功能码	02
起始地址 Hi	27	字节计数	03
起始地址 Lo	11	输入状态 10001~10008(8 位)	AC
输入数量 Hi	00	输入状态 10009~10016(8 位)	DB
输入数量 Lo	16	输入状态 10017~10022(6 位)	35
CRC 校验码_Lo	A3	CRC 校验码_Lo	22
CRC 校验码_Hi	75	CRC 校验码_Hi	88

	输出状态 10001~10008							
十六进制	AC							
二进制	b0	b1	b2	b3	b4	b5	b6	b7
	0	0	1	1	0	1	0	1
对应寄存器地址	10001	10002	10003	10004	10005	10006	10007	10008

	输出状态 10009~10016							
十六进制	DB							
二进制	b0	b1	b2	b3	b4	b5	b6	b7
	1	1	0	1	1	0	1	1
对应寄存器地址	10009	10010	10011	10012	10013	10014	10015	10016

	输出状态 10017~10022							
十六进制	35							
二进制	b0	b1	b2	b3	b4	b5	b6	b7
	1	0	1	0	1	1	0	0
对应寄存器地址	10017	10018	10019	10020	10021	10022	-	-

CRC 错误请求		错误响应	
字段名	**十六进制**	**字段名**	**十六进制**
从机地址	01	从机地址	01
功能码	02	异常功能码	82
起始地址 Hi	27	异常码	07
起始地址 Lo	11	CRC 校验码_Lo	60
输入数量 Hi	00	CRC 校验码_Hi	A2
输入数量 Lo	16		
CRC 校验码_Lo	A3		
CRC 校验码_Hi	77(错误)		

3.6.2 读输入寄存器(功能码：0x04)

读输入寄存器-请求

从机地址	1 字节	1~247(0xF7)
功能码	1 字节	0x04
起始地址	2 字节	0x0000~0xFFFF
输入寄存器数量	2 字节	1~125(0x7D)
CRC 校验码	2 字节	-计算-

读输入寄存器-响应

从机地址	1 字节	1~247(0xF7)
功能码	1 字节	0x04
字节计数	1 字节	2*输入寄存器数量
寄存器值	N * ×2 字节	
CRC 校验码	2 字节	-计算-
N=寄存器的数量		

读输入寄存器-错误响应

从机地址	1 字节	1~247(0xF7)
异常功能码	1 字节	0x84
异常码	1 字节	见《异常码明细表》
CRC 校验码	2 字节	-计算-

示例：请求读取输入寄存器，
ID 号 02 从机，寄存器地址 30001~30003(0x7531~0x7533),共 3(0x03)个。

请求		响应	
字段名	**十六进制**	**字段名**	**十六进制**
从机地址	02	从机地址	01
功能码	04	功能码	02
起始地址 Hi	75	字节计数	06
起始地址 Lo	31	输入寄存器 30001（Hi）	AA
输入数量 Hi	00	输入寄存器 30001（Lo）	BB
输入数量 Lo	03	输入寄存器 30002（Hi）	CC
CRC 校验码_Lo	FB	输入寄存器 30002（Lo）	DD
CRC 校验码_Hi	FB	输入寄存器 30003（Hi）	EE
		输入寄存器 30003（Lo）	FF
		CRC 校验码_Lo	BE
		CRC 校验码_Hi	22

3.6.3 读设备识别码(功能码：0x2B)*

读设备标识-请求

从机地址	1 字节	1~247(0xF7)
功能码	1 字节	0x2B
起始地址	2 字节	0x0000~0xFFFF
输入寄存器数量	2 字节	1~125(0x7D)
CRC 校验码	2 字节	-计算-

读设备标识-响应

从机地址	1 字节	1~247(0xF7)
功能码	1 字节	0x2B
字节计数	1 字节	N*
寄存器值	N* 字节	
CRC 校验码	2 字节	-计算-

读设备标识-错误响应

从机地址	1 字节	1~247(0xF7)
异常功能码	1 字节	0xAB
异常码	1 字节	见《异常码明细表》
CRC 校验码	2 字节	-计算-

示例：读设备标识,

ID 号 04 从机，寄存器地址 40001~40002(0x9C41~0x9C42),共 2(0x02)个。

请求		响应	
字段名	**十六进制**	**字段名**	**十六进制**
从机地址	04	从机地址	04
功能码	2B	功能码	2B
起始地址 Hi	9C	字节计数	06
起始地址 Lo	41	输入寄存器 40001	AA
输入数量 Hi	00	输入寄存器 40001	BB
输入数量 Lo	02	输入寄存器 40001	CC
CRC 校验码_Lo	DA	输入寄存器 40002	DD
CRC 校验码_Hi	1C	输入寄存器 40002	EE
		输入寄存器 40002	FF
		CRC 校验码_Lo	43
		CRC 校验码_Hi	00

注意：以上示例的响应数据共 6 字节，具体如何分配，根据实际定义；

3.6.4 写多个寄存器(功能码：0x10)

写多个寄存器-请求

从机地址	1 字节	1~247(0xF7)
功能码	1 字节	0x10
起始地址	2 字节	0x0000~0xFFFF
寄存器数量	2 字节	1~123（0x7B）
字节计数	1 字节	2×N
寄存器值	N×2 字节	值
CRC 校验码	2 字节	-计算-
* N=寄存器数量		

写多个寄存器-响应

从机地址	1 字节	1~247(0xF7)
功能码	1 字节	0x10
起始地址	2 字节	0x0000~0xFFFF
寄存器数量	2 字节	1~123（0x7B）
CRC 校验码	2 字节	-计算-

写多个寄存器-错误响应

从机地址	1 字节	1~247(0xF7)
异常功能码	1 字节	0x90
异常码	1 字节	见《异常码明细表》
CRC 校验码	2 字节	-计算-

例：请求写入地址
ID 号 03 从机，
写入寄存器地址 20001~20002(0x4E21~0x4E22),共 2(0x02)个，写入值分别为 AABB,CCDD

请求		响应	
字段名	**十六进制**	**字段名**	**十六进制**
从机地址	03	从机地址	03
功能码	10	功能码	10
起始地址 Hi	4E	起始地址 Hi	4E
起始地址 Lo	21	起始地址 Lo	21
寄存器数量 Hi	00	寄存器数量 Hi	00
寄存器数量 Lo	02	寄存器数量 Lo	02
字节计数	04	CRC 校验码_Lo	07
寄存器值 20001(Hi)	AA	CRC 校验码_Hi	08
寄存器值 20001(Lo)	BB		
寄存器值 20002(Hi)	CC		
寄存器值 20002(Lo)	DD		
CRC 校验码_Lo	82		
CRC 校验码_Hi	C4		

4. 协议应用

功能码应用对照表

应用内容	类型	功能码	操作	存储区地址
状态量	位	02H	只读	1XXXX
模拟量	字节	04H	读	3XXXX
设备信息	字节	2BH	读	4XXXX
测试命令	字节	10H	写	2XXXX

4.1 输入状态（地址：1XXXX）数据内容

功能码：0x02

输入状态寄存器地址	内容	类型	说明	备注
10065	UPS 内部温度高	位	1：温度过高 0：正常	
10066	电池电压状态	位	1：电池电压低 0：电池电压正常	
10067	旁路正在升压或正在降压	位	1：旁路正在升压/降压 0：旁路无升/降压	
10068	UPS 故障	位	1：UPS 故障 0：UPS 无故障	
10069	UPS 类型	位	1：离线型 0：在线型	
10070	正在测试	位	1：UPS 正在测试 0：UPS 非测试状态	
10071	正在关机或处于关机状态	位	1：UPS 正在关机或处于关机状态 0：UPS 运行	
10072	蜂鸣器状态	位	1：蜂鸣器鸣叫 0：蜂鸣器静音	
10073	旁路电压高	位	1：旁路电压过高 0：正常	
10074	旁路电压低	位	1：旁路电压过低 0：正常	
10075	旁路频率异常	位	1：旁路频率异常 0：旁路频率正常	
10076	主路电压高	位	1：主路电压过高 0：正常	

10077	主路电压低	位	1：主路电压过低 0：正常	
10078	UPS 供电状态	位	1：逆变供电 0：旁路供电	
10079	逆变器不同步	位	1：逆变器不同步 0：同步	
10080	输出过载	位	1：过载 0：正常	
10081	输出短路	位	1：短路 0：正常	
10082	输出电压异常	位	1：异常 0：正常	
10083	正常充电状态	位	1：正常充电 0：其它	
10084	电池浮充状态	位	1：电池在浮充 0：其它	
10085	电池过压	位	1：电池过压 0：正常	
10086	直流过压	位	1：直流过压 0：正常	

4.2 输入寄存器（地址：3XXXX）数据内容

功能码：0x04

输入寄存器地址	内容	大小	范围	单位	备注
30001	主路输入电压	2Byte	0~3000	0.1V	
30002	主路输入频率	2Byte	0~700	0.1Hz	
30003	旁路输入电压	2Byte	0~3000	0.1V	
30004	旁路输入频率	2Byte	0~700	0.1Hz	
30005	预留	2Byte	/	/	
30006	预留	2Byte	/	/	
30007	输出电压	2Byte	0~3000	0.1V	
30008	输出频率	2Byte	0~700	0.1Hz	
30009	当前负载率	2Byte	0~250	%	百分比表示
30010	直流输入电压	2Byte	0~270	0.01V	
30011	预留	2Byte	/	/	
30012	温度	2Byte	0~2000	0.1℃	

4.3 产品信息地址（地址：4XXXX）数据内容

功能码：0x10

产品信息地址	内容	类型	字节数	示例（ASCII）
40001	机器地址	ASCII 字符串	5	{001}
40002	厂商名称	ASCII 字符串	17	{# X0～X13} 英文 {$ X0～X13} 中文
40003	UPS 机型	ASCII 字符串	12	{Y0～Y9}
40004	软件版本	ASCII 字符串	12	{V0～V9}
40005	UPS 额定信息*	ASCII 字符串	22	{Z0～Z19}*
备注： 1、数据以 ASCII 解析 2、发送信息时，每条信息以’｛’开始，以’}’结束。 3、厂商名称:如果以$开头表示厂商为中文，如果以#开头表示厂商为英文。				

UPS 额定信息*(ASCII 格式说明)

额定输入电压	空格	额定负载	空格	额定电池电压	空格	额定频率
220.0V	space	024	space	192.0	space	50.0

4.4 输出寄存器（地址：2XXXX）数据内容(只能写)

功能码：0x2B

输出寄存器地址	内容	大小	范围
20001	控制寄存器起始地址	2Byte	0~3000

请求命令示例如下

请求		
字段名	**十六进制**	**备注**
从机地址	01	此示例为 01
功能码	2B	
起始地址 Hi	4E	20001
起始地址 Lo	21	
寄存器数量 Hi	00	寄存器数量=字节计数/2；(字节计数=偶数) 寄存器数量=（字节计数+1）/2；(字节计数=奇数)
寄存器数量 Lo	02	
字节计数	03	命令字节数 3 个 (最大 9 个)
命令数据 1	54	电池自检到电池电压低为止：TL<CR> ASCII:54 4C 0D
命令数据 2	4C	
命令数据 3	0D	
CRC 校验码_Lo	B2	
CRC 校验码_Hi	DC	

备注：

地址(20001)为起始地址,数据长度为9个数据，写入不同的字符串（ASCII 码），向 UPS 发出不同命令。

支持的命令如下：

4.4.1 电池自检命令

4.4.1.1 电池自检 10 秒：T

分组号	组 1	
字节数	1	1
内容	T	<CR>
命令	54	0D

说明：

UPS 执行动作：立即自测 10 秒种，然后恢复到正常市电状态。

如果在自测过程中发生了市电低的情况，UPS 马上恢复正常市电状态。

4.4.1.2 电池自检到电池电压低为止：TL

分组号	组 1	
字节数	2	1
内容	TL	<CR>
命令	54 4C	0D

说明：
UPS 执行动作：自测到电池低电压状态，然后恢复到正常市电状态。

4.4.1.3 电池进行指定时间自检：T<n>

分组号	组 1	组 2	
字节数	1	2	1
内容	T	自检时间	<CR>
命令	54	Num Num	0D

组 2：自检时间说明：
自检时间为小数（单位：分钟）

字节序号	2	3
内容	2EH	Num

自检时间为整数（单位：分钟）

字节序号	2	3
内容	Num	Num

说明：
UPS 进行电池自测 <n>分钟；
如果在自测过程中发生了电池低的情况，UPS 马上恢复到正常市电状态。

4.4.1.4 取消电池自检：CT

分组号	组 1	
字节数	2	1
内容	CT	<CR>
命令	43 54	0D

4.4.2 关机命令

4.4.2.1 立即关闭 UPS 输出：S

分组号	组 1	
内容	S	<CR>
命令	53	0D

4.4.2.2 在<n> 分钟后关闭 UPS 输出：S<n>

分组号	组 1	组 2	
字节数	1	2	1
内容	S	关闭延时时间	<CR>
命令	53	Num Num	0D

组 2：关闭延时时间说明：
延时时间为小数（单位：分钟）

字节序号	2	3
内容	2EH	Num

延时时间为整数（单位：分钟）

字节序号	2	3
内容	Num	Num
备注	十位	个位

说明：
1）UPS 将在<n>分钟后关闭，即使仍有市电输入。
2）如果在<n>分钟内发生了市电低，UPS 将立即关闭。
3）如果市电恢复，UPS 将在等待 10 秒种之后恢复 UPS 的输出。

4.4.2.3 取消关机指令：C

分组号	组 1	
字节数	1	1
内容	C	<CR>
命令	43	0D

说明：
UPS 执行动作：取消 S<cr>或 S<n> <cr> 指令的执行。