FAQ-4393

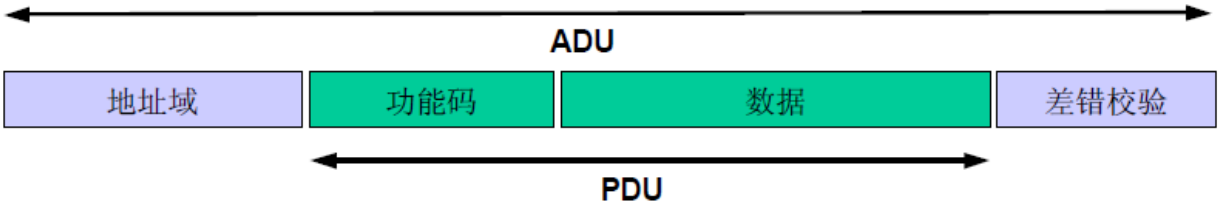
Question:

Siemens保护装置Modbus通讯协议的配置注意事项以及报文解析。

Answer:

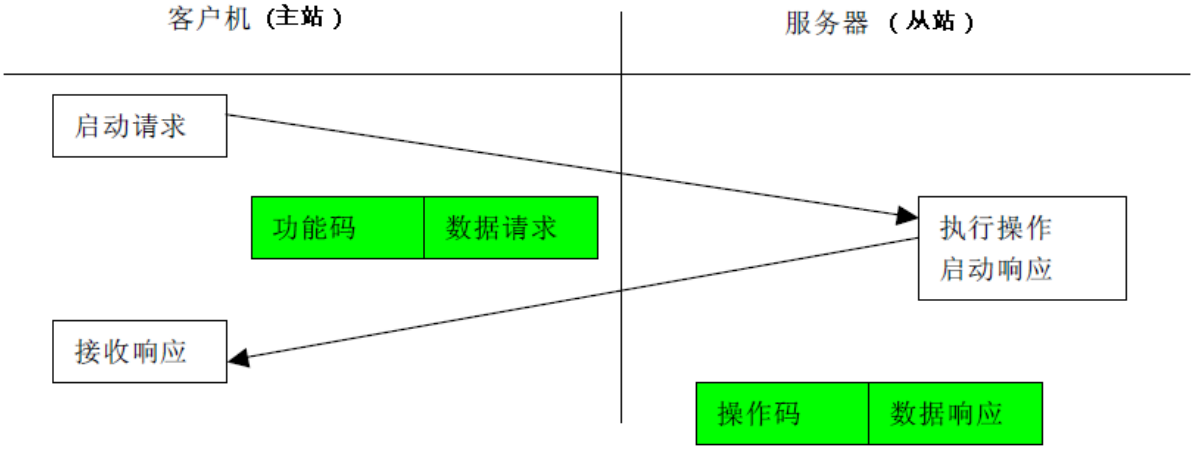
Modbus 协议简介：

MODBUS 协议定义了一个与基础通信层无关的简单协议数据单元（PDU）。特定总线或网络上的MODBUS 协议映射能够在应用数据单元（ADU）上引入一些附加域。



通用 MODBUS 帧

Modbus使用的是主站询问，从站回答的数据传送方式。



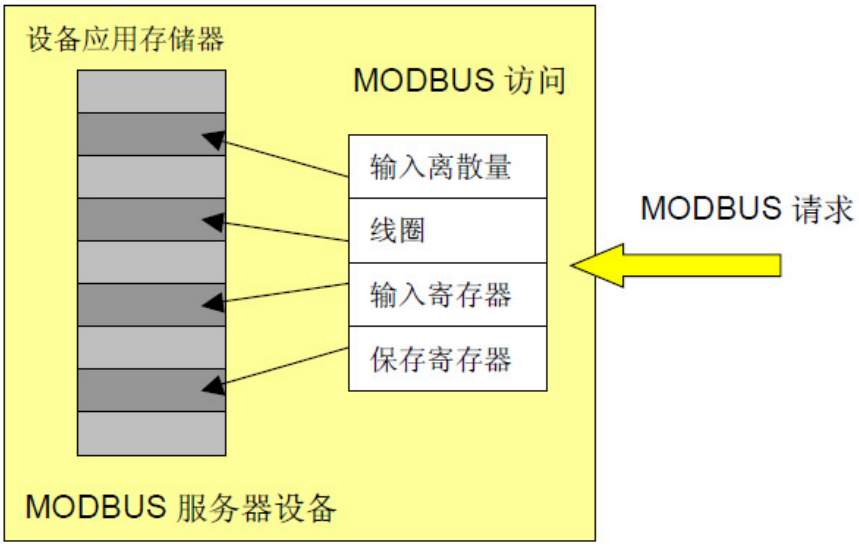
MODBUS 事务处理（无差错）

Modbus 数据模型：

MODBUS 以一系列具有不同特征表格上的数据模型为基础。四个基本表格为：

基本表格	数据对象	访问类型	内容
离散量输入	单个比特	只读	I/O系统提供这种类型数据
线圈	单个比特	读写	通过应用程序改变这种类型数据
输入寄存器	16-比特字	只读	I/O系统提供这种类型数据
保持寄存器	16-比特字	读写	通过应用程序改变这种类型数据

下例示出了设备中的数据结构，这个设备含有数字量和模拟量、输入量和输出量。由于不同块中的数据不相关，每个块是相互独立。按不同MODBUS 功能码访问每个块。



带有独立块的 MODBUS 数据模型

				Date	2012-05-06	**FAQ-4393**
				Drawn	Chen Shou Jiang	
				Appr.	PLM-Name	
				SIEMENS IC SG EA SPA CC		Sheet
1A	third edition	2012-12-05	chen shoujiang	Infrastructure & Cities Sector	I_04393_NKG	2 / 10
Rev.	Description	Date	Name			

Modbus 公共功能码定义：

				功能码		
				码	子码	（十六进制）
数据访问	比特访问	物理离散量输入	读输入离散量	02		02
		内部比特或物理线圈	读线圈	01		01
			写单个线圈	05		05
			写多个线圈	15		0F
	16 比特访问	输入存储器	读输入寄存器	04		04
		内部存储器或物理输出存储器	读多个寄存器	03		03
			写单个寄存器	06		06
			写多个寄存器	16		10
			读/写多个寄存器	23		17
			屏蔽写寄存器	22		16
	文件记录访问		读文件记录	20	6	14
			写文件记录	21	6	15
封装接口			读设备识别码	43	14	2B

Siemens保护的Modbus配置以及报文示例

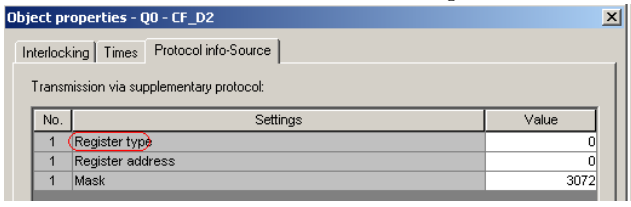
概述：

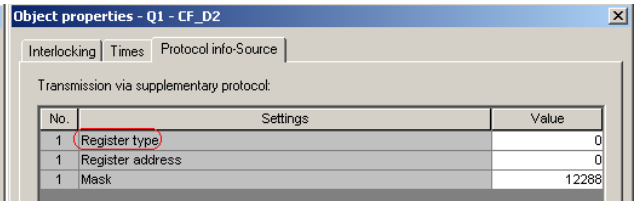
信息类型，寄存器类型，功能码之间的对应关系

信息类型	DIGSI中配置的寄存器类型（register type）	Modbus功能码
双遥控（CF_D2）	0	15
双遥信（DP）	0	01
单遥控（C_S）	0	05
单遥信（SP）	1	02
遥测量（MV）	3	04
电度量（MVMV）	4	03

1 双遥控带双遥信的信号（CF_D2）

a) 配置：双遥控及双遥信信息属于线圈状态类型（coil），在DIGSI中配置在寄存器类型0的范围（可用的地址可以在相应装置的modbus mapping file描述中找到），且遥信与遥控方向地址相同，如下图Q0，Q1





b） 如何从DIGSI配置中换算出Modbus协议中的寄存器号。

寄存器号 Y = Register address + 1 + x， 其中 mask = $2^x + 2^{x+1}$

以上图Q0为例：mask 3072 = 1024 + 2048 = $2^{10} + 2^{11}$， 所以 x = 10

Q0的寄存器号 Y = 0 + 1 + 10 = 11

同理 Q1：mask 12288 = 4096 + 8192 = $2^{12} + 2^{13}$， 所以 x = 12

Q1的寄存器号 Y = 0 + 1 + 12 = 13

c） 示例报文

由于Modbus报文查询是从0开始寻址的，所以报文中的地址比计算的寄存器号小1。

双遥控（写多个线圈）功能码：15

遥控Q0报文

主站发送		
28	地址	
0F	功能码	
00	起始地址 Hi	报文中地址为10，比寄存器号小1.
0A	起始地址 Lo	
00	输出数量 Hi	
02	输出数量 Lo	
01	输出字节数	
01	输出值（01：合闸，02：分闸）	
45	CRC（Lo）	
24	CRC（Hi）	

从站返回	
28	地址
0F	功能码
00	起始地址 Hi
0A	起始地址 Lo
00	输出数量 Hi
02	输出数量 Lo
F3	CRC（Lo）
F1	CRC（Hi）

双遥信（读取多个线圈状态）功能码：01

读取Q0位置报文

主站发送		
28	地址	
01	功能码	
00	起始地址 Hi	报文中地址为10，比寄存器号小1.
0A	起始地址 Lo	
00	输出数量 Hi	
02	输出数量 Lo	
9A	CRC（Lo）	
30	CRC（Hi）	

从站返回	
28	地址
01	功能码
01	字节数
01	输出值（01：合闸，02 分闸）
98	CRC（Lo）
14	CRC（Hi）

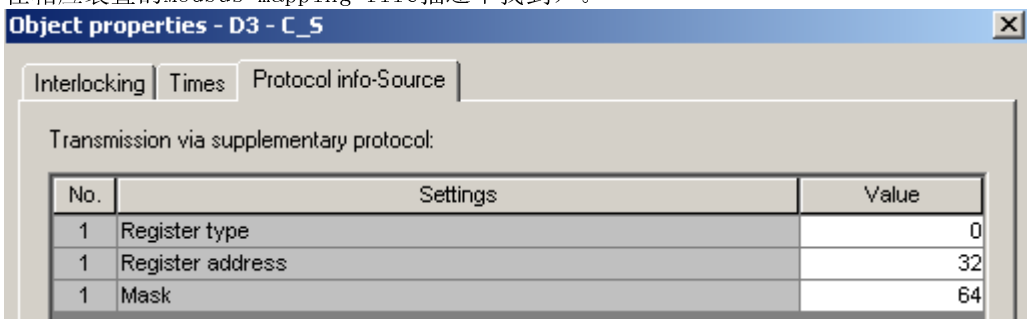
同时读取Q0，Q1位置的报文

主站发送		
28	地址	
01	功能码	
00	起始地址 Hi	报文中地址为10，比寄存器号小1.
0A	起始地址 Lo	
00	输出数量 Hi	
04	输出数量 Lo	
1A	CRC（Lo）	
32	CRC（Hi）	

从站返回	
28	地址
01	功能码
01	字节数
09	输出值（Q0合闸，Q1分闸）
99	CRC（Lo）
D2	CRC（Hi）

2 单遥控信号（C_S）

a) 配置：单遥控信息同样属于线圈类型（coil），在DIGSI中配置在寄存器类型0的范围（可用的地址可以在相应装置的Modbus mapping file描述中找到）。



b) 如何从DIGSI配置中换算出Modbus协议中的寄存器号。

寄存器号 Y = Register address + 1 + Log_2^{mask}

上图中寄存器号 Y = 32 + 1 + Log_2^{64} = 39

c) 示例报文

由于Modbus报文查询是从0开始寻址的，所以报文中的地址比计算的寄存器号小1。

单遥控（写单个线圈）功能码：05

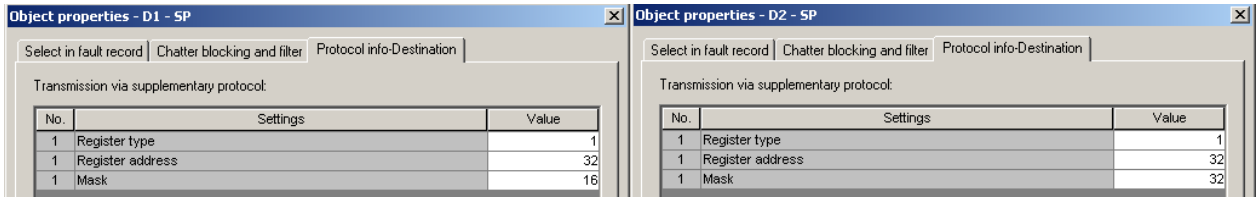
单遥控报文

主站发送				从站返回	
28	地址			28	地址
05	功能码			05	功能码
00	起始地址 Hi	报文中地址为38，		00	起始地址 Hi
26	起始地址 Lo	比寄存器号小1.		26	起始地址 Lo
FF	输出值 Hi	FF 00 为合闸命令		FF	输出值 Hi
00	输出值 Lo	00 00 为分闸命令		00	输出值 Lo
6A	CRC（Lo）			6A	CRC（Lo）
08	CRC（Hi）			08	CRC（Hi）

注意：对于脉冲型输出的单遥控命令，后台发送分闸命令是没有实际意义的，保护装置会拒绝分闸命令，拒绝的附加原因是不合常理（Plausibility error）。

3 单遥信信号（SP）

a) 配置：单遥信信息属于离散量类型，在DIGSI中配置在寄存器类型1的范围。



b) 如何从DIGSI配置中换算出Modbus协议中的寄存器号。

寄存器号 Y = Register address + 1 + Log_2^{mask}

上图中寄存器号分别为 Y = 32 + 1 + Log_2^{16} = 37，Y = 32 + 1 + Log_2^{32} = 38

c) 示例报文

由于Modbus报文查询是从0开始寻址的，所以报文中的地址比计算的寄存器号小1。

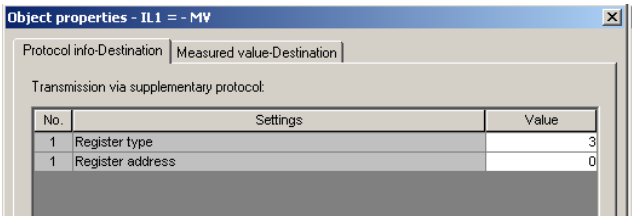
单遥信（读离散量）功能码：02

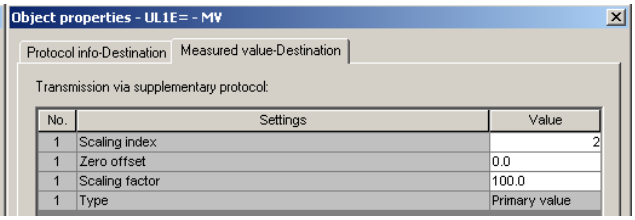
以下是同时读取遥信1与遥信2的报文

主站发送				从站返回	
28	地址			28	地址
02	功能码			02	功能码
00	起始地址 Hi	报文中地址为36，比寄存器号小1		01	字节数
24	起始地址 Lo			02	遥信状态（遥信1：off，遥信2：on）
00	输出数量 Hi			28	CRC（Lo）
02	输出数量 Lo			15	CRC（Hi）
BE	CRC（Lo）				
39	CRC（Hi）				

4 遥测值

a) 配置：遥测值属于输入寄存器类型，DIGSI中配置在寄存器类型3的范围。装置中未给遥测值预留多余地址，如果有用户自定义的遥测值需要配置到后台，则需要把部分默认的遥测值从系统口移除。





b) 如何从DIGSI配置中换算出Modbus协议中的寄存器号。

寄存器号 Y = Register address + 1

上图中 Ia 寄存器号 Y = 0 + 1 = 1，其它模拟量寄存器号可在mapping file描述中查找到。

c) 示例报文

由于Modbus报文查询是从0开始寻址的，所以报文中的地址比计算的寄存器号小1。

遥测（读输入寄存器）功能码：04

下例中是7SJ62 mapping file 3-1，从寄存器号1开始，读取18个寄存器的报文，不同类型装置的寄存器代表的数据内容有所差异，请参考相关装置的mapping file。

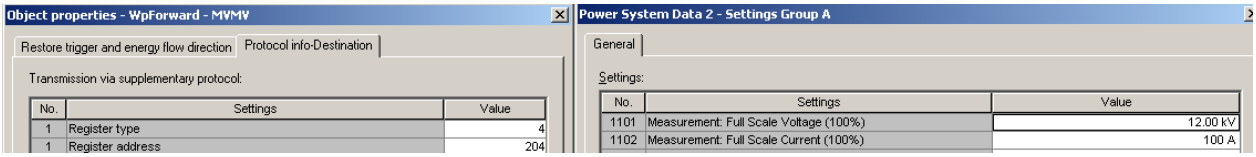
主站发送			从站返回		
28	地址		28	地址	
04	功能码		04	功能码	
00	起始地址 Hi	报文中地址为0，比寄存器号小1	24	字节数	
00	起始地址 Lo		00	输入寄存器1 Hi	Ia
00	输出数量 Hi		00	输入寄存器1 Lo	
12	输出数量 Lo		00	输入寄存器2 Hi	Ib
77	CRC（Lo）		00	输入寄存器2 Lo	
FE	CRC（Hi）		00	输入寄存器3 Hi	Ic
			00	输入寄存器3 Lo	
			00	输入寄存器4 Hi	In
			00	输入寄存器4 Lo	
			02	输入寄存器5 Hi	Va
			42	输入寄存器5 Lo	

			02	输入寄存器6 Hi	Vb
			3C	输入寄存器6 Lo	
			02	输入寄存器7 Hi	Vc
			3C	输入寄存器7 Lo	
			03	输入寄存器8 Hi	Vab
			E4	输入寄存器8 Lo	
			03	输入寄存器9 Hi	Vbc
			E0	输入寄存器9 Lo	
			03	输入寄存器10 Hi	Vca
			E4	输入寄存器10 Lo	
			00	输入寄存器11 Hi	Vn
			00	输入寄存器11 Lo	
			00	输入寄存器12 Hi	P
			00	输入寄存器12 Lo	
			00	输入寄存器13 Hi	Q
			00	输入寄存器13 Lo	
			00	输入寄存器14 Hi	S
			00	输入寄存器14 Lo	
			13	输入寄存器15 Hi	F
			80	输入寄存器15 Lo	
			00	输入寄存器16 Hi	Ins real
			00	输入寄存器16 Lo	
			00	输入寄存器17 Hi	Ins reac
			00	输入寄存器17 Lo	
			80	输入寄存器18 Hi	PF
			00	输入寄存器18 Lo	
			51	CRC（Lo）	
			D7	CRC（Hi）	

遥测值是有符号16位数，数值范围是 -32768 到 +32767，数值 -32768 = Hex8000表示无效值或越限值，输入寄存器5为Va，Hex0242 = 578，除系数100（a配置部分示例图）得到一次值5.78kV。

5 电度量

a) 配置：电度量属于保持寄存器类型，每个电度量占用两个寄存器，DIGSI中配置在寄存器类型4的范围。



b) 如何从DIGSI配置中换算出Modbus协议中的寄存器号。
寄存器号 Y = Register address + 1
上图中 WpForward 寄存器号 Y = 204 + 1 = 205，其它电度量寄存器号可在mapping file描述中查找到。

c) 示例报文
由于Modbus报文查询是从0开始寻址的，所以报文中的地址比计算的寄存器号小1。
遥测（读输入寄存器）功能码：03
下例中从寄存器号205开始，读取4个电度量的报文。

主站发送				从站返回		
28	地址			28	地址	
03	功能码			03	功能码	
00	起始地址 Hi	报文中地址为204，比寄存器号小1		10	字节数	
CC	起始地址 Lo			00	寄存器205 Hi	WpForward
00	输出数量 Hi			DC	寄存器205 Lo	
08	输出数量 Lo			3C	寄存器206 Hi	
83	CRC（Lo）			43	寄存器206 Lo	
CA	CRC（Hi）			01	寄存器207 Hi	WqForward
				08	寄存器207 Lo	
				48	寄存器208 Hi	
				51	寄存器208 Lo	
				01	寄存器209 Hi	WpReverse
				34	寄存器209 Lo	
				54	寄存器210 Hi	
				5E	寄存器210 Lo	
				01	寄存器211 Hi	WqReverse
				60	寄存器211 Lo	
				60	寄存器212 Hi	
				6C	寄存器212 Lo	
				37	CRC（Lo）	
				B2	CRC（Hi）	

电度量是无符号32位数，数值范围是0 to +4294967295。保护装置通过协议上送到主站是电度量的脉冲个数，所以后台收到脉冲数目后还要乘以系数（即每个脉冲代表的电度量值）才能得到与装置上显示相同的电度量值。

系数（即每个脉冲代表的电度量值）与保护参数1101和1102（a配置部分示例图）相关，系数公式为

1.732 * 参数1101 * 参数1102/60000

本例中的系数为 1.732 * 12000 * 100/60000 = 34.64 WH

WpForward的脉冲数目为 Hex00DC3C43 = 14433347, WpForward的电度量为 14433347*34.64/1000000 = 499.971 MWH.

				Date	2012-05-06	FAQ-4393	
				Drawn	Chen Shou Jiang		
				Appr.	PLM-Name		
				SIEMENS IC SG EA SPA CC			Sheet
1A	third edition	2012-12-05	chen shoujiang	Infrastructure & Cities Sector		I_04393_NKG	9 / 10
Rev.	Description	Date	Name				

1 Warnings

WARNING

Dangerous voltages may occur in devices and modules during operation depending on the design and application. Incorrect use of these devices can therefore result in severe personal injury or substantial damage to property.

Only suitably qualified staff should work on this device.

Correct and safe operation of this device is dependent on proper handling, installation, operation and maintenance.

Should you require further information, or should particular problems occur which are not handled in sufficient depth in the Instructions, help can be requested through your local Siemens Office or representative.

QUALIFIED PERSON

A "qualified person" is one who is familiar with the installation, construction and operation of the device and who has the appropriate qualifications, e.g.

- is trained and authorized to operate and maintain devices/systems in accordance with established safety practices for devices with electrical circuits.
- is trained in the proper care and use of protective equipment in accordance with established safety practices.
- is trained in first aid.

Subject to change without prior notice !