控制器 设备与上位机

基于 Modbus 的通信规约

1 范围

本标准规定了控制器 与上位机通信中的数据链路层配置、物理层配置、功能码类型、报文格式、数据区域分配及寄存器地址配置。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 19582.1-2008 基于Modbus协议的工业自动化网络规范第1部分：Modbus应用协议

GB/T 19582.2-2008 基于Modbus协议的工业自动化网络规范第2部分：Modbus协议在串行链路上的实现指南

3 缩略语

H	十六进制	Hex
HMI	人机界面	Human Machine Interface
ADU	应用数据单元	Application Data Unit
PDU	协议数据单元	Protocal Data Unit
CRC	循环冗余码	Cyclic Redundancy Code

4 数据链路层配置

按 GB/T 19582.2-2008 基于Modbus协议的工业自动化网络规范第2部分第6节：数据链路层，对通信数据链路层配置信息进行介绍。

4.1 寻址规则

Modbus 寻址空间由 256 个不同地址组成。Modbus 主站没有特定地址，只有从站有一个地址，在 Modbus 串行总线上，这个地址必须是唯一的。

地址 0 为广播地址，所有从站必须识别广播地址。

表 1 Modbus 寻址范围

0	1～247	248～255
广播地址	从站地址（1：默认）	保留

4.2 MODBUS 帧描述

Modbus/RTU 数据帧由地址域、功能域、数据域和错误检测域四个部分组成，如图 1 所示：

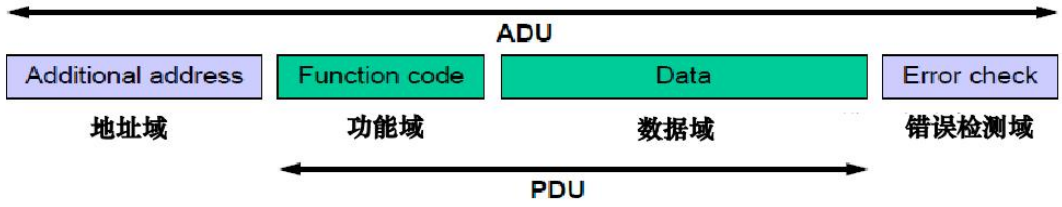

图 1 Modbus/RTU 数据帧格式

5 物理层配置

按GB/T 19582.2-2008 基于Modbus协议的工业自动化网络规范第2部分第7节：物理层，对通信物理层配置信息进行介绍。

5.1 通信接口

控制器 采用了 RS485 通信接口与上位机的通信。

5.2 数据信号传输速率

可以使用的波特率为：1200bit/s、2400bit/s、4800bit/s、9600bit/s（默认）、19200bit/s、38400bit/s。

6 功能码类型

控制器 设备与上位机通信采用标准MODBUS-RTU规约。为标准MODBUS-RTU的部分功能码及相应的说明，见表2。

表 2 功能码及相应的说明

功能码	说明
01H	读线圈状态
02H	读离散输入
03H	读保持寄存器
04H	读输入寄存器
05H	写强制单线圈
06H	写单个寄存器
0FH	写强制多线圈
10H	写多个寄存器
17H	读/写 4X 寄存器
注：读——主站读取从站信息；写——主站发设置子站信息。	

标准 MODBUS-RTU 的错误码及相应的说明，见表 3。

表 3 错误码

错误码	说明
81H（01H+80H）	读线圈状态时，发生错误
82H（02H+80H）	读离散输入时，发生错误
83H（03H+80H）	读保持寄存器时，发生错误
84H（04H+80H）	读输入寄存器时，发生错误
85H（05H+80H）	写强制单线圈时，发生错误
86H（06H+80H）	写单个寄存器时，发生错误
8FH（0FH+80H）	写强制多线圈时，发生错误
90H（10H+80H）	写多个寄存器时，发生错误
97H（17H+80H）	读/写 4X 寄存器时，发生错误
注：读——主站读取从站信息；写——主站发设置子站信息。	

标准 MODBUS-RTU 的异常码及相应的说明，见表 4。

表 4 异常码

异常码	说明	
01H	非法功能码	从站不支持请求所使用的功能码
02H	非法数据地址	数据地址不允许访问（超出了存储器的界限）
03H	非法数据值	请求报文使用了非法数据

04H	从站错误	从站处理报文错误

7 报文格式

按GB/T 19582.1-2008 基于Modbus协议的工业自动化网络规范第1部分第7节：功能码描述，对Modbus协议功能码进行介绍。

7.1 读线圈状态（01H）

读线圈状态（01H）的请求格式、响应格式、出错返回格式，分别见表 5、表 6、表 7。

表 5 主站的请求格式

主站请求		
设备地址	1 BYTE	01H（默认）
功能码	1 BYTE	01H
起始地址	2 BYTE	0000H～FFFFH
读取数量	2 BYTE	N1(1～2000)
校验码（CRC 码）	2 BYTE	0000H～FFFFH
注：N1 为读取数据的个数。		

表 6 从站的响应格式

从站响应		
设备地址	1 BYTE	01H（默认）
功能码	1 BYTE	01H
字节计数	1 BYTE	N2
读取数据	N2 BYTE	第一个数据
		：
		最后一个数据
校验码（CRC 码）	2 BYTE	0000H～FFFFH
注：N2= N1/8，如果余数不为 0，则 N2=N2+1。		

表 7 从站的出错返回格式

从站响应		
设备地址	1 BYTE	01H（默认）
功能码（错误码）	1 BYTE	81H
异常码	1 BYTE	01H/02H/03H/04H
校验码（CRC 码）	2 BYTE	0000H～FFFFH

读线圈状态（01H）的应用举例，见表 8。

表 8 读线圈状态（01H）的应用举例

主站请求		从站响应	
域名称	数据（Hex）	域名称	数据（Hex）
设备地址	01	设备地址	01
功能码	01	功能码	01

起始地址 Hi	00	字节计数	02
起始地址 Lo	01	数据 1（coils 2～9）	12
读取数量 Hi	00	数据 2（coils 10～17）	2D
读取数量 Lo	16	数据 3（coils 18～23）	1A
校验码 CRC 码 Hi	EC	校验码 Hi（CRC 码）	01
校验码 CRC 码 Lo	04	校验码 Lo（CRC 码）	2C

读线圈状态（01H）的报文实例，见本标准 11.1。

7.2 读离散输入寄存器（02H）

读离散输入寄存器（02H）的请求格式、响应格式、出错返回格式，分别见表 9、表 10、表 11。

表 9 主站的请求格式

主站请求		
设备地址	1 BYTE	01H（默认）
功能码	1 BYTE	02H
起始地址	2 BYTE	0000H～FFFFH
读取数量	2 BYTE	N1（1～2000）
校验码（CRC 码）	2 BYTE	0000H～FFFFH
注：N1 为读取数据的个数。		

表 10 从站的响应格式

从站响应		
设备地址	1 BYTE	01H（默认）
功能码	1 BYTE	02H
字节计数	1 BYTE	N
读取数据	N BYTE	第一个数据
		：
		最后一个数据
校验码（CRC 码）	2 BYTE	0000H～FFFFH
注：N= N1/8，如果余数不为 0，则 N=N+1。		

表 11 从站的出错返回格式

从站响应		
设备地址	1 BYTE	01H（默认）
功能码（错误码）	1 BYTE	82H
异常码	1 BYTE	01H/02H/03H/04H
校验码（CRC 码）	2 BYTE	0000H～FFFFH

读离散输入寄存器（02H）的应用举例，见表 12。

表 12 读离散输入寄存器（02H）的应用举例

主站请求		从站响应	
域名称	数据（Hex）	域名称	数据（Hex）
设备地址	01	设备地址	01
功能码	02	功能码	02

起始地址 Hi	00	字节计数	02
起始地址 Lo	01	数据 1（inputs 2～9）	A1
读取数量 Hi	00	数据 2（inputs 10～17）	2C
读取数量 Lo	12	数据 3（inputs 18～19）	03
校验码 Hi（CRC 码）	A9	校验码 Hi（CRC 码）	74
校验码 Lo（CRC 码）	C7	校验码 Lo（CRC 码）	91

7.3 读保持寄存器（03H）

读保持寄存器（03H）的请求格式、响应格式、出错返回格式，分别见表 13、表 14、表 15。

表 13 主站的请求格式

主站请求		
设备地址	1 BYTE	01H（默认）
功能码	1 BYTE	03H
起始地址	2 BYTE	0000H～FFFFH
读取数量	2 BYTE	N（1～125）
校验码（CRC 码）	2 BYTE	0000H～FFFFH
注：N 为读取数据个数。		

表 14 从站的响应格式

从站响应		
设备地址	1 BYTE	01H（默认）
功能码	1 BYTE	03H
字节计数	1 BYTE	N×2
读取数据	N×2 BYTE	第一个数据
		：
		最后一个数据
校验码（CRC 码）	2 BYTE	0000H～FFFFH
注：N 为读取数据个数。		

表 15 从站的出错返回格式

从站响应		
设备地址	1 BYTE	01H（默认）
功能码（错误码）	1 BYTE	83H
异常码	1 BYTE	01H/02H/03H/04H
校验码（CRC 码）	2 BYTE	0000H～FFFFH

读保持寄存器（03H）的应用举例，见表 16。

表 16 读保持寄存器（03H）的应用举例

主站请求		从站响应	
域名称	数据（Hex）	域名称	数据（Hex）
设备地址	01	设备地址	01
功能码	03	功能码	03
起始地址 Hi	00	字节计数	02

起始地址 Lo	01	输入数据 Hi	02
读取数量 Hi	00	输入数据 Lo	13
读取数量 Lo	01	校验码 Hi（CRC 码）	F8
校验码 Hi（CRC 码）	D5	校验码 Lo（CRC 码）	E9
校验码 Lo（CRC 码）	CA		

7.4 读输入寄存器（04H）

读输入寄存器（04H）的请求格式、响应格式、出错返回格式，分别见表 17、表 18、表 19。

表 17 主站的请求格式

主站请求		
设备地址	1 BYTE	01H（默认）
功能码	1 BYTE	04H
起始地址	2 BYTE	0000H～FFFFH
读取数量	2 BYTE	N（1～125）
校验码（CRC 码）	2 BYTE	0000H～FFFFH
注：N 为读取数据个数。		

表 18 从站的响应格式

从站响应		
设备地址	1 BYTE	01H（默认）
功能码	1 BYTE	04H
字节计数	1 BYTE	N×2
读取数据	N×2 BYTE	第一个数据
		：
		最后一个数据
校验码（CRC 码）	2 BYTE	0000H～FFFFH
注：N 为读取数据个数。		

表 19 从站的出错返回格式

从站响应		
设备地址	1 BYTE	01H（默认）
功能码（错误码）	1 BYTE	84H
异常码	1 BYTE	01H/02H/03H/04H
校验码（CRC 码）	2 BYTE	0000H～FFFFH

读输入寄存器（04H）的应用举例，见表 20。

表 20 读输入寄存器（04H）的应用举例

主站请求		从站响应	
域名称	数据（Hex）	域名称	数据（Hex）
设备地址	01	设备地址	01
功能码	04	功能码	04
起始地址 Hi	00	字节计数	02
起始地址 Lo	01	输入数据 Hi	01

读取数量 Hi	00	输入数据 Lo	15
读取数量 Lo	01	校验码 Hi（CRC 码）	79
校验码 Hi（CRC 码）	60	校验码 Lo（CRC 码）	6F
校验码 Lo（CRC 码）	0A		

7.5 写强制单线圈（05H）

写强制单线圈（05H）的请求格式、响应格式、出错返回格式，分别见表 21、表 22、表 23。

表 21 主站的请求格式

主站请求		
设备地址	1 BYTE	01H（默认）
功能码	1 BYTE	05H
起始地址	2 BYTE	0000H～FFFFH
设置内容	2 BYTE	0000H～FF00H
校验码（CRC 码）	2 BYTE	0000H～FFFFH

表 22 从站的响应格式

从站响应		
设备地址	1 BYTE	01H（默认）
功能码	1 BYTE	05H
起始地址	1 BYTE	0000H～FFFFH
设置内容	2 BYTE	0000H～FF00H
校验码（CRC 码）	2 BYTE	0000H～FFFFH

表 23 从站的出错返回格式

从站响应		
设备地址	1 BYTE	01H（默认）
功能码（错误码）	1 BYTE	85H
异常码	1 BYTE	01H/02H/03H/04H
校验码（CRC 码）	2 BYTE	0000H～FFFFH

写强制单线圈（05H）的应用举例，见表 24。

表 24 写强制单线圈（05H）的应用举例

主站请求		从站响应	
域名称	数据（Hex）	域名称	数据（Hex）
设备地址	01	设备地址	01
功能码	05	功能码	05
起始地址 Hi	00	起始地址 Hi	00
起始地址 Lo	01	起始地址 Lo	01
设置内容 Hi	00	设置内容 Hi	00
设置内容 Lo	00	设置内容 Lo	00
校验码 Hi（CRC 码）	9C	校验码 Hi（CRC 码）	9C
校验码 Lo（CRC 码）	0A	校验码 Lo（CRC 码）	0A

7.6 写单个保持寄存器（06H）

写单个保持寄存器（06H）的请求格式、响应格式、出错返回格式，分别见表 25、表 26、表 27。

表 25 主站的请求格式

主站请求		
设备地址	1 BYTE	01H（默认）
功能码	1 BYTE	06H
写入地址	2 BYTE	0000H～FFFFH
写入数据	2 BYTE	0000H～FFFFH
校验码（CRC 码）	2 BYTE	0000H～FFFFH

表 26 从站的响应格式

主站响应		
设备地址	1 BYTE	01H（默认）
功能码	1 BYTE	06H
写入地址	1 BYTE	0000H～FFFFH
写入数据	2 BYTE	0000H～FFFFH
校验码（CRC 码）	2 BYTE	0000H～FFFFH

表 27 从站的出错返回格式

从站响应		
设备地址	1 BYTE	01H（默认）
功能码（错误码）	1 BYTE	86H
异常码	1 BYTE	01H/02H/03H/04H
校验码（CRC 码）	2 BYTE	0000H～FFFFH

写单个保持寄存器（06H）的应用举例，见表 28。

表 28 写单个保持寄存器（06H）的应用举例

主站请求		从站响应	
域名称	数据（Hex）	域名称	数据（Hex）
设备地址	01	设备地址	01
功能码	06	功能码	06
写入地址 Hi	00	写入地址 Hi	00
写入地址 Lo	01	写入地址 Lo	01
写入数据 Hi	00	写入数据 Hi	00
写入数据 Lo	00	写入数据 Lo	00
校验码 Hi（CRC 码）	DB	校验码 Hi（CRC 码）	DB
校验码 Lo（CRC 码）	0A	校验码 Lo（CRC 码）	0A

7.7 写强制多线圈（0FH）

写强制多线圈（0FH）的请求格式、响应格式、出错返回格式，分别见表 29、表 30、表 31。

表 29 主站的请求格式

主站请求		
设备地址	1 BYTE	01H（默认）
功能码	1 BYTE	0FH
起始地址	2 BYTE	0000H～FFFFH
写入个数	2 BYTE	0000H～07B0H
字节计数	1 BYTE	N
写入数据	N BYTE	0000H～07B0H
校验码（CRC 码）	2 BYTE	0000H～FFFFH
注：N=写入线圈个数/8，如果余数不为 0，则 N=N+1。		

表 30 从站的响应格式

从站响应		
设备地址	1 BYTE	01H（默认）
功能码	1 BYTE	0FH
起始地址	2 BYTE	0000H～FFFFH
写入个数	2 BYTE	0000H～07B0H
校验码（CRC 码）	2 BYTE	0000H～FFFFH

表 31 从站的出错返回格式

从站响应		
设备地址	1 BYTE	01H（默认）
功能码（错误码）	1 BYTE	8FH
异常码	1 BYTE	01H/02H/03H/04H
校验码（CRC 码）	2 BYTE	0000H～FFFFH

写强制多线圈（0FH）的应用举例，见表 32。

表 32 写强制多线圈（0FH）的应用举例

主站请求		从站应答	
域名称	数据（Hex）	域名称	数据（Hex）
设备地址	01	设备地址	01
功能码	0F	功能码	0F
起始地址 Hi	00	起始地址 Hi	00
起始地址 Lo	01	起始地址 Lo	01
写入个数 Hi	00	写入个数 Hi	00
写入个数 Lo	01	写入个数 Lo	01
字节计数	02	校验码 Hi（CRC 码）	C5
写入数据 1Hi	02	校验码 Lo（CRC 码）	CB
写入数据 1Lo	31		
校验码 Hi（CRC 码）	26		
校验码 Lo（CRC 码）	79		

7.8 写多个保持寄存器（10H）

写多个保持寄存器（10H）的请求格式、响应格式、出错返回格式，分别见表 33、表 34、

表 35。

表 33 主站的请求格式

主站请求		
设备地址	1 BYTE	01H（默认）
功能码	1 BYTE	10H
起始地址	2 BYTE	0000H～FFFFH
写入个数	2 BYTE	N(0000H～07B0H)
字节计数	1 BYTE	N×2
写入数据	N×2 BYTE	0000H～FFFFH
校验码（CRC 码）	2 BYTE	0000H～FFFFH
注：N 为写入数据个数		

表 34 从站的响应格式

从站响应		
设备地址	1 BYTE	01H（默认）
功能码	1 BYTE	10H
起始地址	2 BYTE	0000H～FFFFH
写入个数	2 BYTE	0000H～07B0H
校验码（CRC 码）	2 BYTE	0000H～FFFFH

表 35 从站的出错返回格式

从站响应		
设备地址	1 BYTE	01H（默认）
功能码（错误码）	1 BYTE	90H
异常码	1 BYTE	01H/02H/03H/04H
校验码（CRC 码）	2 BYTE	0000H～FFFFH

写多个保持寄存器（10H）的应用举例，见表 36。

表 36 写多个保持寄存器（10H）的应用举例

主站请求		从站响应	
域名称	数据（Hex）	域名称	数据（Hex）
设备地址	01	设备地址	01
功能码	10	功能码	10
起始地址 Hi	00	起始地址 Hi	00
起始地址 Lo	01	起始地址 Lo	01
写入个数 Hi	00	写入个数 Hi	00
写入个数 Lo	01	写入个数 Lo	01
字节计数	04	校验码 Hi（CRC 码）	50
写入数据 1Hi	02	校验码 Lo（CRC 码）	09
写入数据 1Lo	31		
校验码 Hi（CRC 码）	89		
校验码 Lo（CRC 码）	D9		

7.9 读/写 4X 寄存器（17H）

读/写 4X 寄存器（17H）的请求格式、响应格式、出错返回格式，分别见表 37、表 38、表 39。

表 37 主站的请求格式

主站请求		
设备地址	1 BYTE	01H（默认）
功能码	1 BYTE	17H
起始地址（读）	2 BYTE	0000H～FFFFH
读取数量（读）	2 BYTE	N1
起始地址（写）	2 BYTE	0000H～FFFFH
写入个数（写）	2 BYTE	N2
字节计数（写）	1 BYTE	N2×2
写入数据	N2×2 BYTE	0000H～FFFFH
校验码（CRC 码）	2 BYTE	0000H～FFFFH
注：N1 为读取数据个数，N2 为写入数据个数。		

表 38 从站的响应格式

从站响应		
设备地址	1 BYTE	01H（默认）
功能码	1 BYTE	17H
字节计数	2 BYTE	N1×2
读取数据	N1×2 BYTE	0000H～FFFFH
校验码（CRC 码）	2 BYTE	0000H～FFFFH
注：N1 为读取数据个数，N2 为写入数据个数。		

表 39 从站的出错返回格式

从站响应		
设备地址	1 BYTE	01H（默认）
功能码（错误码）	1 BYTE	97H
异常码	1 BYTE	01H/02H/03H/04H
校验码（CRC 码）	2 BYTE	0000H～FFFFH

读/写 4X 寄存器（17H）的应用举例，见表 40。

表 40 功能码 17H 的请求实例

主站请求		从站响应	
域名称	数据（Hex）	域名称	数据（Hex）
设备地址	01	设备地址	01
功能码	17	功能码	17
起始地址 Hi（读）	00	字节计数 Hi	00
起始地址 Lo（读）	01	字节计数 Lo	0A
读取数量 Hi（读）	00	数据 1Hi	48
读取数量 Lo（读）	05	数据 1Lo	2D

起始地址 Hi（写）	00	数据 2Hi	36
起始地址 Lo（写）	20	数据 2Lo	74
写入个数 Hi（写）	00	数据 3Hi	A2
写入个数 Lo（写）	02	数据 3Lo	4B
字节计数（写）	04	数据 4Hi	42
写入数据 1Hi	23	数据 4Lo	89
写入数据 1Lo	3A	数据 5Hi	D0
写入数据 2Hi	12	数据 5Lo	2F
写入数据 2Lo	25	校验码（CRC 码）Hi	DB
校验码（CRC 码）Hi	6F	校验码（CRC 码）Lo	27
校验码（CRC 码）Lo	B3		

8 寄存器配置及命令（适用于共补控制器）

8.1 读取数据

主控状态的通信是上位机采用 Modbus 04H 功能码实现从控制器读取主控状态的过程。具体的主控状态寄存器地址码配置，见下表。

寄存器号	物理地址（16 进制）	寄存器类型	数据内容	精确	备注
30001	7531	R	电网电压	1	系统电压（V）
30002	7532	R	保留	1	
30003	7533	R	保留	1	
30004	7534	R	电网电流	1	电网电流(A)
30005	7535	R	保留	1	
30006	7536	R	保留	1	
30007	7537	R	有功功率	1	有功(KW)
30008	7538	R	保留	1	有功
30009	7539	R	保留	1	有功
30010	753A	R	无功功率	1	无功(KVAR)
30011	753B	R	保留	1	无功
30012	753C	R	保留	1	无功
30013	753D	R	电网功率因数	1	/100
30014	753E	R	保留	1	
30015	753F	R	保留	1	
30016	7540	R	电压总谐波（%）	1	/10

30017	7541	R	保留	1	
30018	7542	R	保留	1	
30019	7543	R	电流总谐波（%）	1	/10
30020	7544	R	保留	1	
30021	7545	R	保留	1	
30022	7546	R	温度	1	
30023	7547	R	投切状态	1	bit0-bit15，最低位对应第一路
30024	7548	R	投切状态	1	bit16-bit31（扩展）
30025	7549	R	投切状态	1	Bit32-bit47（扩展）
30026	754A	R	投切状态	1	Bit48-bit63（扩展）
30042	755A	R	CT 变比	5	
30043	755B	R	PT 变比	1	/100
30044	755C	R	过压门限	1	V
30045	755D	R	欠压门限	1	V
30046	755E	R	电压总谐波门限（%）	1	
30047	755F	R	电流总谐波门限（%）	1	
30048	7560	R	投入门限	1	/10
30049	7561	R	切除门限	1	/100
30050	7562	R	目标功率因数	1	/100
30051	7563	R	设备地址	1	
30052	7564	R	分补数量	1	
30053	7565	R	共补数量	1	
30054	7566	R	投切延时	1	N=0 时 :0S; N=1 时:0.5S; N>1 时:(N-1)S
30055	7567	R	电压回差	1	V
30056	7568	R	温度门限	1	

30057	7569	R	投切方式	1	0-逻辑投切；1-循环投切
30058	756A	R	电容系数（%）	1	
30059	756B	R	再投延时	10	S
30061	756D	R	回路1容量	1	KVar
30062	756E	R	回路2容量	1	KVar
30063	756F	R	回路3容量	1	KVar
30064	7570	R	回路4容量	1	KVar
30065	7571	R	回路5容量	1	KVar
30066	7572	R	回路6容量	1	KVar
30067	7573	R	回路7容量	1	KVar
30068	7574	R	回路8容量	1	KVar

30069	7575	R	回路9容量	1	KVar
30070	7576	R	回路10容量	1	KVar
30071	7577	R	回路11容量	1	KVar
30072	7578	R	回路12容量	1	KVar
30073	7579	R	回路13容量	1	KVar
30074	757A	R	回路14容量	1	KVar
30075	757B	R	回路15容量	1	KVar
30076	757C	R	回路16容量	1	KVar

....		R	回路 N 容量	1	KVar, 如果回路多余 16 路，地址按此数往下例推，如果没有，读到的则是无效值。

报文实例及分析

例 1：**主站发送报文：**01 04 75 3C 00 03 6A 0B

主站报文解析：

第 1 个字节，01 为设备地址；

第 2 个字节，04 为功能码；

第 3、4 个字节,75 3C 为从站的寄存器地址，表示从寄存器地址为 753CH（寄存器地址 30012）开始读取数据；

第 5、6 个字节,00 03 为主站需从从站读取的 3 个数据；

第 7、8 个字节，6A 0B 为 CRC 校验码；

从站回复报文：01 04 06 00 AA 00 AA 00 AA D8 D4

从站报文解析：

第 1 个字节，01 为设备地址；

第 2 个字节，04 为功能码；

第 3 个字节，06 为数据大小是 6 个字节；

第 4、5、6、7、8、9 个字节,00 AA 00 AA 00 AA 为主站从从站读取的 3 个数;

第 10、11 个字节，D8 D4 为 CRC 校验码。

8.2 参数修改

主控命令的通信是上位机设备采用 Modbus 06H 功能码实现下载主控命令至控制器 的过程。具体的主控命令寄存器地址码配置，见下表。

40001	9C41	W	CT 变比	5	步长 5
40002	9C42	W	PT 变比	1	/100
40003	9C43	W	过压门限	1	V
40004	9C44	W	欠压门限	1	V
40005	9C45	W	电压总谐波门限（%）	1	

40006	9C46	W	电流总谐波门限（%）	1	
40007	9C47	W	投入门限	1	/10
40008	9C48	W	切除门限	1	/100
40009	9C49	W	目标功率因数	1	/100
40010	9C4A	W	设备地址	1	
40011	9C4B	W	分补数量	1	
40012	9C4C	W	共补数量	1	
40013	9C4D	W	投切延时	1	N=0 时:0S; N=1 时:0.5S; N>1 时:(N-1)S
40014	9C4E	W	电压回差	1	V
40015	9C4F	W	温度门限	1	
40016	9C50	W	投切方式	1	0-逻辑投切；1-循环投切
40017	9C51	W	电容系数（%）	1	
40018	9C52	W	再投延时	10	步长 10
40019	9C53	W	回路1容量	1	KVar
40020	9C54	W	回路2容量	1	KVar
40021	9C55	W	回路3容量	1	KVar
40022	9C56	W	回路4容量	1	KVar
40023	9C57	W	回路5容量	1	KVar
40024	9C58	W	回路6容量	1	KVar
40025	9C59	W	回路7容量	1	KVar
40026	9C5A	W	回路8容量	1	KVar
40027	9C5B	W	回路9容量	1	KVar
40028	9C5C	W	回路10容量	1	KVar
40029	9C5D	W	回路11容量	1	KVar
40030	9C5E	W	回路12容量	1	KVar
40031	9C5F	W	回路13容量	1	KVar
40032	9C60	W	回路14容量	1	KVar

40033	9C61	W	回路15容量	1	KVar
40034	9C62	W	回路16容量	1	KVar
....		W	回路 N 容量	1	KVar,如果回路多余 16 路，地址按此数往下例推，如果没有，读到的则是无效值。

9 寄存器配置及命令（适用于分补控制器）

9.1 读取数据

主控状态的通信是上位机采用 Modbus 04H 功能码实现从控制器读取主控状态的过程。具体的主控状态寄存器地址码配置，见下表。

寄存器号	物 理 地 址（16 进制）	寄存器类型	数据内容	精确	备注
30001	7531	R	电网电压 A	1	系统电压（V）
30002	7532	R	电网电压 B	1	系统电压
30003	7533	R	电网电压 C	1	系统电压
30004	7534	R	电网电流 A	1	电网电流(A)
30005	7535	R	电网电流 B	1	电网电流
30006	7536	R	电网电流 C	1	电网电流
30007	7537	R	有功功率 A	1	有功(KW)
30008	7538	R	有功功率 B	1	有功
30009	7539	R	有功功率 C	1	有功
30010	753A	R	无功功率 A	1	无功(KVAR)
30011	753B	R	无功功率 B	1	无功
30012	753C	R	无功功率 C	1	无功
30013	753D	R	电网功率因数 A	1	/100
30014	753E	R	电网功率因数 B	1	/100
30015	753F	R	电网功率因数 C	1	/100
30016	7540	R	电网电压畸变率 A(%)	1	/10
30017	7541	R	电网电压畸变率 B(%)	1	/10

30018	7542	R	电网电压畸变率 C(%)	1	/10
30019	7543	R	电网电流畸变率 A(%)	1	/10
30020	7544	R	电网电流畸变率 B(%)	1	/10
30021	7545	R	电网电流畸变率 C(%)	1	/10
30022	7546	R	温度	1	
30023	7547	R	投切状态	1	bit0-bit15，最低位对应第一路
30024	7548	R	投切状态	1	bit16-bit31（扩展）
30025	7549	R	投切状态	1	Bit32-bit47（扩展）
30026	754A	R	投切状态	1	Bit48-bit63（扩展）
30042	755A	R	CT 变比	5	
30043	755B	R	PT 变比	1	/100
30044	755C	R	过压门限	1	V
30045	755D	R	欠压门限	1	V
30046	755E	R	电压谐波门限(%)	1	
30047	755F	R	电流谐波门限(%)	1	
30048	7560	R	投入门限	1	/10
30049	7561	R	切除门限	1	/100
30050	7562	R	目标功率因数	1	/100
30051	7563	R	设备地址	1	
30052	7564	R	分补数量	1	
30053	7565	R	共补数量	1	
30054	7566	R	投切延时	1	N=0 时 :0S; N=1 时:0.5S; N>1 时:(N-1)S
30055	7567	R	电压回差	1	V
30056	7568	R	温度门限	1	
30057	7569	R	投切方式	1	0-逻辑投切；1-循环投切
30058	756A	R	电容系数	1	%

30059	756B	R	再投延时	10	S
30061	756D	R	回路1容量	1	KVar
30062	756E	R	回路2容量	1	KVar
30063	756F	R	回路3容量	1	KVar
30064	7570	R	回路4容量	1	KVar
30065	7571	R	回路5容量	1	KVar
30066	7572	R	回路6容量	1	KVar
30067	7573	R	回路7容量	1	KVar
30068	7574	R	回路8容量	1	KVar
30069	7575	R	回路9容量	1	KVar
30070	7576	R	回路10容量	1	KVar
30071	7577	R	回路11容量	1	KVar
30072	7578	R	回路12容量	1	KVar
30073	7579	R	回路13容量	1	KVar
30074	757A	R	回路14容量	1	KVar
30075	757B	R	回路15容量	1	KVar
30076	757C	R	回路16容量	1	KVar
....		R	回路 N 容量	1	KVar,如果回路多余16路，地址按此数往下例推，如果没有，读到的则是无效值。

报文实例及分析

例 1：**主站发送报文：**01 04 75 3C 00 03 6A 0B

主站报文解析：

第 1 个字节，01 为设备地址；

第 2 个字节，04 为功能码；

第 3、4 个字节,75 3C 为从站的寄存器地址，表示从寄存器地址为 753CH（寄存器地址 30012）开始读取数据；

第 5、6 个字节,00 03 为主站需从从站读取的 3 个数据；

第 7、8 个字节，6A 0B 为 CRC 校验码；

从站回复报文：01 04 06 00 AA 00 AA 00 AA D8 D4

从站报文解析：

第 1 个字节，01 为设备地址；

第 2 个字节，04 为功能码；

第 3 个字节，06 为数据大小是 6 个字节；

第 4、5、6、7、8、9 个字节,00 AA 00 AA 00 AA 为主站从从站读取的 3 个数;

第 10、11 个字节，D8 D4 为 CRC 校验码。

9.2 参数修改

主控命令的通信是上位机设备采用 Modbus 06H 功能码实现下载主控命令至控制器 的过程。具体的主控命令寄存器地址码配置，见下表。

40001	9C41	W	CT 变比	5	步长 5
40002	9C42	W	PT 变比	1	/100
40003	9C43	W	过压门限	1	V
40004	9C44	W	欠压门限	1	V
40005	9C45	W	电压谐波门限	1	
40006	9C46	W	电流谐波门限	1	
40007	9C47	W	投入门限	1	/10
40008	9C48	W	切除门限	1	/100
40009	9C49	W	目标功率因数	1	/100
40010	9C4A	W	设备地址	1	
40011	9C4B	W	分补数量	1	
40012	9C4C	W	共补数量	1	
40013	9C4D	W	投切延时	1	N=0 时:0S; N=1 时:0.5S; N>1 时:(N-1)S
40014	9C4E	W	电压回差	1	V
40015	9C4F	W	温度门限	1	
40016	9C50	W	投切方式	1	0-逻辑投切；1-循环投切
40017	9C51	W	电容系数（%）	1	
40018	9C52	W	再投延时	10	步长 10
40019	9C53	W	回路1容量	1	KVar

40020	9C54	W	回路2容量	1	KVar
40021	9C55	W	回路3容量	1	KVar
40022	9C56	W	回路4容量	1	KVar
40023	9C57	W	回路5容量	1	KVar
40024	9C58	W	回路6容量	1	KVar
40025	9C59	W	回路7容量	1	KVar
40026	9C5A	W	回路8容量	1	KVar
40027	9C5B	W	回路9容量	1	KVar
40028	9C5C	W	回路10容量	1	KVar
40029	9C5D	W	回路11容量	1	KVar
40030	9C5E	W	回路12容量	1	KVar
40031	9C5F	W	回路13容量	1	KVar
40032	9C60	W	回路14容量	1	KVar
40033	9C61	W	回路15容量	1	KVar
40034	9C62	W	回路16容量	1	KVar
....		W	回路 N 容量	1	KVar,如果回路多余 16 路，地址按此数往下例推，如果没有，读到的则是无效值。