一、协议概述

1.1 协议类型：

Modbus-RTU 协议

本协议适用于 KST45-2 型智能控制器。

本协议旨在规定终端设备（智能控制器）与总线接口单元（上位机）之间的数据交换以 Modbus 的 RTU（Remote Terminal Unit）模式进行。

采用异步主从半双工方式通讯，总线接口单元（上位机）作为主站，终端设备（智能控制器）作为从站进行工作。由主站发起询问（发起通讯），从站在接到主站请求后作相应的应答。

注：智能控制器响应查询信号的时间为 0.1～0.5 秒（典型值为 0.2 秒）。

1.2 物理层

1.2.1 传输接口：RS-485

1.2.2 通讯地址：1～247（一个网络上最多可挂 128 个站）

1.2.3 通讯波特率：9600 bps 或 19200 bps

1.2.4 通讯介质：屏蔽双绞线

1.3 数据链路层

1.3.1 代码系统： 8-bit 二进制，十六进制数 0…9，A…F。 数据包中每个 8-bit 域都是由两个十六进制字符组成。

1.3.2 传输方式： 异步主从半双工方式。

1.3.3 一个数据帧格式： 1 位起始位，8 位数据，1 位停止位。

1.3.4 一个数据包格式：

地址 Address	功能码 Function	数据 Data	校验码 CRC
8-Bits	8-Bits	N*8-Bits	16-Bits

注：数据包的发送序列总是相同的 — 地址、功能码、数据和与其相应校验码。每个数据包必须作为一个连续的位流传输。

当数据包到达终端设备后，则会进入到相应地址的终端设备（从站）中，该从站自动去掉数据包的“信封” （数据头），读取数据并进行校验；如果没有错误，就执行数据包所请求的任务。然后，它将自己生成的数据加入到取得的“信封”中，把包返回给主站。从站返回的响应数据包中含有了以下内容：从站地址（Address）、被执行了的功能（Function）、执行功能后生成的被请求数据（Data）和一个校验码（CRC） 。发生任何错误都不会有成功的响应。

1.3.4.1 地址（Address）域

地址域在数据包的开始部份，由一个 8 bits 数据组成；这个数据标明主站指定的终端设备（从站）地址。而每一个终端设备（从站）地址必须是唯一的，有效的终端设备（从站）地址在 1～247 的范围内。当主站发送数据包后，只有与主站查询地址相同的终端设备（从站）才会有响应。

1.3.4.2 功能（Function）域

功能域代码告诉被寻址到的终端设备（从站）执行何种功能。表 1-1 列出了所有的功能码及它们的意义。

表 1-1

代码	意 义	实 现 功 能
03H	读数据	读取一个或多个变量的当前二进制值
06H	预置单寄存器	用一个特定的二进制值改写一个变量的值
10H	预置多寄存器	用特定的二进制值改写多个变量的值

1.3.4.4　数据（Data）域

数据域包含有终端设备（从站）执行特定功能所需要的数据或者终端设备（从站）响应查询时采集到的数据。这些数据的内容可能是数值、地址或者极限值等。

1.3.4.4 校验码（CRC）域

校验码域包含主站或从站在 CRC 校验传送数据时形成的 16 bits 校验码值。 由于电噪声和其它干扰，一组数据从一个设备传输到另一个设备时在线路上可能会发生一些改变,CRC 校验能够保证主站或者从站不去响应那些传输过程中发生了改变的数据，这就提高了系统的安全性和效率。

1.4　CRC 校验方法

CRC 值由传送设备计算出来，然后附加到数据包上传送；接收设备在接收数据时重新计算 CRC 值，然后与接收到的校验码（CRC）域中的值进行比较；如果这两个值不相等，就说明数据在传输过程中发生了错误。

CRC 运算时，首先将一个 16 bits 的寄存器预置为全 1，然后连续把数据包中的 8 bits 字节与该寄存器的当前值进行运算。 仅仅每个字节的 8 个数据位参与生成 CRC，起始位和终止位以及可能使用的奇偶位都不影响 CRC。

在生成 CRC 值时，每个 8 bits 字节与寄存器中的内容进行异或，然后将结果向低位移位，高位则用“0”补充；最低位（LSB）移出并检测，如果是“1” ，该寄存器就与一个预设的固定值进行一次异或运算，如果是“0” ，不作任何外理。

上述处理重复进行，直到执行完 8 次移位操作为止。当最后一位（第 7 位）移完以后，下一个 8 bits 字节与寄存器的当前值进行异或运算，同样进行上述的另一个 8 次移位异或操作，当数据包中的所有字节都作了处理，生成的最终值就是 CRC 值。

生成一个 CRC 值的流程为：

1、先将一个 16 bits 寄存器（称之为 CRC 寄存器）置为 0FFFFH（全 1） 。

2、把数据包中的第一个 8 bits 字节与 CRC 寄存器中的低字节进行异或运　　算，结果存回到 CRC 寄存器。

3、将 CRC 寄存器向右移一位，最高位填以“0” ，最低位移出并检测。

4、如果移出位为“0” ：重复第 3 步（下一次移位） 。 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。

5、重复第 3 步和第 4 步直到 8 次移位结束，这样就处理好了一个完整的 8 bits 字节。

6、重复第 2 步到第 5 步来处理下一个 8 bits 字节，直到所有的字节全部处理结束。

7、最终 CRC 寄存器的值就是 CRC 值。

二、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。在每条数据查询格式说明的后面有一个该数据查询所执行功能的解释和一个例子。

协议概述中已经简述了通讯协议和数据包；软件程序员可以使用下述的方法，以便通过协议正确的建立它们特定应用程序。

通讯协议应使用如表 2-1 所示的格式（数字为 16 位进制）。

表 2-1　通讯协议格式范例表

地址	功能码	变量起始地址高字节	变量起始地址低字节	变量的个数高字节	变量的个数低字节	校验码低字节	校验码高字节
03H	03H	00H	01H	00H	03H	55H	E9H

2.1 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 KST45 型智能控制器的系统参数。

主站查询时数据包格式 ：

如下范例（表 2-2）是读取 03 号从站的 3 个采集到的基本数据 Ua、Ub、Uc 的查询数据包；Ua 的地址为 0001H、Ub 的地址为 0002H、Uc 的地址为 0003H。

表 2-2 读取 Ua、Ub 和 Uc 的查询数据包范例

地址	功能码	变量起始地址低字节	变量起始地址高字节	变量的个数高字节	变量的个数低字节	校验码低字节	校验码高字节
03H	03H	00H	01H	00H	03H	55H	E9H

从站响应后数据包格式：

从站响应数据包中含有从站地址、功能码、数据的数量、响应的数据和 CRC 校验码。

如下范例（表 2-3）是读取 Ua，Ub，Uc 的从站响应数据包。

表 2-3 读取 Ua，Ub，Uc 的从站响应数据包范例

地址	功能码	变量的总字节数	变量值高字节	变量值低字节	变量值高字节	变量值低字节	变量值高字节	变量值低字节	校验码低字节	校验码高字节
03H	03H	06H	01H	7CH	01H	7DH	01H	7CH	F9H	9BH

2.2 多寄存器（功能码 10H）

此功能允许主站改写从站多个变量的值。主站可以在任何时刻自从站的任何可读/写变量开始连续改写从站最多 16 个变量的值。

主站查询时数据包格式 ：

如下范例（表 2-4）是修改 3 号从站的负载监控 1 和负载监控 2 的动作电流及延时时间整定值的查询数据包；其中负载监控 1 的动作电流整定值地址为 2AH，延时时间的整定值为 2BH，负载监控 2 的动作电流整定值地址为 2CH，延时时间的整定值为 2DH。

表 2-4 修改负载监控 1 和负载监控 2
动作电流及延时时间整定值的查询数据包范例

地址	功能码	变量起始地址高字节	变量起始地址低字节	变量的个数高字节	变量的个数低字节	变量的总字节数	变量值高字节	变量值低字节	变量值高字节	变量值低字节	变量值高字节	变量值低字节	变量值高字节	变量值低字节	校验码低字节	校验码高字节
03H	10 H	00 H	2A H	00 H	04 H	08H	07 H	D0H	00H	0AH	07H	D0 H	00H	0AH	25H	7CH

从站响应后数据包格式 ：

从站响应数据包含有从站地址、功能码、数据的起始地址、数据的数量和 CRC 校验码。

如下范例（表 2-5）是修改负载监控 1 和负载监控 2 动作电流及延时时间整定值的从站响应数据包。

表 2-5 修改负载监控 1 和负载监控 2
动作电流及延时时间整定值的从站响应数据包范例

地址	功能码	变量起始地址高字节	变量起始地址低字节	变量的个数高字节	变量的个数低字节	校验码低字节	校验码高字节
03H	10H	00H	2AH	00H	04H	EBH	8DH

2.3 预置单寄存器（功能码 06H）

此功能允许主站改写从站一个变量的值。主站可以在任何时刻自从站的任何可读/写变量开始改写从站一个变量的值。

主站查询时数据包格式 ：

如下范例（表 2-6）是修改 03 号从站过载长延时电流整定值 Ir1 的查询数据包。Ir1 地是 002EH。

表 2-6 修改过载长延时电流整定值 Ir1 的查询数据包范例

地址	功能码	变量起始地址高字节	变量起始地址低字节	变量高字节	变量低字节	校验码低字节	校验码高字节
03H	06H	00H	2EH	07H	0D0H	EBH	8DH

从站响应后数据包格式:

对于此功能查询的正常响应是在变量的值改变以后将接收到的数据传送回去。

如下范例（表 2-7）是修改过载长延时电流整定值 Ir1 的从站响应数据包。

表 2-7 修改过载长延时电流整定值 Ir1 的从站响应数据包范例

地址	功能码	变量起始地址高字节	变量起始地址低字节	变量高字节	变量低字节	校验码低字节	校验码高字节
03H	06H	00H	2EH	07H	0DH	EBH	8DH

三、变量地址分配

地址	变量代号	变量名称	变量类型	单位	读写性质	变量格式
系统参数						
00H	Device_Code	设备识别号	R		00H	Device_Code
电网参数						
01H	Ua	A 相电压	Int	V	R	×1
02H	Ub	B 相电压	Int	V	R	
03H	Uc	C 相电压	Int	V	R	
04H	COS	功率因数	Int		R	/100
05H	Hz	频率	Int	Hz	R	
6H	kW_L（低字）	功率	Int	kW	R	/100
07H	kW_H（高字）		Int	kW	R	
08H	Ia	A 相电流	Int	A	R	×1 或×2 注 1
09H	Ib	B 相电流	Int	A	R	
0AH	Ic	C 相电流	Int	A	R	
0BH	In	N 相电流	Int	A	R	
0CH	Ig	接地电流	Int	A	R	
0DH	IMBa	A 相不平衡率	Int		R	/100
0EH	IMBb	B 相不平衡率	Int		R	
0FH	IMBc	C 相不平衡率	Int		R	
电网故障记录数据						
10H	Fault_L1	A 相电流	Int	A	R	×1 或×2 注 1
11H	Fault_L2	B 相电流	Int	A	R	
12H	Fault_L3	C 相电流	Int	A	R	
13H	Fault_Ln	N 相电流	Int	A	R	

14H	Fault_Ig	接地漏电电流	Int	A	R	
15H	Fault_IMBa	A 相不平衡率	Int		R	/100
16H	Fault_IMBb	B 相不平衡率	Int		R	
17H	Fault_IMBc	C 相不平衡率	Int		R	
18H	Fault_TL（低字）	故障延时时间	Int	s	R	/50
19H	Fault_TH（高字）		Int	s	R	
1AH	Fault_I	故障电流	Int	A	R	×1 或×2 注 1
1BH	Fault_Style	故障类别	Int		R	见 4.1
设备诊断信息及电网状态信息						
1CH	Self_Check	自诊断信息	Int		R	见 4.2
1DH	Circuit_Check	电网状态信息	Int		R	见 4.3
保护整定值及系统参数设置						
28H	输出触点 1 功能 输出触点 2 功能				R/W	见 4.4
29H	输出触点 3 功能 输出触点 4 功能				R/W	
2AH	IC1	负载 1 整定值	Int	A	R/W	×1 或×2 注 1
2BH	TC1	负载 1 整定时间	Int	s	R/W	见 4.9.1
2CH	IC2	负载 2 整定值	Int	A	R/W	×1 或×2 注 1
2DH	TC2	负载 2 整定时间	Int	s	R/W	见 4.9.1
2EH	Ir1	长延时整定值	Int	A	R/W	×1 或×2 注 1
2FH	TL	长延时整定时间	Int	A	R/W	见 4.9.1
30H	Ir21	短延时反时限整定值	Int	A	R/W	×1 或×2 注 1
31H	Ir22	短延时定时限 整定值	Int	A	R/W	
32H	TS	短延时定时限 整定时间	Int	s	R/W	见 4.9.4
33H	Ir4	接地漏电整定值	Int	A	R/W	×1 或×2 注 1
34H	TG	接地漏电 整定时间	Int	s	R/W	见 4.9.2
35H	KG	接地反时限系数	Int		R/W	见 4.9.3
36H	Ir3	瞬时整定值	Int	A	R/W	×1 或×2 注 1
37H	IMB	不平衡率整定值	Int		R/W	百分数
38H	TB	不平衡整定时间	Int	s	R/W	见 4.9.2
39H	ON_OFF	系统功能开关	Int		R/W	见 4.5
3AH	Type_Curve	保护曲线类型	Int		R/W	见 4.6
3BH	Rated_I	额定电流	Int	A	R/W	见 4.8
3CH	Rated_Igmi	接地互感器额定电流	Int		R/W	
3DH	Model	断路器型号	Int		R/W	见 4.10
3EH	Product_Code_L（低字）	产品出厂编号	Int		R/W	

3FH	Product_Code_H（高字）		Int		R/W	
40H	Product_Date_L（低字）	生产日期	Int		R/W	见 4.11
41H	Product_Date_H（高字）		Int		R/W	
42H	Address	通讯地址	Int		R/W	
43H	Size	框架等级	Int		R/W	见 4.7
系统时钟						
44H	Minute_Second	分，秒	BCD 码		R/W	见 4.12
45H	Day_Hour	日，时	BCD 码		R/W	
46H	Year_Month	年，月	BCD 码		R/W	
47H	Contactor_Wear	触头磨损率	Int		R/W	/100
4AH	Operated_Num	操作次数	Int		R/W	/10
4CH	Ctrl_order	分合闸指令—动令	Int		W	FF00 分闸 00FF 合闸 见 4.13
4DH	Pre_Ctrl_order	分合闸指令—预令	Int		W	
电网故障发生日期						
4EH	Minute_Second	分，秒	BCD 码		R/W	见 4.12
4FH	Day_Hour	日，时	BCD 码		R/W	
50H	Year_Month	年，月	BCD 码		R/W	

注 1：当额定电流 Rated_I 的值小于 9 时传输格式为×1，否则传输格式×2。

四、变量格式说明

4.1 故障类别变量（Fault_Style）：

bit：0	1	2	3	4	5	6	7	8-15
瞬时 故障	接地 故障	不平衡 故障	未定义	短延时 故障	长延时 故障	负载监控 1 故障	负载监控 2 故障	未定义

4.2 自诊断信息变量（Self_Check）：

bit：0	1	2	3	4	5	6	7
	执行元 件断线						
bit：8	9	10	11	12	13	14	15
		触头磨 损严重	断路器 拒动	A/D 转 换出错	E2PROM 出错	超温	

4.3 电网状态信息变量（Circuit_Check）：

bit：0	1	2	3	4	5	6	7
电压报警	温度报警	短延时 报警	过载 报警	负载监控 1 报警	负载监控 2 报警	不平衡报警	接地 报警
bit：8	9	10	11	12	13	14	15

锁状态：设置	锁状态：本地	锁状态：远程	断路器状态： 0：分闸 1：合闸	设备 自诊断信息	电网 有报警信息	电网故障信息未读取	故障跳闸

注：锁状态是三种互斥的，也即只有其中一种状态为“1”。

4.4 触点功能的编程：

变量地址与输出触点编号的对应关系如下：

变量 28H 的低字节 —— 输出触点 1

变量 28H 的高字节 —— 输出触点 2

变量 29H 的低字节 —— 输出触点 3

变量 29H 的高字节 —— 输出触点 4

输出触点的可编程功能码及其含义如下：

00----未定义　　01----瞬时故障跳闸报警

02----接地漏电故障跳闸报警　　03----不平衡故障跳闸报警

04----短延时故障跳闸报警　　05----长延时故障跳闸报警

06----故障跳闸报警　　07----负载监控 1 卸载输出

08----负载监控 2 卸载输出　　09----自诊断报警

10----电网故障状态报警

4.5 系统功能开关变量（ON_OFF）：

bit：0	1	2	3	4	5	6	7
长延时热记忆 1：关闭 0：打开	短延时热记忆 1：关闭 0：打开	负载监控方式 1：方式 1 0：方式 2	断路器极数选择 1：4 极 0：3 极	漏电互感器类别 1：5A 0：1A	控制器类型 1：H 型 0：M 型	保护类型 1：配电用 0：发电用	N 相设置 1：100% 0：50%
bit：8	9	10	11	12	13	14	15
接地、漏电选择 1：接地方式 0：漏电方式	控制指令已获取	通讯波特率 1：19.2k 0：9.6k	面板键整定功能锁定 1：锁定 0：未锁	通讯协议类型 1：Modbus-RTU 0： Profibus-DP or Device_Net	电网类型 1:三相三线制 0:三相四线制	电压等级： 1:140V 0:690V 及以下	功率因数符号 1：负号 0：正号

4.6 保护曲线类型变量（Type_Curve）：

变量值	含义
0	曲线 1：标准反时限
1	曲线 2：快速反时限
2	曲线 3：特快反时限（一般配电用）
3	曲线 4：特快反时限（电机保护用）
4	曲线 5：高压熔丝兼容
5	曲线 6：特快反时限 2（一般配电保护用）

4.7 架等级变量（Size）：

变量值	1	2	3
框架等级	框 I	框 II	框 III
额定电流 变量范围	0≤Rated_I≤8	9≤Rated_I≤15	16≤Rated_I≤20

4.8 额定电流变量（Rated_I）：

变量值	0	1	2	3	4	5	6	7	8	9	10
额定 电流值	250	400	630	800	1000	1250	1600	1900	2000	2000	2500
变量值	11	12	13	14	15	16	17	18	19	20	
额定 电流值	2900	3150	3200	3900	4000	4000	4900	5000	5900	6300	

4.9 动作时间变量值与实值对照

4.9.1 过载保护和负载监控的时间对照表

过载保护和负载监控的时间对照表

变量值	动作时间实值（s）					
	对应 2 倍整定值的动作时间					对应 1.5 倍整定值的动作时间
	标准 反时限 曲线 1	快速 反时限 曲线 2	特快 反时限 一般用途 曲线 3	特快 反时限 马达保护 曲线 4	高压熔丝 兼容 曲线 5	特快 反时限 一般用途 曲线 6
0	0.36	1.00	3.32	2.94	0.66	15
1	0.58	1.60	5.32	4.72	1.06	20
2	0.86	2.40	8.00	7.06	1.60	25
3	1.42	4.00	13.32	11.78	2.66	30
4	2.14	6.00	20.00	17.68	4.00	40
5	2.86	8.00	26.66	23.58	5.32	50
6	3.58	10.00	33.30	29.46	6.66	60
7	5.36	13.50	45.00	39.78	9.00	80
8	6.44	18.00	60.00	53.04	12.00	100
9	10.02	28.00	93.32	82.52	18.66	120
10	14.32	40.00	133	117	26.66	160
11	21.48	60.00	200	176	40.00	200
12	28.64	80.00	266	235	53.32	240
13	35.80	100	333	294	66.66	320
14	42.98	120	400	353	80.00	400
15	50.14	140	433	383	86.66	480

4.9.2 不平衡和接地漏电定时限保护的时间对照表

变量值	0	1	2	3	4	5	6	7	8	9	10
时间值	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0	OFF

4.9.3 接地反时限系数对照表

变量值	0	1	2	3	4	5	6	7	8	9	10
时间值	1.5	2	2.5	3	3.5	4	4.5	5	5.5	6	OFF

4.9.4 短延时定时限整定时间对照表

变量值	0	1	2	3	4	5	6	7	8	9
时间值	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0

4.10 断路器型号变量值与实值对照表

变量值	0	1	2	3	4	5	6	7	8
实值	DW40	DW45	DW48	DW15	DW17	DW18	DW914	DW30	DW19

4.11 生产日期格式

Product_Date_L：YEAR = 0～99（低字节），MONTH = 1～12（高字节）；

Product_Date_H：DAY = 1～31（低字节）

4.12 系统时钟格式

Minute_Second：MINUTE = 0～59（高字节），SECOND = 0～59（低字节）

Day_Hour： DAY = 1～31（高字节），HOUR = 0～23（低字节）

Year_Month： YEAR = 0～99（高字节），MONTH = 1～12（低字节）

注：数据传输必须用 BCD 码。

4.13 遥控操作格式

遥控只能通过 06 功能传输，必须先发预令；当控制器已接收到预令后，再发动令才会有响应。控制器接收到预令后，“控制命令已获取”位为 0 。