

# 电能质量监测终端

## Modbus 应用层协议

TN01010101 V1.10 Date:2017/02/06

工程技术笔记

类别	内容
关键词	电能质量、Modbus
摘要	电能质量监测终端与上位机软件数据通信时采用 Modbus 通信协议进行实时监测和管理

## 修订历史

版本	日期	原因
V1.00	2017/01/05	创建文档
V1.10	2017/02/06	调整说明实例等

# 目 录

1. 基本概念.....	1
2. 帧格式.....	2
3. 地址.....	3
4. 功能码.....	4
5. 功能码描述.....	5
5.1    (0x01) 读告警状态信息.....	5
5.1.1    请求命令说明.....	5
5.1.2    响应命令说明.....	5
5.1.3    交互流程.....	6
5.2    (0x03) 读系统参数.....	6
5.2.1    请求命令说明.....	7
5.2.2    响应命令说明.....	7
5.2.3    交互流程.....	8
5.3    (0x04) 读实时数据.....	8
5.3.1    请求命令信息.....	9
5.3.2    响应命令说明.....	10
5.3.3    交互流程.....	11
6. 异常响应.....	12
7. 数据校验.....	14

## 1. 基本概述

本协议定义了 E8300 电能质量监测系统中设备与后台软件的通讯规则，遵循标准 Modbus 通信接口，并针对电能质量数据的特点对通信规则进行了重新定义。

- 协议 Modbus 基于 RS-485 硬件接口，是一个主从格式的总线协议，一个总线上最多可以挂接 248 个设备，只允许一个主站，其余 247 个站点是从站。E8300 设备在该总线上作为从站。
- 所有会话逻辑采用“主站请求→从站回应”的逻辑方式。
- 在通信过程中采用“big-Endian”模式传输数据。
- 本协议采用 RTU 模式，并根据电能质量数据的特点在标准的 Modbus 上作了调整，重新定义了请求的数据个数和帧边界。

RTU 模式的串口通信参数如下：

- **波特率**：界面可选，可选值有 19200、38400、56000、57600、115200；
- **数据位**：固定 8 位；
- **停止位**：固定 1 位；
- **奇偶校验位**：固定偶校验；
- **协议地址**：界面可设，范围 1-247；

## 2. 帧格式

帧格式如下所示：

地址域	功能码	数据	差错校验
-----	-----	----	------

帧内容解释表如表 2-1 所示。

表 2-1 帧内容解释表

帧数据项	长度 (byte)	描述
地址域	1	发送这一数据帧的目的地址 (0x01~0xF7)
功能码	1	功能码
数据	N	具体数据
差错校验	2	使用 CRC16，校验区域从源地址开始，一直到数据区结尾

### 3. 地址

地址指主站发送数据到从站时地址域为：0x01~0xF7，0x00 为总线广播地址。

## 4. 功能码

E8300 支持如下功能码：

功能码	对象类型	访问类型	功能描述
0x01	单个比特	读	读告警状态
0x03	32 比特位	读	读系统参数
0x04	32 比特位	读	读实时数据

## 5. 功能码描述

### 5.1 (0x01) 读告警状态信息

该命令用于获取设备当前的告警信息状态值。

#### 5.1.1 请求命令说明

功能码	起始地址高位	起始地址低位	数据高位	数据低位	校验和 CRC
0x01	0xN0	0xnn	0xnn	0xnn	0xnmmm

请求命令中指定了请求的线圈起始地址和线圈数量，起始地址的前 4 位值 N 表示请求板卡编号为 N 的数据，N 可取 0-5。起始地址的后 12 位值指定了线圈数据的起始地址，从 0 开始编号，每个线圈地址对应的具体告警信息条目如下表 5-1 所示。

表 5-1 线圈地址对应告警列表

地址	内容
0	频率上偏差告警
1	频率下偏差告警
2	电压上偏差告警
3	电压下偏差告警
4	短闪变超限告警
5	长闪变超限告警
6	电压波动超限告警
7	电压负序不平衡度超限告警
8	电流负序不平衡度超限告警
9	电压总畸变率超限告警
10	奇次谐波电压超限告警
11	偶次谐波电压超限告警
12~60	2-50 次谐波电压超限告警序列
61~109	2-50 次谐波电流超限告警序列
110	终端上电
111	终端掉电

#### 5.1.2 响应命令说明

正常的响应命令帧如下描述：

功能码	字节数	线圈状态	CRC 数据校验
0x01	N* (1 字节)	N*字节	0xnmmm

注：N\*=请求线圈数量/8，如果余数不等于 0，那么□N\* = N\* + 1

相应命令帧线圈状态部分的返回所请求的线圈的状态，每个比特对应一个线圈地址的所对应的告警的状态，1 表示处于告警状态，0 表示正常状态。

数据部分按照字节为单位填充数据，首先返回起始地址开始的 8 个线圈状态，字节内部先发送线圈高地址的告警状态，后发送线圈低地址的告警状态。如果请求的线圈数量不是 8 的倍数，将用零填充最后数据字节中的剩余比特（一直到字节的高位端）。

如下为一个请求板卡 1 线圈 20~38 的状态信息实例：



请求		响应	
域名	(十六进制)	域名	(十六进制)
功能	01	功能	01
起始地址 Hi	00	字节数	03
起始地址 Lo	13	输出寄存器 27-20	CD
输出数量 Hi	00	输出寄存器 35-28	6B
输出数量 Lo	13	输出寄存器 38-36	05

将线圈 27-20（地址为 26-19）的状态表示为十六进制字节值 CD，因此直接传输二进制 1100 1101，第 8 位对应线圈 27 的状态，第 8 位对应线圈 20 的状态。

线圈 35-28 的状态表示为十六进制的 6B。

线圈 38-36 的状态为 101，因不满 8 位，需要先用 0 填充这一字节的高位部分，即先传输 5 个 0，后传输线圈 38-36 状态 101，最终传输的值为 0x05。

### 5.1.3 交互流程

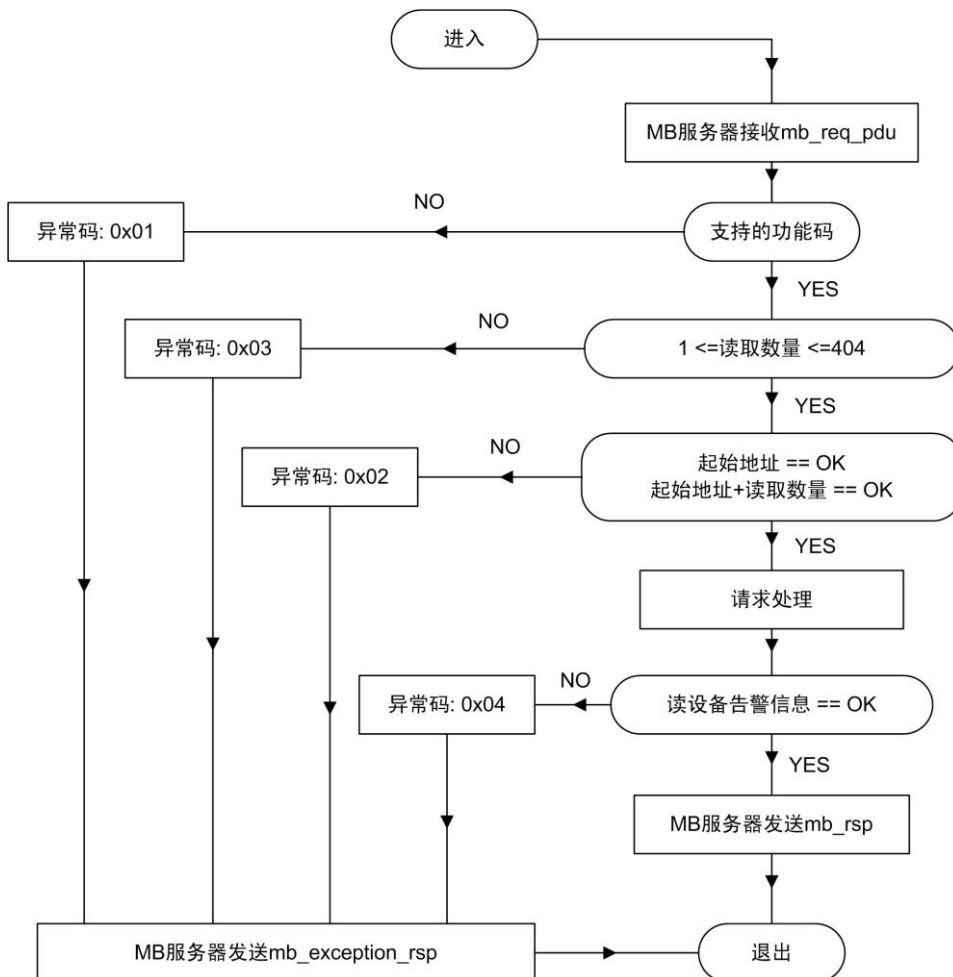


图 5.1 读告警信息状态图

## 5.2 (0x03) 读系统参数

该命令可获取设备系统参数的信息。

### 5.2.1 请求命令说明

功能码	起始地址高位	起始地址低位	寄存器个数高位	寄存器个数低位	校验和 CRC
0x03	0xN0	0xnn	0xnn	0xnn	0xnnnn

请求命令中指定了请求的寄存器起始地址和寄存器数量，起始地址的前 4 位值 N 表示请求板卡编号为 N 的数据，N 可取 0-5。起始地址的后 12 位值指定了数据的起始地址，从 0 开始编号，每个寄存器地址对应的具体的系统参数如下表 5-2 所示。

Modbus 串口 RTU 每帧只能传送 250 字节的数据内容，每个系统参数都需要 2 个寄存器才能表示，所以请求系统参数的报文中的寄存器个数最多为 124 (250/4\*2)，代表一次最多只能传送 62 (124/2) 个系统参数。

表 5-2 寄存器地址对应系统参数项列表

地址	内容	值单位	值类型
0	电压互感系数	无	浮点数
2	电流互感系数	无	浮点数
4	电压等级	V	浮点数
6	标称电压	V	浮点数
8	额定电流	A	浮点数
10	统计间隔	min	有符号整数
12	统计存储间隔	hour	有符号整数
14	用户协议容量	MVA	浮点数
16	最小短路容量	MVA	浮点数
18	设备容量	MVA	浮点数
20	频率上越限	Hz	浮点数
22	频率下越限	Hz	浮点数
24	电压上偏差	%	浮点数
26	电压下偏差	%	浮点数
28	短闪变越限阈值	无	浮点数
30	长闪变越限阈值	无	浮点数
32	电压总畸变阈值	%	浮点数
34	电流总畸变阈值	%	浮点数
36	奇次谐波越限阈值	%	浮点数
38	偶次谐波越限阈值	%	浮点数
40	电压负序不平衡度越限	%	浮点数
42	电流负序不平衡度越限	%	浮点数
44	电压骤升阈值	%	浮点数
46	电压骤降阈值	%	浮点数
48	电压中断阈值	%	浮点数
50	冲击电流阈值	%	浮点数
52~49	谐波电流越限阈值 2-25 次	A	浮点数

### 5.2.2 响应命令说明

功能码	字节数	寄存器值	校验和 CRC
0x03	N*		

注：N\*= 2\*请求命令中寄存器个数。

将响应报文中的寄存器数据每 4 字节分成一个系统参数，对于每个系统参数，第一个字节存储参数的最高位比特，第四个字节存储最低位比特。

例如：请求读系统参数第 5 个额定电流参数值，该值为浮点数 5.0，“big-Endian”模式下对应的内存内容为（内存地址从低到高）：0x40 0xA0 0x00 0x00。主站在解析时，先根据自身处理器的模式将数据进行装换，再通过表 5-2 可知，需要将数据内容按照浮点数来解析。请求及响应帧信息如下所示：

请求		响应	
域名	(十六进制)	域名	(十六进制)
功能	03	功能	03
起始地址 Hi	00	字节数	04
起始地址 Lo	08	数据域 1	40
参数个数	02	数据域 2	A0
		数据域 3	00
		数据域 4	00

### 5.2.3 交互流程

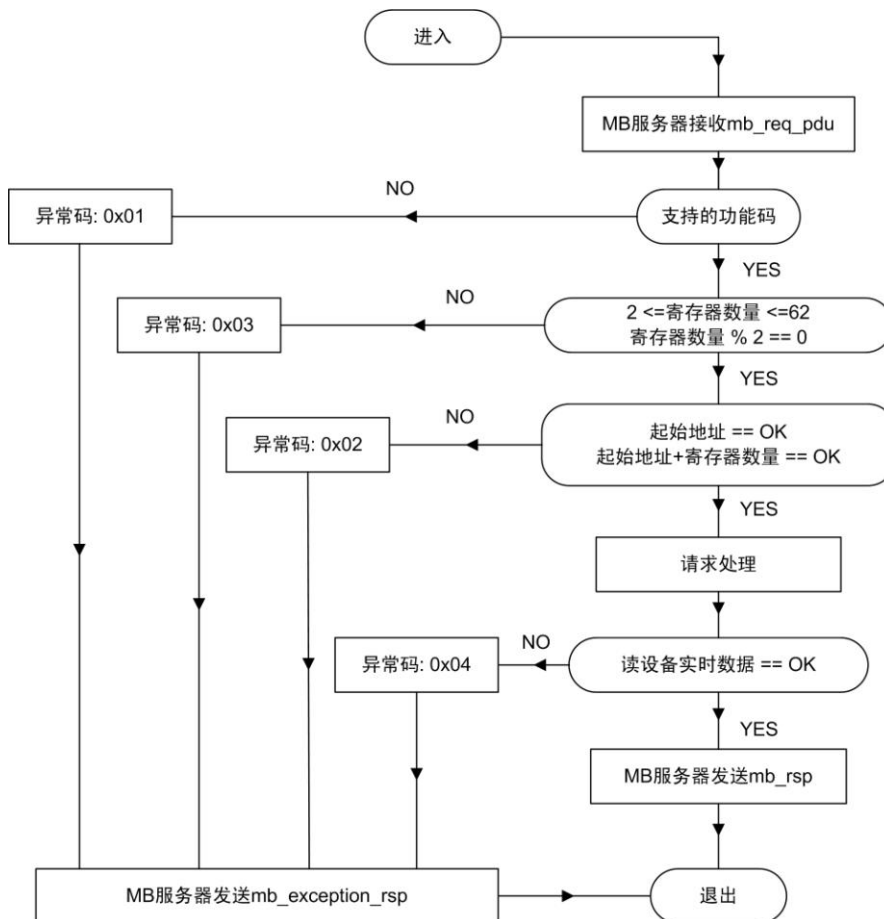


图 5.2 读系统参数状态图

### 5.3 (0x04) 读实时数据

考虑到实时传输数据量较大，装置在传输实时数据时会把数据编码成 2 字节，每个数据

项对应一个寄存器地址。2 字节的实时数据的编码方式如下表 5-3 所示：

表 5-3 实时数据编码格式

位地址	说明
0	是否有效标志位，1 表示无效，0 表示有效值
1	数据符号位，0 表示正数，1 表示负数
2-7	数据内容的高 6 位
8-15	数据内容的低 8 位

2 字节的数据内容中包含起始的 1 位有效标志以及占用 15 位的数据内容，数据内容按照有符号整数存储，负数用补码表示。

### 5.3.1 请求命令信息

功能码	起始地址高位	起始地址低位	寄存器个数高位	寄存器个数低位	校验和 CRC
0x04	0xN0	0xnn	0xnn	0xnn	0xnmmn

请求命令中指定了请求的寄存器起始地址和寄存器数量，起始地址的前 4 位值 N 表示请求板卡编号为 N 的数据，N 可取 0-5。起始地址的后 12 位值指定了数据的起始地址，从 0 开始编号，每个寄存器地址对应的具体的实时数据项如下表 5-4 所示。

该命令寄存器个数最大值为 125 个，主站获取到 E8300 返回的数据后进行解析，解析得到的有符号整数 X 还需要按照表 5-4 除以对应的转换系数才能得到真正的数据值。

表 5-4 数据项列表

数据地址	数据内容	相序	单位	转换系数
0	频率	--	Hz	273.05
1	电压总有效值	A/AB	V	32.766
2	电压总有效值	B/BC		
3	电压总有效值	C/CA		
4	电流总有效值	A	A	546.1
5	电流总有效值	B		
6	电流总有效值	C		
7	正序电压	--	V	32.766
8	负序电压	--		
9	零序电压	--		
10	正序电流	--	A	546.1
11	零序电流	--		
12	负序电流	--		
13	电压负序不平衡度	--	%	163.83
14	电压零序不平衡度	--		
15	电流负序不平衡度	--		
16	电流零序不平衡度	--		
17	有功功率 P	A/AB	W	1.6383
18	有功功率 P	B/BC		
19	有功功率 P	C/CA		
20	总有功功率 P	--		

21	无功功率 Q	A/AB	VAr	8191.5	
22	无功功率 Q	B/BC			
23	无功功率 Q	C/CA			
24	总无功功率 Q	--			
25	视在功率 S	A/AB	VA		
26	视在功率 S	B/BC			
27	视在功率 S	C/CA			
28	总视在功率 S	--			
29	功率因素 PF	A/AB	无		
30	功率因素 PF	B/BC			
31	功率因素 PF	C/CA			
32	总功率因数 PF	--			
33	位移功率因素 DF	A/AB	无		
34	位移功率因素 DF	B/BC			
35	位移功率因素 DF	C/CA			
36	总位移功率因素 DF	--			
37	短时间闪变	A/AB	无		409.575
38	短时间闪变	B/BC			
39	短时间闪变	C/CA			
40	长时间闪变	A/AB			
41	长时间闪变	B/BC			
42	长时间闪变	C/CA			
43	电压波动	A/AB	%		
44	电压波动	B/BC			
45	电压波动	C/CA			
46	谐波电压总畸变率	A/AB	%	163.83	
47	谐波电压总畸变率	B/BC			
48	谐波电压总畸变率	C/CA			
49	谐波电流总畸变率	A			
50	谐波电流总畸变率	B			
51	谐波电流总畸变率	C			
52~76	1-25 次谐波相电压含有率序列	A			
77~101	1-25 次谐波相电压含有率序列	B			
102~126	1-25 次谐波相电压含有率序列	C			
127~151	1-25 次谐波电流序列	A	A		546.1
152~176	1-25 次谐波电流序列	B			
177~201	1-25 次谐波电流序列	C			

例如：板卡 2 第 6 个数据项为 B 相电流总有效值，其对应的 04 功能码中寻址地址为：0x1005。

### 5.3.2 响应命令说明

正常的响应命令帧如下描述：

功能码	数据长度	数据	校验和 CRC
0x04	N*（1 字节）	N*个字节	0xnn

例如：请求第 6 个电能质量实时数据项 B 项电流总有效值，即获取寄存器地址为 5 的内容。具体请求及响应命令帧如下所示。0x0AAA 表示有符号数 2730，根据实时数据对照表可知转换系数为 546.1，则实际的电流有效值为 4.999。

请求		响应	
域名	(十六进制)	域名	(十六进制)
功能	04	功能	04
起始地址 Hi	00	字节数	02
起始地址 Lo	05	输入寄存器 6Hi	0A
输入寄存器数量 Hi	00	输入寄存器 6Li	AA
输入寄存器数量 Li	01		

### 5.3.3 交互流程

数据通信状态图如所示。

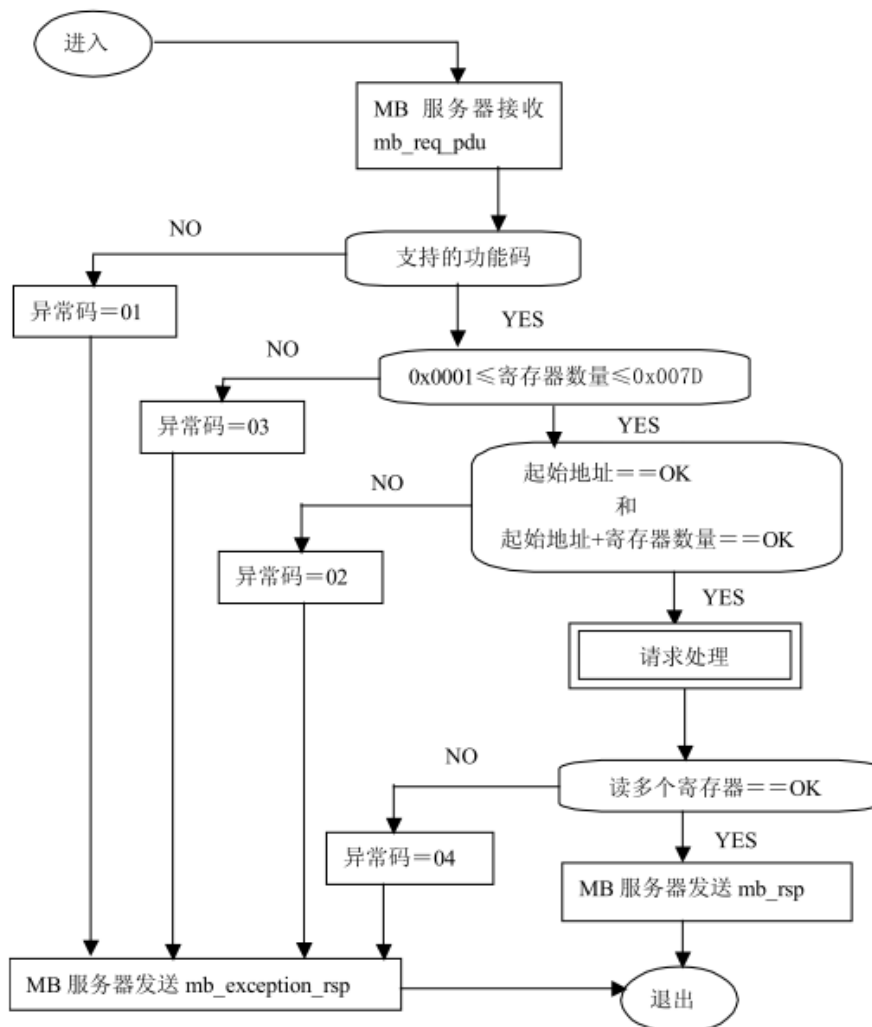


图 5.3 读实时数据状态图

## 6. 异常响应

当主设备向 E8300 从设备发送请求时，主设备希望一个正常响应。从主站询问中出现下列四种可能事件之一：

1、如果服务器设备接收到无通信错误的请求，并且可以正常地处理询问，那么服务器设备将返回一个正常响应。

2、如果由于通信错误，服务器没有接收到请求，那么不能返回响应。客户机程序将最终处理请求的超时状态。

3、如果服务器接收到请求，但是检测到一个通信错误（奇偶校验、LRC、CRC、...），那么不能返回响应。客户机程序将最终处理请求的超时状态。

4、如果服务器接收到无通信错误的请求，但不能处理这个请求（例如，如果请求读一个不存在的输出或寄存器），服务器将返回一个异常响应，通知用户错误的本质特性。

异常响应报文有两个与正常响应不同的域：

**功能码域：**在正常响应中，服务器利用响应功能码域来应答最初请求的功能码。所有功能码的最高有效位（MSB）都为 0（它们的值都低于十六进制 80）。在异常响应中，服务器设置功能码的 MSB 为 1。这使得异常响应中的功能码值比正常响应中的功能码值高十六进制 80。通过设置功能码的 MSB，客户机的应用程序能够识别异常响应，并且能够检测异常码的数据域。

**数据域：**在正常响应中，服务器可以返回数据域中数据或统计表（请求中要求的任何报文）。在异常响应中，服务器返回数据域中的异常码。这就定义了产生异常的服务器状态。

异常响应的帧格式如下表所示：

<b>功能码域</b>	1 字节	功能码+0x80
<b>数据域</b>	1 字节	0x01、0x02、0x03、0x04

客户机请求和服务器异常响应的实例：

请求		响应	
域名	(十六进制)	域名	(十六进制)
功能	01	功能	81
起始地址 Hi	04	异常码	02
起始地址 Lo	A1		
输出数量 Hi	00		
输出数量 Li	01		

在这个实例中，客户机对服务器设备寻址请求。功能码(01)用于读输出状态操作。它将请求地址 1245(十六进制 04A1)的输出状态。值得注意的是，象输出域(0001)号码说明的那样，只读出一个输出。

如果在服务器设备中不存在输出地址，那么服务器将返回异常码(02)的异常响应。这就说明从站的非法数据地址。

表 6-1 MODBUS 异常码

代码	名称	含义
----	----	----

01	非法功能	询问中接收到的功能码是不可允许的操作，不能被识别
02	非法数据地址	询问中接收到的数据地址是不可允许的地址。特别是，参考号和传输长度的组合是无效的。对于带有 100 个寄存器的控制器来说，带有偏移量 96 和长度 4 的请求会成功，带有偏移量 96 和长度 5 的请求将产生异常码 02
03	非法数据值	询问中包括的值是不可允许的值
04	从站设备故障	E8300 不能正确的获取相应的数据来返回。



## 7. 数据校验

数据传输过程依赖于传输模式，两种校验模式都使用：**RTU** 或 **ASCII**，该协议默认采用 **RTU** 模式。在 **RTU** 模式，包含一个对全部报文内容执行的，基于循环冗余校验(**CRC - Cyclical RedundancyChecking**) 算法的错误检验域。**CRC** 域检验整个报文的内容。不管报文有无奇偶校验，均执行此检验。