

# ZE-C310 对外通讯协议 V2.0

## 1、通信配置说明

通信链路	RS485/RS232
通信波特率	9600（可在触摸屏设置）
数据位	8位
停止位	1位
校验位	无校验
MODBUS模式	RTU
设备地址	01-0XF7（可在触摸屏设置）

表1 RTU帧格式

设备地址	功能代码	数据	CRC校验
8bit	8bit	n个8bit	16bit

表2 ModBus功能码ModBus各功能码对应的数据类型

代码	功能	数据类型	备注
03	读	整形、浮点、字符	读多个寄存器
16	写	整形、浮点、字符	写多个寄存器

表3 数据类型

数据类型	描述及要求
BYTE	无符号单字节整型(字节, 8 位)
WORD	无符号双字节整型(字, 16 位)
DWORD	无符号四字节整型(双字, 32 位)
FLOAT	四字节浮点数型(字节, 32 位) IEEE 754 标准
BYTE[n]	n 字节
STRING	GBK 编码, 采用 0 终结符, 若无数据, 则放一个 0 终结符
DATE	日期类型 6 字节 年(byte)-月(byte)-日(byte)-时(byte)-分(byte)-秒(byte) 其中: 年=byte+2000, 月:1-12, 日:1-31, 时:0-23 分:0-59 秒:0-59

### 传输规则

协议采用大端模式(big-endian)的网络字节序来传递字和双字, 浮点数。

约定如下:

- 字节 (BYTE)的传输约定:按照字节流的方式传输;
- 字(WORD)的传输约定:先传递高八位, 再传递低八位;
- 双字(DWORD)的传输约定:先传递高 24 位, 然后传递高 16 位, 再传递高八位, 最后传递低八位。
- 浮点数(FLOAT)的传输约定:先传递高 24 位, 然后传递高 16 位, 再传递高八位, 最后传递低八位。

## 2、帧数据结构

本仪表使用 ModBus 2 条指令,下面对这 2 条指令帧格式进行介绍.

### 2.1 功能码(0x03)读

主机请求:

设备地址 (1BYTE) + 功能码 (1BYTE)+ 寄存器地址 (2BYTE)+ 寄存器数量 (2BYTE)+CRC 校验 (2BYTE)

说明:

设备地址: 主控板地址, 为 0x01-0xF7 可选

功能码: 为 0x03

寄存器地址: 要读取数据的存放开始地址, 高位在前, 低位在后。

寄存器数量: 要读取的寄存器的个数, 高位在前, 低位在后

CRC 校验: 采用 CRC-16 校验, 高字节在前, 低字节在后

从机应答:

设备地址 (1BYTE)+功能码 (1BYTE)+数据字节数 (1BYTE)+数据 (N BYTE)+CRC 校验

说明:

设备地址: 下位机地址, 为 0x01-0xF7 可选

功能码: 为 0x03

数据字节数: 寄存器数量\*2

数据: N =(寄存器数量\*2)BYTE

CRC 校验: 采用 CRC-16 校验, 高字节在前, 低字节在后

错误应答: 设备地址 (1BYTE)+出错功能码+错误类型 (1BYTE)+CRC 校验

**PS: 出错功能码是功能码 byte 最高位取反得到。例如 0x03 出错功能码为 0x83**

错误类型:

- 01 非法功能
- 02 非法数据地址
- 03 非法数据值
- 04 从站设备故障
- 05 确认
- 06 从属设备忙

错误类型码详细说明见“MODBUS 异常码”

#### 示例

主机读取当前测量值的命令数据串:

```
01 03 00 00 00 02 C4 0B (设备地址 01)
02 03 00 00 00 02 C4 38 (设备地址 02)
03 03 00 00 00 02 C5 E9 (设备地址 03)
04 03 00 00 00 02 C4 5E (设备地址 04)
```

其中设备地址 (01)+功能码 (03)+寄存器起始地址 (00 00)+寄存器数量 (00 02 即指数据长度为 2 个字)+CRC 校验 (C4 0B)

下位机输出当前测量值的数据串:

```
01 03 04 41 CB 42 B7 EF 27
```

设备地址(01)+ 功能码(03)+数据字节数(04) + 测量值(按照低字在前高字在后传输, 实际为2字16进制数42 B7 41 CB对应的浮点型数据为91.63 mg/L)+ CRC 校验(EF 27)。

## 2.2 功能码(0x10)写

主机请求:

设备地址(1BYTE)+功能码(1BYTE)+寄存器地址(2BYTE)  
+寄存器数量(2BYTE)+字节数(1BYTE)+ 数据+CRC 校验(2BYTE)

说明:

设备地址: 主控板地址, 为0x01-0xF7 可选

功能码: 为0x10

寄存器地址: 要读取数据的存放开始地址, 高位在前, 低位在后

寄存器数量: 要写入寄存器的个数

字节数: 写入数据的字节数

数据: 要写入的数据

CRC 校验: 采用CRC-16 校验, 高字节在前, 低字节在后

Ps: 如写一个寄存器, 则寄存器数量为1, 字节数为2, 数据为一个Word

从机应答:

设备地址(1BYTE)+功能码(1BYTE)+寄存器地址(2BYTE)+寄存器数量(2BYTE) +CRC 校验(2BYTE)

示例

主机发送: 01 10 00 6B 00 02 04 00 0F 06 08 86 51

从机回复: 01 10 00 6B 00 02 30 14

错误应答: 设备地址(1BYTE)+出错功能码+错误类型(1BYTE)+CRC 校验

**PS: 出错功能码是功能码 byte 最高位取反得到。例如 0x03 出错功能码为 0x83**

错误类型:

- 01 非法功能
- 02 非法数据地址
- 03 非法数据值
- 04 从站设备故障
- 05 确认
- 06 从属设备忙

错误类型码详细说明见“MODBUS 异常码”

### 3、仪表通讯命令说明

#### 通讯命令说明

寄存器名称	地址	寄存器内容（连续的寄存器空间）	备注	读/写
测量信息	0x1000	<p>读取命令： 设备地址+功能码 (0x03)+寄存器地址 (0x1000)+ 寄存器数量 (0x0c) + CRC校验 (2BYTE)</p> <p>仪表响应： 设备地址 (1BYTE)+功能码 (0x03)+数据字节数 (0x18)+数据内容 (N BYTE)+CRC校验 (2BYTE)</p> <p>数据内容： 测量值 + 测量时间 + 吸光度 Float          Date          Float +测量电压 +参比电压+数据标识 Float          Float          word</p>	<p>测量值:mg/l 电压:V 占用字节数: 4+6+4+4+4+2=24 =0x18</p>	只读
标定信息	0x1040	<p>读取命令： 设备地址+功能码 (0x03)+寄存器地址 (0x1040)+ 寄存器数量 (0x11) + CRC校验 (2BYTE)</p> <p>仪表响应： 设备地址 (1BYTE)+功能码 (0x03)+数据字节数 (0x2a)+数据内容 (N BYTE)+CRC校验 (2BYTE)</p> <p>数据内容： 斜率+ 截距+标液浓度+吸光度一+测量电压一+参比电压一 Float   Float   Float          Float          Float          Float +吸光度二 + 测量电压二 + 参比电压二 Float          Float          Float + 标定时间   Date</p>	<p>占用字节数: 4*9+6=42 =0x2a</p>	只读
仪表操作命令	0x1080	<p>写命令： 设备地址+功能码 (0x10)+寄存器地址 (0x1080)+寄存器数量 (1 ) +字节数 (2) +数据 (操作码N) + CRC校验 (2BYTE)</p> <p>仪表响应 设备地址 (1BYTE)+功能码 (1BYTE)+寄存器地址 (2BYTE)+寄存器数量 (2BYTE) +CRC 校验 (2BYTE)</p> <p>仪表操作码： 0:测量 1:标定 2:清洗 3:标液校准</p>	<p>占用字节数: 2字节</p>	只写

		4:空白校准 5:标样核查 6:停止 7. 远程留样		
仪表状态	0x10c0	读取命令: 设备地址+功能码(0x03)+寄存器地址(0x10c0)+ 寄存器数量(0x06) + CRC校验(2BYTE) 仪表响应: 设备地址(1BYTE)+功能码(0x03)+数据字节数(0x0c)+数据内容(N BYTE)+CRC校验(2BYTE) 数据内容: 仪器模式 +仪器状态 +步骤码 + 状态码 word word word byte[6] 仪器模式(word): 0: 在线 1: 离线 2: 维护 3: 故障 仪器状态(word): 0:测量 1:标定 2:空白校准 3:标样校准 4:清洗 5:标样核查 6:仪器告警 7:仪器维护 8:上电检查 9:断电处理 10:空闲状态 步骤 (word): 详见附录 步骤表 状态码 BYTE[6]: 6字节 详见附录 状态码表	占用字节数: 2*3+6=12=0x0c	只读
系统维护命令	0x1100	写命令: 设备地址+功能码(0x10)+寄存器地址(0x1100) +寄存器数量(1) +字节数(2)+ 寄存器内容(操作码N) +CRC校验(2BYTE) 仪表响应 设备地址(1BYTE)+功能码(1BYTE)+寄存器地址(2BYTE)+寄存器数量(2BYTE) +CRC 校验(2BYTE) 维护操作码: 0:进入维护 1:退出维护 2:管路清理 3:初始装液 4:采水开始 5:采水结束 6:取留样液 7:即刻留样 8:计量电压调节 9:测量电压调节 10: 清零开门次数 11: 仪表自检	占用字节数: 2字节	只写
部件维护命令	0x1140	写命令: 设备地址+功能码(0x10)+寄存器地址(0x1140)+寄存器数量(1) +字节数(2)+寄存器内容(操作码N) +CRC校验(2BYTE) 仪表响应 设备地址(1BYTE)+功能码(1BYTE)+寄存器地址(2BYTE)+寄存器数量(2BYTE) +CRC 校验(2BYTE) 部件维护命令码: 0:水样阀 1:零标阀 2:量标阀 3:试剂A阀 4:试剂B阀 5:试剂C阀 6:试剂D阀 7:试剂E阀 8:试剂F阀	占用字节数: 2字节	只写

		9:公共阀    10:左废液阀    11:自定义阀 12:空气阀    13:反应池阀    14:告警灯 15:风扇    16:泵左转    17:泵右转 18:测量灯一    19:测量灯二		
步骤维护命令	0x1180	写命令: 设备地址+功能码(0x10)+寄存器地址(0x1180)+ 寄存器数量 (1 ) +字节数 (2) +寄存器内容(操作码N) +CRC校验(2BYTE) 仪表响应: 设备地址(1BYTE)+功能码(1BYTE)+寄存器地址(2BYTE)+寄 存器数量(2BYTE) +CRC 校验(2BYTE) 步骤维护命令: 0:进零标    1:进水样    2:进量标 3:进试剂一    4:进试剂二    5:进试剂三 6:进试剂四    7:进试剂五    8:进试剂六 9:清洗    10:排空    11:润洗 12:高计量灯    13:中计量灯    14:低计量灯 15:吹气    16:冷却    17:高温消解 18:检测一    19:检测二	占用字节数: 2字节	只写
读取仪表信息	0x11c0	读取命令: 设备地址+功能码(0x03)+寄存器地址(0x11c0)+ 寄存器数量 (0x14) + CRC校验(2BYTE) 仪表响应: 设备地址(1BYTE)+功能码(0x03)+数据字节数(0x2a)+数据内 容(N BYTE)+CRC校验(2BYTE) 内容: 仪表序列号 + 软件版本号 + 硬件版本号 BYTE[12]    BYTE[10]    BYTE[10] +测量因子+测量范围 + 定量下限 Word    float    float 测量因子详见附录 因子表	占用字节数: 42byte	只读
读取/设置基 本参数	0x1200	读取命令: 设备地址+功能码(0x03)+寄存器地址(0x1200)+ 寄存器数量 (0x0b) + CRC校验(2BYTE) 仪表响应: 设备地址(1BYTE)+功能码(0x03)+数据字节数(0x16)+数据内 容(N BYTE)+CRC校验(2BYTE) 数据内容: 采水时长    WORD    单位s +超标点    float    单位mg/L +标定间隔时间    WORD    单位hour +测量间隔时间    WORD    单位min +标样核查间隔时间    WORD    单位hour +标样核查选择    WORD    (0禁止, 1:零标2:量标)	占用字节数: 22byte	读写

		+测量模式 WORD (0:间隔 1:定点 2:外部触发) +采水后静置时间 WORD 单位分钟 +整点测量 DWORD bit0-23 代表整点 设置命令: 设备地址+功能码(0x10)+寄存器地址(0x1200)+寄存器数量 (0x0b)+字节数(22)+数据内容+CRC校验(2BYTE) 数据内容: 同上		
读取/设置接口参数	0x1240	读取与设置命令格式同 基本参数, 内容如下: 数据内容: 仪器485设备地址 WORD 0-255 +485接口波特率 WORD 0:4800 1:9600 2:19200 3:38400 4:57600 5:115200 +485奇偶位 WORD 0:无校验1:奇校验2:偶校验 +485数据位 WORD 5, 6, 7, 8位 +485停止位 WORD 1停止位, 2停止位 +232接口波特率 WORD 同485 +232奇偶位 WORD 同485 +232数据位 WORD 同485 +232停止位 WORD 同485 +4-20mA输出量程范围 float +DTU配置 WORD 0:不使用 1:232 2:485	占用字节数: 24byte	读写
读取/设置告警参数	0x1280	读取与设置命令格式同 基本参数, 内容如下: 告警继电器 WORD 0:继电器1 非0: 继电器2 +告警类型 byte[24], 0为不支持, 1为支持 (告警类型见附录的告警类型表)	占用字节数: 26byte	读写
读取/设置标定参数	0x12c0	读取与设置命令格式同 基本参数, 内容如下: 数据内容: 低中量程切换值 float +中高量程切换值 float +标定清洗次数 WORD +量程配置 WORD 0:低 1:中 2:高 +低量程标液 float +中量程标液 float +高量程标液 float	占用字节数: 24	读写
读取/设置系统参数	0x1300	读取与设置命令格式同 基本参数, 内容如下: 数据内容: + 量程自动切换 WORD 1: 使能 0: 关闭 + 超标留样功能 WORD 1: 使能 0: 关闭 + 消解时长 WORD 单位分钟 + 清洗类型 WORD 0:零标洗 1:加热零标洗 2:酸洗 3: 加热酸洗 + 消解温度 WORD 单位: 摄氏度 + 协议选择 WORD 0:中兴协议	占用字节数: 16byte	读写

		1:国标HJT212 + 自定义阀功能 WORD 0:试剂 1:为右废液阀 2:清洗水管(清洗纯水从水样管排出) + 润洗次数 WORD		
读取开门记录	0x1340	读取命令: 设备地址+功能码(0x03)+寄存器地址(0x1340)+寄存器数量(0x09)+CRC校验(2BYTE) 仪表响应: 设备地址(1BYTE)+功能码(0x03)+数据字节数(0x12)+数据内容(N BYTE)+CRC校验(2BYTE) 数据内容: 开门次数(1字,无符号整数)+最后一次开门时间(6个字节,年+月+日+时+分+秒)+最近清除开门记录的时间(6个字节,年+月+日+时+分+秒)	占用字节数: 14个字节	只读
读取/设置 仪表时间	0x1380	读取命令: 设备地址+功能码(0x03)+寄存器地址(0x1380)+寄存器数量(0x03)+CRC校验(2BYTE) 仪表响应: 设备地址(1BYTE)+功能码(0x03)+数据字节数(0x06)+数据内容(N BYTE)+CRC校验(2BYTE) 数据内容: 仪表时间(date) 设置命令: 设备地址+功能码(0x10)+寄存器地址(0x1380)+寄存器数量(0x03)+字节数(6)+数据内容+CRC校验(2BYTE)	6字节	读写
读取诊断相关信息	0x13C0	读取命令: 设备地址+功能码(0x03)+寄存器地址+寄存器数量(0x0A)+CRC校验(2BYTE) 仪表响应: 设备地址(1BYTE)+功能码(0x03)+数据字节数(0x14)+数据内容(N BYTE)+CRC校验(2BYTE) 数据内容: 高液位电压+中液位电压+低液位电压+测量电压+当前温度	20字节	只读
读取最近24小时测量结果	0x1400	读取命令: 设备地址+功能码(0x03)+寄存器地址+寄存器数量(24)+CRC校验(2BYTE) 仪表响应: 设备地址(1BYTE)+功能码(0x03)+数据字节数()+数据内容(N BYTE)+CRC校验(2BYTE) 数据内容: 测量结果记录个数N(1字节)+测量结果记录(0-N) 测量结果字段 = 测量值+测量时间	不定长字节	只读



仪表监控信息	0x1440	<p>读取命令:</p> <p>设备地址+功能码(0x03)+寄存器地址+ 寄存器数量(17) + CRC 校验(2BYTE)</p> <p>仪表响应:</p> <p>设备地址(1BYTE)+功能码(0x03)+数据字节数(34)+数据内容(N BYTE)+CRC校验(2BYTE)</p> <p>数据内容: 当前量程+斜率+截距+吸光度+  Word float float float  浓度+测量电压+参比电压+试剂余量+消解  Float float float word word  时长+消解温度+测量间隔  word word</p>	占用字节数 6*4+6*2=34字节	只读
定时上报信息	0x1480	<p>读取命令:</p> <p>设备地址+功能码(0x03)+寄存器地址+ 寄存器数量(21) + CRC 校验(2BYTE)</p> <p>仪表响应:</p> <p>设备地址(1BYTE)+功能码(0x03)+数据字节数(42)+数据内容(N BYTE)+CRC校验(2BYTE)</p> <p>数据内容: 测量值 + 测量时间 + 吸光度  Float Date Float  +测量电压 +参比电压+数据标识  Float Float word  +仪器模式 +仪器状态 +步骤码 + 状态码  word word word byte[6]  +状态变化时间  Date</p>	占用字节数 4+6+4+4+4+2 +2+2+2+6+6=42	只读
空白校准信息	0x14C0	<p>读取命令:</p> <p>设备地址+功能码(0x03)+寄存器地址(0x1000)+ 寄存器数量(0x0c) + CRC校验(2BYTE)</p> <p>仪表响应:</p> <p>设备地址(1BYTE)+功能码(0x03)+数据字节数(0x18)+数据内容(N BYTE)+CRC校验(2BYTE)</p> <p>数据内容:</p> <p>零点漂移值 + 测量时间 + 吸光度  Float Date Float  +测量电压 +参比电压+数据标识  Float Float word</p>	测量值:mg/l 电压:V 占用字节数: 4+6+4+4+4+2=24 =0x18	只读
标液校准信息	0x1500	<p>读取命令:</p> <p>设备地址+功能码(0x03)+寄存器地址(0x1000)+ 寄存器数量(0x0c) + CRC校验(2BYTE)</p> <p>仪表响应:</p> <p>设备地址(1BYTE)+功能码(0x03)+数据字节数(0x18)+数据内容(N BYTE)+CRC校验(2BYTE)</p>	测量值:mg/l 电压:V 占用字节数: 4+6+4+4+4+2=24 =0x18	只读

		数据内容： 量程漂移值 + 测量时间 + 吸光度 Float          Date          Float +测量电压 +参比电压+数据标识 Float          Float          word		
--	--	---	--	--

## 4、在线升级说明

注意升级命令功能码 0x10 主机请求包格式和上面的介绍的 modbus 标准帧格式有微小区别  
0x10 功能码 modbus 标准主机请求帧格式：

设备地址 (1BYTE)+功能码 (1BYTE)+寄存器地址 (2BYTE)

**+寄存器数量 (2BYTE) +字节数 (1BYTE) + 数据+CRC 校验 (2BYTE)**

0x10 功能码在线升级命令中主机请求帧格式：

设备地址 (1BYTE)+功能码 (1BYTE)+寄存器地址 (2BYTE)

**+寄存器字节数 (2BYTE) + 数据+CRC 校验 (2BYTE)**

目的在于写数据时每包的字节数能大于 256 字节，因为标准格式字节数只有 1BYTE  
从机响应包格式相同。

### 4.1 升级开始

主机请求：

设备地址 (1BYTE)+功能码 (1BYTE)+寄存器地址 (2BYTE)

**+寄存器字节数 (2BYTE) + 数据+CRC 校验 (2BYTE)**

设备地址：主控板地址，为 0x01-0xF7 可选

功能码:0x10

寄存器地址：0x9C6F

寄存器字节数：0x0007

数据：程序包标志高区或低区(1 BYTE)+ 程序包的个数（1024 Byte 定义为 1 包，2BYTE） + 程序字节数（4BYTE）

程序包标志 0:高区 1:低区

从机应答：

设备地址 (1BYTE)+功能码 (1BYTE)+寄存器地址 (2BYTE)+寄存器字节数（2BYTE） +请求结果 (1BYTE)+CRC 校验 (2BYTE)

请求结果：0：接受升级请求 1：拒绝升级请求

错误应答：设备地址 (1BYTE)+出错功能码 (0x90)+错误类型 (1BYTE)+CRC 校验 (2BYTE)

错误类型： 01 非法的功能码  
02 非法的数据地址  
03 非法数据值  
04 设备失败

## 4.2 写数据

主机请求：

设备地址 (1BYTE)+功能码 (1BYTE)+寄存器地址 (2BYTE)

+寄存器字节数 (2BYTE)+ 数据+CRC 校验 (2BYTE)

设备地址：主控板地址，为 0x01-0xF7 可选

功能码:0x10

寄存器地址：0x9C70

寄存器字节数：2 + 升级数据包的字节数(一般 1024, 除非是最后一包程序包)

数据：数据包序号 N（2BYTE） + 数据包的数据

从机应答：

设备地址 (1BYTE)+功能码 (1BYTE)+寄存器地址 (2BYTE)+寄存器字节数（2BYTE） +数据包处理结果 (2BYTE)+CRC 校验 (2BYTE)

数据包处理结果:0，此数据包接收处理成功。

:序号 N, 请求重传数据包 N。

错误应答：设备地址 (1BYTE)+出错功能码 (0x90)+错误类型 (1BYTE)+CRC 校验 (2BYTE)

错误类型： 01 非法的功能码  
02 非法的数据地址  
03 非法数据值  
04 设备失败

## 4.3 写结束

主机请求：

设备地址 (1BYTE)+功能码 (1BYTE)+寄存器地址 (2BYTE)

+寄存器字节数 (2BYTE)+ 数据+CRC 校验 (2BYTE)

设备地址：主控板地址，为 0x01-0xF7 可选

功能码:0x10

寄存器地址：0x9C71

寄存器字节数：0x0002

数据：程序包 CRC16（2YTE）

从机应答：

设备地址 (1BYTE)+功能码 (1BYTE)+寄存器地址 (2BYTE)+寄存器字节数 (2BYTE) +写结束回应 (1BYTE)+CRC 校验 (2BYTE)

写结束回应：0：程序包 CRC 通过，升级成功。

1：程序包 CRC 不通过，升级失败。

错误应答：设备地址 (1BYTE)+出错功能码 (0x90)+错误类型 (1BYTE)+CRC 校验 (2BYTE)

错误类型： 01 非法的功能码  
02 非法的数据地址  
03 非法数据值  
04 设备失败

## 4.4 放弃升级

主机请求：

设备地址 (1BYTE)+功能码 (1BYTE)+寄存器地址 (2BYTE)  
+寄存器字节数 (2BYTE)+ 数据+CRC 校验 (2BYTE)

设备地址：主控板地址，为 0x01-0xF7 可选

功能码:0x10

寄存器地址：0x9C72

寄存器字节数：0x0002

数据：0x0000

从机应答：

设备地址 (1BYTE)+功能码 (1BYTE)+寄存器地址 (2BYTE)+寄存器字节数 (2BYTE) +CRC 校验 (2BYTE)

错误应答：设备地址 (1BYTE)+出错功能码 (0x90)+错误类型 (1BYTE)+CRC 校验 (2BYTE)

错误类型： 01 非法的功能码  
02 非法的数据地址  
03 非法数据值  
04 设备失败

## 4.5 获取当前程序地址

主机请求：

设备地址 (1BYTE)+功能码 (1BYTE)+寄存器起始地址 (2BYTE)+寄存器数量 (2BYTE)+CRC 校验 (2BYTE)

说明：

设备地址：主控板地址，为 0x01-0xF7 可选

功能码：为 0x10

寄存器起始地址：0x9C73

寄存器数量：2

CRC 校验：采用 CRC-16 校验，高字节在前，低字节在后

从机应答：

设备地址 (1BYTE)+功能码 (1BYTE)+寄存器地址 (2BYTE)+寄存器字节数 (2BYTE) +数据

(4BYTE)+CRC 校验 (2BYTE)

**说明:**

设备地址: 主控板地址, 为 0x01-0xF7 可选

功能码: 为 0x10

数据字节数: 0x4

数据: 当前程序地址, 4BYTE

CRC 校验: 采用 CRC-16 校验, 高字节在前, 低字节在后

**错误应答:** 设备地址 (1BYTE)+出错功能码 (0x83)+错误类型 (1BYTE)+CRC 校验 (2BYTE)

**错误类型:** 01 非法的功能码

02 非法的数据地址

03 非法数据值

04 设备失败

## 4.6 获取当前升级信息

**主机请求:**

设备地址 (1BYTE)+功能码 (1BYTE)+寄存器起始地址 (2BYTE)+寄存器数量  
(2BYTE)+CRC 校验 (2BYTE)

**说明:**

设备地址: 主控板地址, 为 0x01-0xF7 可选

功能码: 为 0x10

寄存器起始地址: 0x9C74

寄存器数量: 2

CRC 校验: 采用 CRC-16 校验, 高字节在前, 低字节在后

**从机应答:**

设备地址 (1BYTE)+功能码 (1BYTE)+寄存器地址 (2BYTE)+寄存器字节数 (2BYTE) + 升级信息  
(6BYTE)+CRC 校验 (2BYTE)

**说明:**

设备地址: 主控板地址, 为 0x01-0xF7 可选

功能码: 为 0x10

数据字节数: 0x6

数据: 1BYTE upgrade\_flag; 是否在升级的标志 0: 不在升级状态 1: 在升级状态

1BYTE program\_flag; 程序包的标志, 0: 高区程序 1: 低区程序

2BYTE current\_num; 当前升级包序号

2BYTE pack\_total; 程序包的总个数

CRC 校验: 采用 CRC-16 校验, 高字节在前, 低字节在后

**错误应答:** 设备地址 (1BYTE)+出错功能码 (0x83)+错误类型 (1BYTE)+CRC 校验 (2BYTE)

**错误类型:** 01 非法的功能码

02 非法的数据地址

03 非法数据值

04 设备失败

## 4.7 注意事项

1. 升级时，需记录每一段程序的升级记录，全部成功时，才下发写结束指令。
2. 写失败10次，直接报错，停止升级。
3. 发数据后 5 秒无返回数据，报超时，停止升级。

## 5、使用 DTU 传输数据的说明

### 5.1 协议数据帧结构

1. 所有上行的数据包(通过 DTU 发到服务器) 需添加包头分隔符 0x7E 结构如下:

标识位 0x7E + 原先的数据报文 + 标识位 0x7E

标识位 采用 0x7e 表示，若数据报文中出现 0x7e，则要进行转义处理，转义 规则定义如下:

0x7e<—>0x7d 后紧跟一个 0x02;

0x7d<—>0x7d 后紧跟一个 0x01。

转义处理过程如下:

发送消息时:消息封装——>计算并填充校验码——>转义;

接收消息时:转义还原——>验证校验码——>解析消息。

示例:

发送一包内容为 0x30 0x7e 0x08 0x7d 0x55 的数据包，则经过封装如下:0x7e 0x30 0x7d 0x02 0x08 0x7d 0x01 0x55 0x7e

### 5.2. 帧数据结构改动

帧数据结构改为: **设备 ID(12 BYTE)** + 命令地址(2BYTE)+ 设备地址+功能码(1BYTE)+寄存器地址(2BYTE)+ 寄存器数量(2BYTE)+CRC 校验(2BYTE)

设备 ID 是对应仪表的 IEM 码，贴在仪表机柜上。设备 ID 为 12 个 ascii 码。

## 附录

### 1.设备状态码表

Byte \ Bit	0	1	2	3	4	5
0	测量	重启仪器	管路清理	缺水样	缺试剂 F	通讯出错
1	标定	进入离线	设置时间标志	缺零标	缺试剂 G	试剂漏液
2	清洗	退出离线	超标留样	缺量标	加热超时	参数出错
3	标液校准	进入维护	开关门	缺试剂 A	加热出错	标定异常

4	零标校准	退出维护	在级升级	缺试剂 B	冷却太慢	标样核查出错
5	标液核查	采水开始	开机	缺试剂 C	计量出错	超标告警
6	初始装液	采水结束	保留	缺试剂 D	测量出错	超量程告警
7	停止	清理废液	保留	缺试剂 E	排空出错	试剂余量不足

## 2.告警类型表

Byte	0	1	2	3	4	5	6	7
类型	缺水样	缺零标	缺量标	缺试剂 A	缺试剂 B	缺试剂 C	缺试剂 D	缺试剂 E
Byte	8	9	10	11	12	13	14	15
类型	缺试剂 F	缺试剂 G	加热超时	加热异常	冷却超时	计量异常	测量异常	排空异常
Byte	16	17	18	19	20	21	22	23
类型	通讯异常	仪表漏液	参数异常	标定异常	标定核查异常	超标告警	超量程告警	试剂余量不足

## 3.步骤说明表

数值	步骤
0	进水样
1	进零标
2	进量标
3	进试剂 A
4	进试剂 B
5	进试剂 C
6	进试剂 D
7	进试剂 E
8	进试剂 F
9	进试剂 G
10	预备
11	润洗
12	进样
13	高温消解
14	吹气
15	冷却
16	检测
17	排空
18	清理
19	挂壁处理
20	空闲
21	采水
22	初始进液
23	管理清理
24	超标留样
25	静置



## 4. MODBUS 异常码

代码 名称 含义

01 非法功能 对于服务器(或从站)来说, 询问中接收到的功能码是不可允许的操作。这也许是因为功能码仅仅适用于新设备而在被选单元中是不可实现的。同时, 还指出服务器(或从站)在错误状态中处理这种请求, 例如: 因为它是未配置的, 并且要求返回寄存器值。

02 非法数据地址 对于服务器(或从站)来说, 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 对于服务器(或从站)来说, 询问中包括的值是不可允许的值。这个值指示了组合请求剩余结构中的故障, 例如: 隐含长度是不正确的。并不意味着, 因为 MODBUS 协议不知道任何特殊寄存器的任何特殊值的重要意义, 寄存器中被提交存储的数据项有一个应用程序期望之外的值。

04 从站设备故障 当服务器(或从站)正在设法执行请求的操作时, 产生不可重新获得的差错。

05 确认 与编程命令一起使用。服务器(或从站)已经接受请求, 并且正在处理这个请求, 但是需要长的持续时间进行这些操作。返回这个响应防止在客户机(或主站)中发生超时错误。客户机(或主站)可以继续发送轮询程序完成报文来确定是否完成处理。

06 从属设备忙 与编程命令一起使用。服务器(或从站)正在处理长持续时间的程序命令。当服务器(或从站)空闲时, 用户(或主站)应该稍后重新传输报文。

08 存储奇偶性差错 与功能码 20 和 21 以及参考类型 6 一起使用, 指示扩展文件区不能通过一致性校验。

服务器(或从站)设法读取记录文件, 但是在存储器中发现一个奇偶校验错误。客户机(或主方)可以重新发送请求, 但可以在服务器(或从站)设备上要求服务。

0A 不可用网关路径 与网关一起使用, 指示网关不能为处理请求分配输入端口至输出端口的内部通信路径。通常意味着网关是错误配置的或过载的。

0B 网关目标设备响应失败 与网关一起使用, 指示没有从目标设备中获得响应。通常意味着设备未在网络中

## 5. 因子表

因子数值	简写	中文名
0	NH4	氨氮
1	Cod	化学需氧量
2	Tcu	总铜
3	Cr6	六价铬
4	Tcr	总铬
5	Tni	总镍
6	Cd	镉
7	Pb	铅
8	Tfe	总铁
9	Tzn	总锌

10	TAs	总砷
11	Tmn	总锰
12	TP	总磷

## 6. CRC 校验算法

modbus crc 校验代码:

unsigned short CRC16 ( unsigned char \*ptr, unsigned int len)

```
{
    unsigned short crc=0xFFFF;
    unsigned int i, j;
    for ( j=0; j<len; j++)
    {
        crc=crc ^*ptr++;
        for ( i=0; i<8; i++)
        {
            if( ( crc&0x0001) >0)
            {
                crc=crc>>1;
                crc=crc^ 0xa001;
            }
            else
            {
                crc=crc>>1;
            }
        }
    }
    return ( crc);
}
```