

P900F 通用型控制器系列

MODBUS 协议(I)

1、协议概述

1.1、协议类型 Modbus RTU 协议

本协议适用于 PAN-GLOBE E900 系列通讯仪表

本协议规定仪表和上位机的数据交换模式。

采用异步主从半双工方式通讯，上位机做主站，仪表做从站，有上位机发询问信息，仪表做相应应答。

1.2、物理层

传输接口：RS485

通讯地址：1~247（一个网络上最多挂 128 个站）

波特率：9600、19200

通讯介质：屏蔽双绞线

1.3、数据链路层

采用 8 位二进制，每个代码由两个十六进制字符表示。帧格式是：1 个起始位，8 个数据位，没有校验位，2 个停止位。

一个数据包的格式是：(表：1)

地址	功能码	数据码	CRC 校验码
8bits	8bits	n*8bits	16bits

功能码定义：(表：2)

代码	功能定义
03H	读取一个或多个寄存器的数值
10H	写多个寄存器的数值
06H	写一个寄存器的数值

注：1 个寄存器占 2 个字节

1.4、CRC 校验算法

生成一个 CRC 的流程是：

先将一个 16 位寄存器(CRC 寄存器)置为 0FFFFH。

把数据包中的第一个 8 位字节与 CRC 中的低位字节进行异或运算，结果存回 CRC 寄存器。

将 CRC 向右移一位，最高位填'0'，最低位移出并检测。

如果移出位为'0'，重复第 3 步。

如果移出位为'1'，将 CRC 寄存器与一个预设的固定值(0A001H)进行异或运算。

重复步骤 3 和步骤 4，直到 8 次移位结束，这样就处理好了一个完整的 8 位字节。

重复步骤 2 到步骤 5 处理下一个 8 位字节，直到所有字节全部处理结束。

最终 CRC 寄存器的值就是 CRC 值。

2、应用层功能详解

应用层功能详解的目的是定义特定有效命令的通用格式。

软件程序员可以使用下述方法，以便通过协议正确的建立特定的应用程序。

通讯协议使用下述的格式(表： 3)

地址	功能码	地址高字节	地址低字节	数据高字节	数据低字节	CRC 低字节	CRC 高字节
01	03	00	10	00	02	C5	CE

2.1、PC 读数据（功能码 03）

此功能允许主站读取从站采集到的或记录的数据及仪表的系统参数。

主站查询时的数据包格式如下范例。

PC 读数据范例：地址为 01H，SV 地址为 00H(表： 4)

地址	功能码	地址高字节	地址低字节	数据高字节	数据低字节	CRC 低字节	CRC 高字节
01	03	00	00	00	02	C4	0B

从站响应：(表： 5)

地址	功能码	变量总字节数	变量植高字节	变量值低字节	变量值高字节	变量值低字节	CRC 低字节	CRC 高字节
01	03	04	02	BC	00	00	3A	6F

2.2、预置多寄存器（功能码 10H）

此功能允许主站改写从站 3 字节变量值。(已转换为 2 字节定点数，负数为 4 字节补码形式)

PC 写数据范例：写 SV(表： 6)

地址	功能码	地址高字节	地址低字节	变量个数高字节	变量个数低字节	变量总字节数	变量值高字节	变量值低字节	变量值高字节	变量值低字节	CRC 低字节	CRC 高字节
01	10	00	00	00	02	04	03	E8	00	00	73	DF

从机返回：(表： 7)

地址	功能码	地址高字节	地址低字节	变量个数高字节	变量个数低字节	CRC 低字节	CRC 高字节
01	10	00	00	00	02	41	C8

预置单寄存器（功能码 06H）

此功能允许主站改写从站单字节变量值。由于每次发送按双字节寄存器发送，所以，高位补 0。

PC 写数据范例，写 CYT(表： 8)

地址	功能码	地址高字节	地址低字节	变量值高字节	变量值低字节	CRC 低字节	CRC 高字节
01	06	00	23	00	09	B8	06

从机返回：(表：9)

地址	功能码	地址高字节	地址低字节	变量值高字节	变量值低字节	CRC 低字节	CRC 高字节
01	06	00	23	00	09	B8	06

参数地址分配

参数	地址	十进制地址	长度(BYTE)	读写性质
SV	00H	0	4	R/W
AT	03H	3	1	R/W
AL1	04H	4	4	R/W
AL2	08H	8	4	R/W
AL3	0CH	12	4	R/W
ADD	6AH	106	1	R/W
P	10H	16	4	R/W
I	14H	20	4	R/W
D	18H	24	4	R/W
OUD	1BH	27	1	R/W
HYS	1CH	28	4	R/W
CYT	1FH	31	1	R/W
HY1	20H	32	4	R/W
AD1	23H	35	1	R/W
HY2	24H	36	4	R/W
AD2	27H	39	1	R/W
HY3	28H	40	4	R/W
AD3	2BH	43	1	R/W
OUL	2CH	44	4	R/W
OUH	30H	48	4	R/W
TH	34H	52	1	R/W
INP	36H	54	1	R/W
LSP	38H	56	4	R/W
USP	3CH	60	4	R/W
CF	48H	72	1	R/W
SFT	49H	73	1	R/W
DP	4AH	74	1	R/W
BRL	5CH	92	4	R/W
BRH	60H	96	4	R/W
PVOS	64H	100	4	R/W
TOP	6CH	108	4	R/W
U0	70H	112	4	R/W
TOSV	74H	116	1	R/W
INP2	76H	118	1	R/W
LSP2	78H	120	4	R/W
USP2	7CH	124	4	R/W
PVS2	80H	128	4	R/W

M/A	5DH	93	1	R/W
MV	5EH	94	4	R/W
PV1	C3H	195	4	R

注:

- 1、写 MV 前请先写 00H 到 M/A，使系统转为手动控制状态
写 40H 到 M/A 可使系统转为自动控制状态