HT 系列定时器 MODBUS 通讯协议

一、协议概述

1、协议类型　Modbus RTU 协议

本协议适用于 YOTO HT 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，若有上位机发询问信息，仪表做相应应答

2、 物理层

传输接口：RS485

通讯地址：1～99……（一个网络上最多挂 128 个站）

通讯介质：屏蔽双绞线

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。采用异步主从半双工方式。

帧格式是：1 个起始位，8 个数据位，1 个停止位，无校验位。

一个数据包的格式是：

从机地址	功能码	数据码	CRC 校验码
8bit	8bit	n*8bit	16bit

功能码定义：

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

4、 CRC 校验算法

生成一个 CRC 流程是：

（1）先将一个 16 位寄存器（CRC 寄存器）预置为 0FFFFH；

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

（3）将 CRC 寄存器右移一位，最高位填“0”，最低位移出并检测；

（4）如果移出位为“0”，重复第（3）步，如果移出位为“1”，将 CRC 寄存器与一个固定值（0A001H）进行异或运算；

（5）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 8 位字节；

（6）重复步骤（2）到步骤（5）处理下一个 8 位字节，直到所有字节处理结束；

（7）最终 CRC 寄存器的值就是 CRC 值

二、应用层功能祥解

应用层功能祥解的目的是定义特定有效命令的通用格式。程序员可以使用下述方法，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：

从机地址	功能码	地址高字节	地址低字节	数据个数高字节	数据个数低字节	CRC 高字节	CRC 低字节
01	03	00	B0	00	02	C5	EC

1、主机读数据（功能码 03H）

此功能允许主站读取从站采集到的或记录的数据及从站的系统参数，主站的发送数据包如下范例：

从机地址	功能码	地址高字节	地址低字节	数据个数高字节	数据个数低字节	CRC 高字节	CRC 低字节
01	03	00	B6	00	02	25	ED

从站响应的数据包如下：

从机地址	功能码	数据总字节数	数据高字节	数据低字节	数据高字节	数据低字节	CRC 高字节	CRC 低字节
01	03	04	23	45	00	01	21	A2

2、主机向从机写多个寄存器（功能码10H）

此功能允许主站改写从站4字节变量值，变量值从高字节到低字节排序为DATA4、DATA3、DATA2、DATA1,则发送顺序为DATA2、DATA1、DATA4、DATA3，即先发送低寄存器，再发送高寄存器，如下范例：

从机地址	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	DATA2	DATA1	DATA4	DATA3	CRC高字节	CRC低字节
01	10	00	B6	00	02	04	23	45	00	01	A3	60

从站响应的数据包如下：

从机地址	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高字节	CRC低字节
01	10	00	B6	00	02	A0	2E

3、主机向从机写1个寄存器（功能码06H）

此功能允许主站改写从站1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，如下范例：

从机地址	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高字节	CRC低字节
01	06	00	D0	00	55	48	0C

从站响应的数据包如下：

从机地址	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高字节	CRC低字节
01	06	00	D0	00	55	48	0C

仪表可读与参数一览表：

参数地址	参数类型	数据长度	数据类型	数据范围	备注
B0H-B3H	PV(只读)	4	BCD(10进制)	0.00-99999	计时PV值
B4H-B5H	FLAG1(只读)	2	HEX(16进制)	参看以下B5H定义	输出报警
B6H-B9H	SV2 (可读写)	4	BCD(10进制)	0.00-9999.9	HI报警设定值
BAH-BDH	SV1(可读写)	4	BCD(10进制)	0.00-9999.9	LO报警设定值
BEH-BFH	RAN(可读写)	2	HEX(16进制)	参看以下BFH定义	定时范围设定
C0H-C1H	OUT(可读写)	2	HEX(16进制)	参看以下C1H定义	HI输出方式设定
C2H-C3H	TDAN(可读写)	2	HEX(16进制)	参看以下C3H定义	延时单位设定
C4H-C7H	DKEY2(可读写)	4	BCD(10进制)	000.00-999.99	HI延时设定
C8H-CBH	DKEY1(可读写)	4	BCD(10进制)	000.00-999.99	LO延时设定
CCH-CDH	LOM(可读写)	2	HEX(16进制)	参看以下CDH定义	LO输出方式设定
CEH-CFH	CTLBIT(可读写)	2	HEX(16进制)	参看以下CFH定义	功能位设定
D0H-D1H	LCK(可读写)	2	BCD(10进制)	0000-9999	按键密码设定

FLAG1(B5H)输出报警定义：

数据位	置位(1)	复位(0)
D0	HI报警	HI未报警
D1	未定义	未定义
D2	LO报警	LO未报警
D3	未定义	未定义
D4	未定义	未定义
D5	未定义	未定义
D6	未定义	未定义
D7	未定义	未定义

RAN(BFH)定时范围定义：

数值	定义
01	0-9999.9S
02	0-999.99S
04	0-9999.9M
08	0-999.99M
10	0-9999.9H
20	0-999.99H
40	0-9H59M59S
80	0-9M59S.99

OUT(C1H)报警模式定义：

数值	定义
01	F报警模式
02	N报警模式
04	R报警模式
08	C报警模式

TDAN(C3H)延时单位定义：

数值	定义
01	延时值以秒为单位
02	延时值以分单位
04	延时值以小时单位

LOM(CdH)延时单位定义：

数值	定义
01	DHOL方式
02	DOFF方式
04	DTIM方式

CTLBIT(CFH)状态标志定义：

数据位	置位(1)功能	复位(0)功能
D0	有掉电保持	无掉电保持
D1	上电CP1触发计时	上电CP1短接计时
D2	未定义	未定义
D3	未定义	未定义
D4	未定义	未定义
D5	未定义	未定义
D6	未定义	未定义
D7	未定义	未定义