



FR-UK33(V5.1)北向人机

# Modbus 通信协议(V1.00)



# 声 明

版权所有©科华数据股份有限公司 2021。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



和其他科华商标均为科华数据股份有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

## 注意

您购买的产品、服务或特性等应受科华公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，科华公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

## 科华数据股份有限公司

地址：                  厦门火炬高新区火炬园马垄路 457 号

公司网址：              www.kehua.com.cn

E-MAIL:                  service@kehua.com

客户服务中心热线：    400-808-9986

电话：                  0592-5160516

传真：                  0592-5162166

# 目 录

|  |          |
|--|----------|
| <b>第 1 章 概述</b> .....                  | <b>1</b> |
| 1.1 协议描述.....                          | 1        |
| 1.2 适用范围.....                          | 1        |
| 1.3 相关术语及描述.....                       | 1        |
| 1.4 通信配置.....                          | 2        |
| 1.4.1 RS485 接口配置.....                  | 2        |
| 1.4.2 以太网接口配置.....                     | 2        |
| <b>第 2 章 信息地址</b> .....                | <b>3</b> |
| 2.1 读输入离散量（状态量）功能码 0x02 .....          | 3        |
| 2.1.1 标准状态量查询.....                     | 3        |
| 2.1.2 扩展状态量查询.....                     | 4        |
| 2.2 读输入寄存器（模拟量）功能码 0x04 .....          | 5        |
| 2.2.1 标准模拟量查询 1（UPS 通用模拟量） .....       | 5        |
| 2.2.2 标准模拟量查询 2（UPS 扩展模拟量） .....       | 6        |
| 2.3 读写线圈（状态量）读功能码 0x01，写功能码 0x05 ..... | 7        |
| 2.3.1 标准状态量设置.....                     | 7        |
| 2.4 写单个保持寄存器（模拟量）功能码 0x06.....         | 7        |
| 2.4.1 标准模拟量设置.....                     | 7        |
| 2.5 写多个保持寄存器（模拟量）功能码 0x10 .....        | 7        |
| <b>A Modbus 通信协议</b> .....             | <b>8</b> |

# 第1章 概述

## 1.1 协议描述

本协议为科华公司大功率塔式 UPS 标准 Modbus 通信协议，以该协议实现对科华公司大功率塔式 UPS 的上位机监控。

## 1.2 适用范围

本协议适用科华公司 FR-UK33 (V5.1) 系列机型与上位机的通信。

## 1.3 相关术语及描述

| 名称         | 描述                        |
|------------|---------------------------|
| 主站         | 该总线通信方式中，主动发起通信的一方        |
| 从站         | 该总线通信方式中，被动响应命令的一方        |
| UINT16     | 无符号 16 位整型。高字节在前，低字节在后    |
| UINT32     | 无符号 32 位整型。高字节在前，低字节在后    |
| INT16      | 有符号 16 位整型。高字节在前，低字节在后    |
| INT32      | 有符号 32 位整型。高字节在前，低字节在后    |
| String     | 每个字节内容以 ASCII 表示的字符串      |
| MLB        | 多字节(multibyte)            |
| Bitfield16 | 16 位宽度的按位表达数据。高字节在前，低字节在后 |
| RW         | 可读可写寄存器                   |
| RO         | 只读寄存器                     |

## 1.4 通信配置

本协议适用于标准 RS485、以太网通信方式。

### 1.4.1 RS485 接口配置

| 名称        | 描述                                 |
|-----------|------------------------------------|
| 传输模式      | RTU                                |
| 波特率       | 默认为 9600bps, 可设置为 4800bps, 9600bps |
| 起始位       | 1 位                                |
| 数据位       | 8 位                                |
| 校验位       | 无                                  |
| 停止位       | 1 位                                |
| 帧间隔       | 不小于 3.5 个字节时间                      |
| 帧内字符间隔    | 不大于 1.5 个字节时间                      |
| 帧长度最大值    | 100 个字节                            |
| 从站应答时间最大值 | 150 个字节时间                          |
| 主站轮询间隔最小值 | 200 个字节时间                          |

### 1.4.2 以太网接口配置

| 名称        | 描述        |
|-----------|-----------|
| 传输模式      | TCP/IP    |
| 端口号       | 502       |
| 从站应答时间最大值 | 100ms     |
| 主站轮询间隔最小值 | 100ms     |
| IP        | 通过 HMI 设置 |

## 第2章 信息地址

注：下列表格的地址已与实际信息帧中的地址相同，无需再进行偏移或作其它转换，地址为十进制数。

### 2.1 读输入离散量（状态量）功能码 0x02

#### 2.1.1 标准状态量查询

| 地址        | 故障内容（显示标签）         | 逻辑含义           | 备注   |
|-----------|--------------------|----------------|------|
| 5000-5001 | 预留                 |                |      |
| 5002      | 电池逆变状态             | 0-非电池逆变；1-电池逆变 |      |
| 5003-5004 | 预留                 |                |      |
| 5005      | 温度异常（整流器过温、逆变过温保护） | 0-正常；1-异常      |      |
| 5006      | 市电异常               | 0-正常；1-异常      |      |
| 5007      | 输出异常               | 0-正常；1-异常      |      |
| 5008      | 输出过载               | 0-正常；1-异常      |      |
| 5009      | 旁路输出状态             | 0-关闭；1-开启      |      |
| 5010      | 旁路异常               | 0-正常；1-异常      |      |
| 5011-5015 | 预留                 |                |      |
| 5016      | 风机故障               | 0-正常；1-异常      |      |
| 5017      | 保险丝故障              | 0-正常；1-异常      |      |
| 5018-5023 | 预留                 |                |      |
| 5024      | 电池测试中              | 0-未测试；1-测试中    |      |
| 5025      | 电池欠压保护             | 0-正常；1-异常      | 鼎坚协议 |
| 5026      | UPS 类型             | 0-在线式；1-后备式    | 鼎坚协议 |
| 5027      | 开关机状态              | 0-关机；1-开机      | 鼎坚协议 |
| 5028      | 蜂鸣器状态              | 0-关闭；1-开启      | 鼎坚协议 |
| 5029      | 整流器异常              | 0-正常；1-异常      | 鼎坚协议 |
| 5030      | 整流器运行状态            | 0-未工作；1-运行中    | 鼎坚协议 |
| 5031      | 逆变器运行状态            | 0-未工作；1-运行中    | 鼎坚协议 |
| 5032      | 预留                 |                |      |
| 5033      | 手动旁路空开状态（维护旁路空开状态） | 0-断开；1-闭合      | 鼎坚协议 |

|      |                |           |           |
|------|----------------|-----------|-----------|
| 5034 | 预留             |           |           |
| 5035 | 过热停机（过温保护）     | 0-正常；1-异常 | 鼎坚协议      |
| 5036 | 逆变输出电压异常停机     | 0-正常；1-异常 | 鼎坚协议      |
| 5037 | 过载保护           | 0-正常；1-异常 | 鼎坚协议      |
| 5038 | 手动旁路闭合停机       | 0-正常；1-异常 | 逆变器关闭保护状态 |
| 5039 | 直流输入过高停机（母线过压） | 0-正常；1-异常 | 鼎坚协议      |
| 5040 | EPO            | 0-关闭；1-开启 | 鼎坚协议      |

注：为兼容旧版协议，对于相同项需进行或运算处理。

## 2.1.2 扩展状态量查询

| 地址        | 故障内容（显示标签）     | 逻辑含义      | 备注 |
|-----------|----------------|-----------|----|
| 5100      | 市电幅值异常         | 0-正常；1-异常 |    |
| 5101      | 预留             |           |    |
| 5102      | 市电频率异常         | 0-正常；1-异常 |    |
| 5103-5105 | 预留             |           |    |
| 5106      | 市电相序异常         | 0-正常；1-异常 |    |
| 5107-5117 | 预留             |           |    |
| 5118      | 电池回路异常         | 0-正常；1-异常 |    |
| 5119      | 电池极性接反         | 0-正常；1-异常 |    |
| 5120-5121 | 预留             |           |    |
| 5122      | 电池保险丝异常        | 0-正常；1-异常 |    |
| 5123      | 电池过充告警         | 0-正常；1-异常 |    |
| 5124      | 电池过充保护         | 0-正常；1-异常 |    |
| 5125-5131 | 预留             |           |    |
| 5132      | 旁路过压（旁路幅值异常）   | 0-正常；1-异常 |    |
| 5133      | 预留             |           |    |
| 5134      | 旁路频率过频（旁路频率异常） | 0-正常；1-异常 |    |
| 5135-5136 | 预留             |           |    |
| 5137      | 旁路相序异常         | 0-正常；1-异常 |    |
| 5138-5139 | 预留             |           |    |
| 5140      | 旁路过载保护         | 0-正常；1-异常 |    |
| 5141-5147 | 预留             |           |    |
| 5148      | 输出回路异常（输出空开断开） | 0-正常；1-异常 |    |
| 5149      | 预留             |           |    |
| 5150      | 输出过压保护         | 0-正常；1-异常 |    |
| 5151      | 输出低压保护         | 0-正常；1-异常 |    |
| 5152-5163 | 预留             |           |    |
| 5164      | 内部通讯故障         | 0-正常；1-异常 |    |
| 5165      | 预留             |           |    |



|           |             |           |  |
|-----------|-------------|-----------|--|
| 5166      | ECO 故障      | 0-正常；1-异常 |  |
| 5167      | 整流器保护       | 0-正常；1-异常 |  |
| 5168      | 逆变器保护       | 0-正常；1-异常 |  |
| 5169      | 逆变过压        | 0-正常；1-异常 |  |
| 5170      | 逆变欠压        | 0-正常；1-异常 |  |
| 5171      | 预留          |           |  |
| 5172      | 逆变过载保护      | 0-正常；1-异常 |  |
| 5173      | 逆变过温保护      | 0-正常；1-异常 |  |
| 5174-5186 | 预留          |           |  |
| 5187      | 并机线异常       | 0—正常；1—异常 |  |
| 5188      | 并机无冗余（半载告警） | 0—正常；1—异常 |  |
| 5189-5195 | 预留          |           |  |

## 2.2 读输入寄存器（模拟量）功能码 0x04

注：对于双字(32bit)或双字以上的数据，先发送高字，后发送低字。（没有检测的数据项上报 0xFFFF）。

### 2.2.1 标准模拟量查询 1（UPS 通用模拟量）

| 地址        | 意义         | 数据类型   | 备注（精度、单位及其他）                |
|-----------|------------|--------|-----------------------------|
| 5000-5001 | 预留         |        |                             |
| 5002      | 电池剩余供电时间   | UINT16 | 1min，值 0xFFFF 表示计算中         |
| 5003      | 电池剩余容量     | UINT16 | 1%                          |
| 5004      | 电池电压       | UINT16 | 0.1V                        |
| 5005      | 电池电流       | INT16  | 0.1A，正值为充电电流；负值为放电电流        |
| 5006      | 电池温度       | INT16  | 0.1℃，值 0x8000 表示温度传感器未接     |
| 5007      | 输入相数       | UINT16 |                             |
| 5008      | 预留         |        |                             |
| 5009      | 输入市电频率     | UINT16 | 0.1Hz                       |
| 5010-5018 | 预留         |        |                             |
| 5019      | 输出工作方式     | UINT16 | 0-其它输出/1-无输出/2-市电/3-旁路/4-电池 |
| 5020      | 输出频率       | UINT16 | 0.1Hz                       |
| 5021      | 输出相数       | UINT16 |                             |
| 5022      | 输出(U相)电压   | UINT16 | 0.1V                        |
| 5023      | 输出V相电压     | UINT16 | 0.1V                        |
| 5024      | 输出W相电压     | UINT16 | 0.1V                        |
| 5025      | 输出(U相)电流   | UINT16 | 0.1A                        |
| 5026      | 输出V相电流     | UINT16 | 0.1A                        |
| 5027      | 输出W相电流     | UINT16 | 0.1A                        |
| 5028      | 输出(U相)有功功率 | UINT16 | 0.1kW                       |
| 5029      | 输出V相有功功率   | UINT16 | 0.1kW                       |
| 5030      | 输出W相有功功率   | UINT16 | 0.1kW                       |
| 5031      | 输出(U相)负载率  | UINT16 | 1%                          |
| 5032      | 输出V相负载率    | UINT16 | 1%                          |

|           |             |          |                          |
|-----------|-------------|----------|--------------------------|
| 5033      | 输出 W 相负载率   | UINT16   | 1%                       |
| 5034      | 旁路输入频率      | UINT16   | 0.1Hz                    |
| 5035      | 旁路相数        | UINT16   |                          |
| 5036      | 旁路(U 相)电压   | UINT16   | 0.1V                     |
| 5037      | 旁路 V 相电压    | UINT16   | 0.1V                     |
| 5038      | 旁路 W 相电压    | UINT16   | 0.1V                     |
| 5039-5046 | 预留          |          |                          |
| 5047      | 电池运行状态      | UINT16   | 0-放电, 1-均充, 2-浮充, 3-未知   |
| 5048      | 电池节数        | UINT16   |                          |
| 5049      | 输出(U 相)视在功率 | UINT16   | 0.1kVA                   |
| 5050      | 输出 V 相视在功率  | UINT16   | 0.1kVA                   |
| 5051      | 输出 W 相视在功率  | UINT16   | 0.1kVA                   |
| 5052      | 环境温度 (机内温度) | INT16    | 0.1℃, 值 0x8000 表示温度传感器未接 |
| 5053      | 工作制式        | UINT16   | 0-3/3,1-3/1,2-1/1,1/3    |
| 5054      | 额定输出电压      | UINT16   | 1V                       |
| 5055      | 预留          |          |                          |
| 5056      | 额定输出频率      | UINT16   | 1Hz                      |
| 5057      | 额定输出功率      | UINT16   | 1kVA                     |
| 5058      | 额定电池电压      | UINT16   | 1V                       |
| 5059-5076 | 预留          |          |                          |
| 5077-5108 | 制造商         | 64*ASCII |                          |
| 5109-5140 | 产品型号        | 64*ASCII |                          |
| 5141-5144 | 预留          |          |                          |

### 2.2.2 标准模拟量查询 2 (UPS 扩展模拟量)

| 地址        | 意义         | 数据类型    | 备注 (精度、单位及其他)  |
|-----------|------------|---------|--|
| 5200      | 市电 U-V 线电压 | UINT16  | 0.1V   |
| 5201      | 市电 V-W 线电压 | UINT16  | 0.1V   |
| 5202      | 市电 W-U 线电压 | UINT16  | 0.1V   |
| 5203      | 旁路 U-V 线电压 | UINT16  | 0.1V   |
| 5204      | 旁路 V-W 线电压 | UINT16  | 0.1V   |
| 5205      | 旁路 W-U 线电压 | UINT16  | 0.1V   |
| 5206      | 输出 U-V 线电压 | UINT16  | 0.1V   |
| 5207      | 输出 V-W 线电压 | UINT16  | 0.1V   |
| 5208      | 输出 W-U 线电压 | UINT16  | 0.1V   |
| 5209-5211 | 预留         |         |  |
| 5212      | 输出 U 相功率因数 | UINT16  | 0.01   |
| 5213      | 输出 V 相功率因数 | UINT16  | 0.01   |
| 5214      | 输出 W 相功率因数 | UINT16  | 0.01   |
| 5215-5223 | 预留         |         |  |
| 5224      | 系统运行状态     | UINT16  | 0-关机; 1-旁路; 2-逆变; 3-维护旁路; 4-故障; 5-ECO 供电; 6-EPO; 7 待机;8-调试模式 |
| 5225-5228 | HMI 软件版本   | 8*ASCII |  |
| 5229-5232 | 整流器软件版本    | 8*ASCII |  |
| 5233-5236 | 逆变器软件版本    | 8*ASCII |  |
| 5237-5240 | 预留         |         |  |
| 5241-5244 | 系统版本       | 8*ASCII |  |

## 2.3 读写线圈（状态量）读功能码 0x01，写功能码 0x05

### 2.3.1 标准状态量设置

| 地址        | 意义      | 数据长度   | 备注（精度、单位及其他） |
|-----------|---------|--------|--------------|
| 5900      | 立即开关机设置 | UINT16 | 1 开机；0-关机    |
| 5901-5902 | 预留      |        |              |

## 2.4 写单个保持寄存器（模拟量）功能码 0x06

### 2.4.1 标准模拟量设置

| 地址        | 意义    | 数据长度   | 备注（精度、单位及其他）   |
|-----------|-------|--------|----------------|
| 5400-5401 | 预留    |        |                |
| 5402      | 蜂鸣器设置 | UINT16 | 0-关闭；1-开启；2-静音 |
| 5403-5404 | 预留    |        |                |

## 2.5 写多个保持寄存器（模拟量）功能码 0x10

| 地址        | 意义     | 数据长度   | 备注（精度、单位及其他） |
|-----------|--------|--------|--------------|
| 5500      | 系统时间-年 | UINT16 | 2000~2099    |
| 5501      | 系统时间-月 | UINT16 | 1~12         |
| 5502      | 系统时间-日 | UINT16 | 支持闰年，大小月     |
| 5503      | 系统时间-时 | UINT16 | 0~23         |
| 5504      | 系统时间-分 | UINT16 | 0~59         |
| 5505      | 系统时间-秒 | UINT16 | 0~59         |
| 5506-5507 | 预留     |        |              |

# A Modbus 通信协议

## A.1 功能码描述

本协议适用于主从工作方式的通信，主站循环向从站要求数据，从站接收请求指令，并应答相应数据。

本协议仅用到标准 Modbus 协议的部分功能码，具体如下表。

| 功能码  | 含义     | 备注                     |
|------|--------|------------------------|
| 0x01 | 读线圈    | 按字节读取                  |
| 0x02 | 读离散量输入 | 按字节读取                  |
| 0x03 | 读保持寄存器 | 按字读取                   |
| 0x04 | 读输入寄存器 | 按字读取                   |
| 0x05 | 写单个线圈  | OFF-0x0000 ; ON-0xFF00 |
| 0x06 | 写单个寄存器 | 按字写                    |
| 0x10 | 写多个寄存器 | 按字写                    |

## A.2 Modbus RTU 指令详述

### A.2.1 读线圈（功能码：0x01）

主站指令(16 进制)

| 站号 | 功能码  | 寄存器起始地址 |     | 数量  |     | CRC16 |     |
|----|------|---------|-----|-----|-----|-------|-----|
|    |      | 高字节     | 低字节 | 高字节 | 低字节 | 低字节   | 高字节 |
| xx | 0x01 | xx      | xx  | xx  | xx  | xx    | xx  |

## 从站回复(16 进制)

| 站号 | 功能码  | 字节数 | 第 1 字节<br>线圈状态 | ... | 第 N 字节<br>线圈状态 | CRC16 |     |
|----|------|-----|----------------|-----|----------------|-------|-----|
|    |      |     |                |     |                | 低字节   | 高字节 |
| xx | 0x01 | xx  | xx             | ... | xx             | xx    | xx  |

 说明

回复信息中的第 1 字节线圈状态的最低位对应查询中的寻址地址，由低位到高位顺序排列，直至 8 个位为止，下一个字节中的 8 个位也是从低位到高位顺序排列。若返回的信号点数量小于 8 或者不是 8 的整数倍，则在最后一组信号点的剩余位直至最高位全部填零。

## A.2.2 读离散量输入（功能码：0x02）

## 主站指令(16 进制)

| 站号 | 功能码  | 寄存器起始地址 |     | 数量  |     | CRC16 |     |
|----|------|---------|-----|-----|-----|-------|-----|
|    |      | 高字节     | 低字节 | 高字节 | 低字节 | 低字节   | 高字节 |
| xx | 0x02 | xx      | xx  | xx  | xx  | xx    | xx  |

## 从站回复(16 进制)

| 站号 | 功能码  | 字节数 | 第 1 组<br>信号点 | ... | 第 N 组<br>信号点 | CRC16 |     |
|----|------|-----|--------------|-----|--------------|-------|-----|
|    |      |     |              |     |              | 低字节   | 高字节 |
| xx | 0x02 | xx  | xx           | ... | xx           | xx    | xx  |

 说明

回复信息中的第 1 字节离散量的最低位对应查询中的寻址地址，由低位到高位顺序排列，直至 8 个位为止，下一个字节中的 8 个位也是从低位到高位顺序排列。若返回的信号点数量小于 8 或者不是 8 的整数倍，则在最后一组信号点的剩余位直至最高位全部填零。

### A.2.3 读保持寄存器（功能码：0x03）

#### 主站指令(16 进制)

| 站号 | 功能码  | 寄存器起始地址 |     | 寄存器数量 |     | CRC16 |     |
|----|------|---------|-----|-------|-----|-------|-----|
|    |      | 高字节     | 低字节 | 高字节   | 低字节 | 低字节   | 高字节 |
| xx | 0x03 | xx      | xx  | xx    | xx  | xx    | xx  |

#### 从站回复(16 进制)

| 站号 | 功能码  | 字节数 | 寄存器 1 |     | ... |     | 寄存器 N |     | CRC16 |     |
|----|------|-----|-------|-----|-----|-----|-------|-----|-------|-----|
|    |      |     | 高字节   | 低字节 | ... | ... | 高字节   | 低字节 | 低字节   | 高字节 |
| xx | 0x03 | xx  | xx    | xx  | ... | ... | xx    | xx  | xx    | xx  |

 说明

读一个或多个寄存器通过寄存器数量来区分，寄存器数量为 1 则为一个寄存器，大于 1 则为多个寄存器。寄存器 1 对应起始地址。

### A.2.4 读输入寄存器（功能码：0x04）

#### 主站指令(16 进制)

| 站号 | 功能码  | 寄存器起始地址 |     | 寄存器数量 |     | CRC16 |     |
|----|------|---------|-----|-------|-----|-------|-----|
|    |      | 高字节     | 低字节 | 高字节   | 低字节 | 低字节   | 高字节 |
| xx | 0x04 | xx      | xx  | xx    | xx  | xx    | xx  |

## 从站回复(16 进制)

| 站号 | 功能码  | 字节数 | 寄存器 1 |     | ... |     | 寄存器 N |     | CRC16 |     |
|----|------|-----|-------|-----|-----|-----|-------|-----|-------|-----|
|    |      |     | 高字节   | 低字节 | ... | ... | 高字节   | 低字节 | 低字节   | 高字节 |
| xx | 0x04 | xx  | xx    | xx  | ... | ... | xx    | xx  | xx    | xx  |

 说明

读一个或多个寄存器通过寄存器数量来区分，寄存器数量为 1 则为一个寄存器，大于 1 则为多个寄存器。  
寄存器 1 对应起始地址。

## A.2.5 写单个线圈（功能码：0x05）

## 主站指令(16 进制)

| 站号 | 功能码  | 寄存器地址 |     | 寄存器设定值 |     | CRC16 |     |
|----|------|-------|-----|--------|-----|-------|-----|
|    |      | 高字节   | 低字节 | 高字节    | 低字节 | 低字节   | 高字节 |
| xx | 0x05 | xx    | xx  | xx     | xx  | xx    | xx  |

 说明

由于写输入状态仅有 ON/OFF 状态，0xFF00 请求输入状态为 ON 状态，0x0000 请求输入状态为 OFF 状态。

## 从站回复(16 进制)

| 站号 | 功能码  | 寄存器地址 |     | 寄存器设定值 |     | CRC16 |     |
|----|------|-------|-----|--------|-----|-------|-----|
|    |      | 高字节   | 低字节 | 高字节    | 低字节 | 低字节   | 高字节 |
| xx | 0x05 | xx    | xx  | xx     | xx  | xx    | xx  |

## A.2.6 写单个寄存器（功能码：0x06）

## 主站指令(16 进制)

| 站号 | 功能码  | 寄存器地址 |     | 寄存器设定值 |     | CRC16 |     |
|----|------|-------|-----|--------|-----|-------|-----|
|    |      | 高字节   | 低字节 | 高字节    | 低字节 | 低字节   | 高字节 |
| xx | 0x06 | xx    | xx  | xx     | xx  | xx    | xx  |

## 从站回复(16 进制)

| 站号 | 功能码  | 寄存器地址 |     | 寄存器设定值 |     | CRC16 |     |
|----|------|-------|-----|--------|-----|-------|-----|
|    |      | 高字节   | 低字节 | 高字节    | 低字节 | 低字节   | 高字节 |
| xx | 0x06 | xx    | xx  | xx     | xx  | xx    | xx  |

## A.2.7 写多个寄存器（功能码：0x10）

## 主站指令(16 进制)

| 站号 | 功能码  | 寄存器设置起始地址 |     | 寄存器设置数量(N) |     | 字节数<br>2*N | 寄存器设定值 |     | 寄存器... | CRC16 |     |
|----|------|-----------|-----|------------|-----|------------|--------|-----|--------|-------|-----|
|    |      | 高字节       | 低字节 | 高字节        | 低字节 |            | 高字节    | 低字节 |        | 低字节   | 高字节 |
| xx | 0x10 | xx        | xx  | xx         | xx  | xx         | xx     | xx  | ...    | xx    | xx  |

## 从站回复(16 进制)

| 站号 | 功能码  | 寄存器地址 |     | 预设寄存器数 |     | CRC16 |     |
|----|------|-------|-----|--------|-----|-------|-----|
|    |      | 高字节   | 低字节 | 高字节    | 低字节 | 低字节   | 高字节 |
| xx | 0x10 | xx    | xx  | xx     | xx  | xx    | xx  |

## A.2.8 错误信息及数据的处理

## 从站回复(16 进制)

| 地址 | 功能码     | 错误码 | CRC16 |     |
|----|---------|-----|-------|-----|
|    |         |     | 低字节   | 高字节 |
| xx | xx 0x80 | xx  | xx    | xx  |

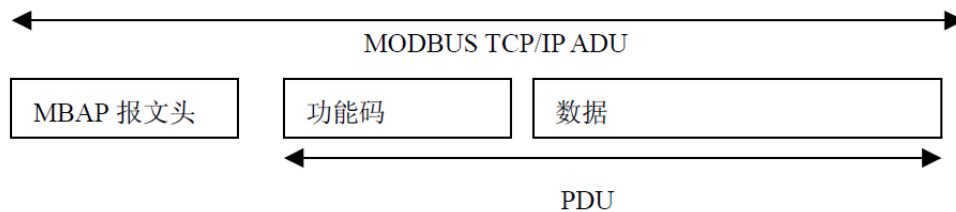
从站通信模块检测到除了 CRC 码出错以外的错误时，必须向主站回送信息，功能码的最高位置为 1，即在主站发送的功能码的基础上加 128。从站通信模块响应回送的错误码：

- 0x01 非法的功能码 服务器不了解功能码
- 0x02 非法的数据地址 与请求有关
- 0x03 非法的数据值 与请求有关



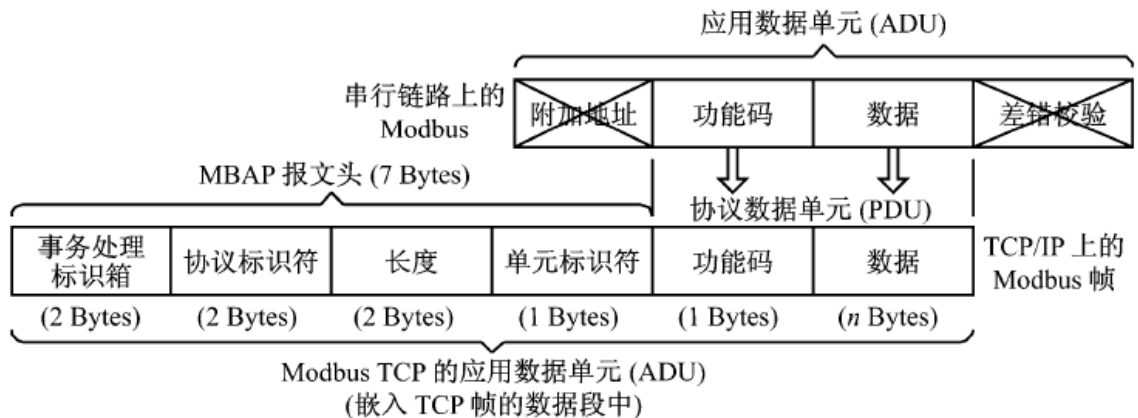
- 0x04 服务故障 从站通信模块在执行过程中无法取出数据故障
- 0x10 错误的寄存器设定值（密码输入不匹配、设置越界等）
- 0x11 无权限

### A.3 Modbus TCP 指令详述



在 TCP/IP 上使用一种专用报文头识别 Modbus 应用数据单元，称为 MBAP 报文头（Modbus 协议报文头）。

Modbus TCP 数据帧与串行链路数据帧的区别：



MBAP 报文头包括下列域：

| 域      | 长度     | 描述                    | 客户机        | 服务器            |
|--------|--------|-----------------------|------------|----------------|
| 事务元标识符 | 2 Byte | Modbus 请求响应事务处理的识别码   | 客户机启动      | 服务器从接收的请求中重新复制 |
| 协议标识符  | 2 Byte | 0: Modbus 协议          | 客户机启动      | 服务器从接收的请求中重新复制 |
| 长度     | 2 Byte | 以下字节的数量               | 客户机启动 (请求) | 服务器 (响应) 启动    |
| 单元标识符  | 1 Byte | 串行链路或其它总线上连接的远程从站的识别码 | 客户机启动      | 服务器从接收的请求中重新复制 |

报文头为 7 个字节长：

- 事务处理标识符：用于事务处理配对。在响应中，Modbus 服务器复制请求的事务处理标识符。
- 协议标识符：用于系统内的多路复用。通过值 0 识别 Modbus 协议。
- 长度：长度域是下一个域的字节数，包括单元标识符和数据域。
- 单元标识符：为了系统内路由，使用这个域。专门用于通过以太网 TCP-IP 网络和 Modbus 串行链路之间的网关对 Modbus 或 Modbus+ 串行链路从站的通信。Modbus 客户机在请求中设置这个域，在响应中服务器必须利用相同的值返回这个域。
- 在注册的 502 端口上利用 TCP 发送所有 Modbus/TCP ADU。

### A.3.1 读线圈（功能码：0x01）

请求 PDU

| 功能码  | 起始地址 |     | 数量  |     |
|------|------|-----|-----|-----|
|      | 高字节  | 低字节 | 高字节 | 低字节 |
| 0x01 | xx   | xx  | xx  | xx  |

响应 PDU

| 功能码  | 字节数 | 第 1 字节线圈状态 | ... | 第 N 字节线圈状态 |
|------|-----|------------|-----|------------|
| 0x01 | xx  | xx         | ... | xx         |

 说明

回复信息中的第 1 字节线圈状态的最低位对应查询中的寻址地址，由低位到高位顺序排列，直至 8 个位为止，下一个字节中的 8 个位也是从低位到高位顺序排列。若返回的信号点数量小于 8 或者不是 8 的整数倍，则在最后一组信号点的剩余位直至最高位全部填零。

### A.3.2 读离散量输入（功能码：0x02）

请求 PDU

| 功能码  | 起始地址 |     | 数量  |     |
|------|------|-----|-----|-----|
|      | 高字节  | 低字节 | 高字节 | 低字节 |
| 0x02 | xx   | xx  | xx  | xx  |

## 响应 PDU

| 功能码  | 字节数 | 第 1 组信号点 | ... | 第 N 组信号点 |
|------|-----|----------|-----|----------|
| 0x02 | xx  | xx       | ... | xx       |

 说明

回复信息中的第 1 字节离散量的最低位对应查询中的寻址地址,由低位到高位顺序排列,直至 8 个位为止,下一个字节中的 8 个位也是从低位到高位顺序排列。若返回的信号点数量小于 8 或者不是 8 的整数倍,则在最后一组信号点的剩余位直至最高位全部填零。

## A.3.3 读保持寄存器（功能码：0x03）

## 请求 PDU

| 功能码  | 起始地址 |     | 寄存器数量 |     |
|------|------|-----|-------|-----|
|      | 高字节  | 低字节 | 高字节   | 低字节 |
| 0x03 | xx   | xx  | xx    | xx  |

## 响应 PDU

| 功能码  | 字节数 | 寄存器 1 |     | ... |     | 寄存器 N |     |
|------|-----|-------|-----|-----|-----|-------|-----|
|      |     | 高字节   | 低字节 | ... | ... | 高字节   | 低字节 |
| 0x03 | xx  | xx    | xx  | ... | ... | xx    | xx  |

 说明

读一个或多个寄存器通过寄存器数量来区分,寄存器数量为 1 则为一个寄存器,大于 1 则为多个寄存器。寄存器 1 对应起始地址。

## A.3.4 读输入寄存器（功能码：0x04）

## 请求 PDU

| 功能码  | 起始地址 |     | 寄存器数量 |     |
|------|------|-----|-------|-----|
|      | 高字节  | 低字节 | 高字节   | 低字节 |
| 0x04 | xx   | xx  | xx    | xx  |

## 响应 PDU

| 功能码  | 字节数 | 寄存器 1 |     | ... |     | 寄存器 N |     |
|------|-----|-------|-----|-----|-----|-------|-----|
|      |     | 高字节   | 低字节 | ... | ... | 高字节   | 低字节 |
| 0x04 | xx  | xx    | xx  | ... | ... | xx    | xx  |

 说明

读一个或多个寄存器通过寄存器数量来区分，寄存器数量为 1 则为一个寄存器，大于 1 则为多个寄存器。  
寄存器 1 对应起始地址。

## A.3.5 写单个线圈（功能码：0x05）

## 请求 PDU

| 功能码  | 寄存器地址 |     | 寄存器设定值 |     |
|------|-------|-----|--------|-----|
|      | 高字节   | 低字节 | 高字节    | 低字节 |
| 0x05 | xx    | xx  | xx     | xx  |

 说明

由于写输入状态仅有 ON/OFF 状态，0xFF00 请求输入状态为 ON 状态，0x0000 请求输入状态为 OFF 状态。

## A.3.6 写单个寄存器（功能码：0x06）

## 请求 PDU

| 功能码  | 寄存器地址 |     | 寄存器设定值 |     |
|------|-------|-----|--------|-----|
|      | 高字节   | 低字节 | 高字节    | 低字节 |
| 0x06 | xx    | xx  | xx     | xx  |

## 响应 PDU

| 功能码  | 寄存器地址 |     | 寄存器设定值 |     |
|------|-------|-----|--------|-----|
|      | 高字节   | 低字节 | 高字节    | 低字节 |
| 0x06 | xx    | xx  | xx     | xx  |

### A.3.7 写多个寄存器（功能码：0x10）

请求 PDU

| 功能码  | 寄存器设置起始地址 |     | 寄存器设置数量 (N) |     | 字节数 | 寄存器设定值 |     | 寄存器... |     |
|------|-----------|-----|-------------|-----|-----|--------|-----|--------|-----|
|      | 高字节       | 低字节 | 高字节         | 低字节 | 2*N | 高字节    | 低字节 | ...    | ... |
| 0x10 | xx        | xx  | xx          | xx  | xx  | xx     | xx  | ...    | ... |

响应 PDU

| 功能码  | 寄存器地址 |     | 预设寄存器数 |     |
|------|-------|-----|--------|-----|
|      | 高字节   | 低字节 | 高字节    | 低字节 |
| 0x10 | xx    | xx  | xx     | xx  |

### A.3.8 错误信息及数据的处理

响应 PDU

| 功能码     | 错误码 |
|---------|-----|
| xx 0x80 | xx  |

从站通信模块检测到除了 CRC 码出错以外的错误时，必须向主站回送信息，功能码的最高位置为 1，即在主站发送的功能码的基础上加 128。从站通信模块响应回送的错误码：

- 0x01 非法的功能码 服务器不了解功能码
- 0x 02 非法的数据地址 与请求有关
- 0x 03 非法的数据值 与请求有关
- 0x 04 服务故障 从站通信模块在执行过程中无法取出数据故障。



科华数据股份有限公司

---

地址：厦门火炬高新区火炬园马垄路457号

邮编：361000

电话：0592-5160516

传真：0592-5162166

网址：[www.kehua.com.cn](http://www.kehua.com.cn)

WRWF-0A099-01 002