

无锡信捷电气股份有限公司技术文档

卷 号：

卷内编号：

V2.0版

Modbus通讯协议软件开发

**产品规格说明书**

Product Specification

|  |  |
| --- | --- |
| 项 目 承 担 部 门 | 研发中心/培训部/研发训练营 |
| 撰 写 人（签名） | 姚京序 |
| 完 成 日 期 | 2020.08.26 |
| 评 审 负 责 人（签名）： |  |
| 评 审 日 期： |  |

表1 产品规格书基本信息

目录

[1. 引言 1](#_Toc18327)

[1.1. 开发目的 1](#_Toc22638)

[1.2. 限制与约束 1](#_Toc20425)

[1.3. 术语与缩略词 1](#_Toc14282)

[2. 软件概要 2](#_Toc29310)

[2.1. 总体要求 2](#_Toc4967)

[2.2. 软件结构 2](#_Toc521)

[3. 功能概要 2](#_Toc13501)

[3.1. 总体要求 2](#_Toc2247)

[4. TCP模式 3](#_Toc20587)

[4.1. TCP通讯指标 3](#_Toc21927)

[4.2. TCP通讯数据帧 4](#_Toc31535)

[4.3. 数据帧样例 5](#_Toc19921)

[4.3.1. 功能码0x01 5](#_Toc9063)

[4.3.2. 功能码0x03 5](#_Toc13474)

[4.3.3. 功能码0x0F 6](#_Toc7082)

[4.3.4. 功能码0x10 7](#_Toc25682)

[5. RTU模式 8](#_Toc26443)

[5.1. RTU通信指标 8](#_Toc1279)

[5.2. RTU通信数据帧 9](#_Toc16313)

[5.3. 数据帧样例 10](#_Toc31993)

[5.3.1. 功能码0x01 10](#_Toc16923)

[5.3.2. 功能码0x03 10](#_Toc27776)

[5.3.3. 功能码0x0F 11](#_Toc28318)

[5.3.4. 功能码0x10 12](#_Toc22610)

[6. 异常码 13](#_Toc12099)

[6.1. 异常码说明 13](#_Toc436)

[6.2. 异常码响应数据帧 13](#_Toc2626)

|  |  |  |  |
| --- | --- | --- | --- |
| 完成日期 | 版本号 | 审核人 | 作者 |
| 2020年8月21日 | V1.0 |  | Somuns |
| 2020年8月27日 | V2.0 |  | Somuns |
|  |  |  |  |
|  |  |  |  |

表2 产品规格书修改记录

# 引言

## 开发目的

所有支持 Modbus协议的工控设备进行通信的软件。

## 限制与约束

开发期限：2020年9月10日前全部完成。

硬件限制：应使用PLC设备进行Modbus串口通讯，但可能会由于实际情况采用虚拟串口的方式进行串口通讯。

编程语言：C#（含界面UI设计）

## 术语与缩略词

|  |  |
| --- | --- |
| 名称 | 释义 |
| Master | 主设备 |
| Slave | 从设备 |
| Client | 客户端 |
| Server | 服务器 |
| ADU | 应用数据单元 |
| PDU | 协议数据单元 |
| MSB | 最高有效位 |
| LSB | 最低有效位 |
| TCP | 面向广域网的通信协议 |
| MBAP | ModbusTCP数据帧报头 |
| PLC | 可编程逻辑控制器 |

表2-1 名词解释

# 软件概要

## 总体要求

编写程序，完成基于Modbus的

①：TCP/IP(无线)通信，

②：RTU（串口）通信。

## 软件结构

Modbus的TCP/IP(无线)通信采用B/S模式。

Modbus的RTU(串口)通信采用B/S模式。

# 功能概要

## 总体要求

1. 需要实现下表3-1 中功能

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 功能码 | 作用 | 从机地址 | 位/字操作 | 操作数 |
| 0x01 | 读线圈 | 00001-09999 | 位操作 | 单个或多个 |
| 0x03 | 读保持寄存器 | 40001-49999 | 字操作 | 单个或多个 |
| 0x0F | 写多个线圈 | 00001-09999 | 位操作 | 多个 |
| 0x10 | 写多个保持寄存器 | 40001-49999 | 字操作 | 多个 |

表3-1 Modbus功能码说明

2、能够检验数据传输是否正确（CRC等）。

3、编写串口驱动和网口驱动来实现 Modbus 通信，可以和所有支持 Modbus协议的工控设备进行通信。

4、软件能够按 Modbus 协议读取从机寄存器、线圈的值，能够写数据到从机寄存器、线圈中。

5、TCP模式：检测从机返回的数据帧是否正常。异常则丢弃。

RTU模式：检测主机发送的数据帧是否合理，合理则返回正常数据帧；若异常，则返回异常数据帧。

（详见6.2.异常码响应数据帧）

# TCP模式

## TCP通讯指标

设备：PLC主站（TCP客户端）

通信模块：WIFI / 网线

异常响应：要求远程端口异常关闭或故障，主站立即显示断连信息。

响应超时：可自主设置，合适范围为（0-2000ms）

连接超时：主机在尝试与从机建立连接，远端因故障尝试连接最大时长不得超过7秒。

通信协议说明：

该**查询报文**共需要发送的数据有：MBAP、FUNC、DATA。（下文详细说明）

## TCP通讯数据帧

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 名称 | MBAP | | | | FUNC | DATA | |
|  | 传输标识 | 协议标识 | 长度 | 单元标识 | 功能码 | 地址 | 数量 |
| 字节 | 2 | 2 | 2 | 1 | 1 | 2 | 2 |

表4-1 Tcp模式查询报文数据帧基本格式

说明：

**传输标识**：“TCP发送顺序号”,在每一个请求发送时自动＋1;来识别事务处理的内容，以便记忆当前的远端服务器和未处理的请求，最大表示65535，达到极值置0。占2字节，

**协议标识：**在TCP中固定为0x00，0x00，占两字节。

**长度：**剩余字节长度**，**在TCP中由客户端生成，占两字节。

**单元标识符：**对于直连的设备而言，使用0xFF填充，对于多设备连接情况而言，需要更改为设备ID。占1字节。

**功能码：**本通讯协议中，选定了0x01、0x03、0x0F、0x10四个功能码，其余为无效功能码。占1字节。

**数据：**在查询报文中，

前两个字节为**Modbus起始地址**，且高位在前、低位在后。占2字节。

后两个字节为**读取的线圈或寄存器个数**，同样为高位在前低位在后。

占2字节。共占4字节。

## **数据帧样例**

### 功能码0x01

**查询报文**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 名称 | MBAP | | | | FUNC | DATA | |
|  | 传输标识 | 协议标识 | 长度 | 单元标识 | 功能码 | 地址 | 数量 |
| 数据 | 00 01 | 00 00 | 00 06 | 01 | 01 | 00 04 | 00 01 |

**响应报文**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 名称 | MBAP | | | | FUNC | DATA | |
|  | 传输标识 | 协议标识 | 长度 | 单元标识 | 功能码 | 长度 | 值 |
| 数据 | 00 01 | 00 00 | 00 04 | 01 | 01 | 01 | 01 |

### 功能码0x03

**查询报文**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 名称 | MBAP | | | | FUNC | DATA | |
|  | 传输标识 | 协议标识 | 长度 | 单元标识 | 功能码 | 地址 | 数量 |
| 数据 | 00 02 | 00 00 | 00 06 | 01 | 03 | 00 04 | 00 01 |

**响应报文**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 名称 | MBAP | | | | FUNC | DATA | |
|  | 传输标识 | 协议标识 | 长度 | 单元标识 | 功能码 | 长度 | 值 |
| 数据 | 00 02 | 00 00 | 00 06 | 01 | 03 | 02 | 00 05 |

### 功能码0x0F

**查询报文**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 名称 | MBAP | | | | FUNC | DATA | |
|  | 传输标识 | 协议标识 | 长度 | 单元标识 | 功能码 | 地址 | 数量 |
| 数据 | 00 03 | 00 00 | 00 08 | 01 | 0F | 00 04 | 00 0B |

|  |  |
| --- | --- |
| CHANGE | |
| 变更数据 | |
| D1 | 05 |

**响应报文**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 名称 | MBAP | | | | FUNC | DATA | |
|  | 传输标识 | 协议标识 | 长度 | 单元标识 | 功能码 | 地址 | 数量 |
| 数据 | 00 03 | 00 00 | 00 06 | 01 | 0F | 00 04 | 00 0B |

### 功能码0x10

**查询报文**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 名称 | MBAP | | | | FUNC | DATA | |
|  | 传输标识 | 协议标识 | 长度 | 单元标识 | 功能码 | 地址 | 数量 |
| 数据 | 00 04 | 00 00 | 00 0C | 01 | 10 | 00 13 | 00 03 |

|  |  |  |
| --- | --- | --- |
| CHANGE | | |
| 变更数据 | | |
| 01 55 | 01 56 | 01 57 |

**响应报文**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 名称 | MBAP | | | | FUNC | DATA | |
|  | 传输标识 | 协议标识 | 长度 | 单元标识 | 功能码 | 地址 | 数量 |
| 数据 | 00 04 | 00 00 | 00 06 | 01 | 10 | 00 13 | 00 03 |

# RTU模式

## RTU通信指标

USART（串口）通信基本设置：

|  |  |  |  |
| --- | --- | --- | --- |
| 参数名 |  | 可设定 | 拟设定 |
| Baud Rate | 波特率 | 9600/115200 | 9600 |
| Data Bits | 数据位 | 5/7/8 | 8 |
| Parity Bit | 奇偶校验位 | 奇/偶 | 偶 |
| Stop Bit | 停止位 | 1/1.5/2 | 1 |

表 5-1 USART（串口）通信基本设置

设备：RTU从站

通信模块：拟采用RS485，或根据实际情况采用虚拟串口。

超时时间：消息发送和接收以3.5个字符时间(4.0ms)间隔为标志。

通信协议说明：

该**响应报文**共需要发送的数据有：

S\_ADDR、FUNC、LENGTH、DATA、CRC。

## RTU通信数据帧

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | S\_ADDR | FUNC | LENGTH | DATA | CRC |
|  | 从机地址 | 功能码 | 长度 | 数据 | CRC校验 |
| 字节 | 1 | 1 | 1 | 不定长 | 2 |

说明：

**从机地址：**同查询报文。占1字节。

**功能码：**同查询报文。占1字节。

**长度：**剩余字节长度，占1字节。

**响应数据：**正常响应报文中包含了寄存器、线圈等信息；

异常响应报文中功能码最高位置1，同时不包含DATA信息，下一字节包含异常码。（详见6.2.异常码响应数据帧）

**CRC校验：**冗余循环校验码，占2字节。

## 数据帧样例

### 功能码0x01

**查询报文**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | S\_ADDR | FUNC | R\_ADDR | R\_AMOUNT | CRC |
|  | 从机地址 | 功能码 | 线圈地址 | 线圈数 | CRC校验 |
| 数据（HEX） | 01 | 01 | 00 13 | 00 25 | 2（字节） |

**响应报文**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | S\_ADDR | FUNC | LENGTH | DATA | CRC |
|  | 从机地址 | 功能码 | 长度 | 数据 | CRC校验 |
| 数据（HEX） | 01 | 01 | 05 | 53 6B 01 F4 1B | 2（字节） |

### 功能码0x03

**查询报文**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | S\_ADDR | FUNC | R\_ADDR | R\_AMOUNT | CRC |
|  | 从机地址 | 功能码 | 寄存器地址 | 寄存器数 | CRC校验 |
| 数据（HEX） | 07 | 03 | 00 C8 | 00 03 | 2（字节） |

**响应报文**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | S\_ADDR | FUNC | LENGTH | DATA | CRC |
|  | 从机地址 | 功能码 | 长度 | 数据 | CRC校验 |
| 数据（HEX） | 07 | 03 | 06 | 03 53  01 F3 01 05 | 2（字节） |

### 功能码0x0F

**查询报文**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | S\_ADDR | FUNC | R\_ADDR | R\_AMOUNT | LENGTH |
|  | 从机地址 | 功能码 | 线圈地址 | 线圈数 | 字节数 |
| 数据（HEX） | 05 | 0F | 00 13 | 00 0B | 02 |

|  |  |
| --- | --- |
| CHANGE | CRC |
| 变更数据 | CRC校验 |
| D1 05 | 2（字节） |

**响应报文**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | S\_ADDR | FUNC | DATA | | CRC |
|  | 从机地址 | 功能码 | 地址 | 数量 | CRC校验 |
| 数据（HEX） | 05 | 0F | 00 13 | 00 0B | 2（字节） |

### 功能码0x10

**查询报文**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | S\_ADDR | FUNC | R\_ADDR | R\_AMOUNT | LENGTH |
|  | 从机地址 | 功能码 | 寄存器地址 | 寄存器数 | 字节数 |
| 数据（HEX） | 05 | 10 | 00 13 | 00 03 | 06 |

|  |  |
| --- | --- |
| CHANGE | CRC |
| 变更数据 | CRC校验 |
| 01 55 01 56 01 57 | 2（字节） |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | S\_ADDR | FUNC | R\_ADDR | R\_AMOUNT | CRC |
|  | 从机地址 | 功能码 | 寄存器地址 | 寄存器数 | CRC校验 |
| 数据（HEX） | 05 | 10 | 00 13 | 00 03 | 2（字节） |

**响应报文**

# 异常码

## 异常码说明

|  |  |  |
| --- | --- | --- |
| 异常码 | 名称 | 说明 |
| 01 | 非法功能码 | 从站设备不支持此功能码 |
| 02 | 非法数据地址 | 指定的数据地址在从站设备中不存在 |
| 03 | 非法数据值 | 指定的数据超过范围或者不允许使用 |
| 04 | 从站设备故障 | 从站设备处理响应的过程中  出现未知错误等 |

表 6-1 异常码及其对应说明

## 异常码响应数据帧样例

### 异常码0x01

**查询报文（读线圈）**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | S\_ADDR | FUNC | R\_ADDR | R\_AMOUNT | CRC |
|  | 从机地址 | 功能码 | 地址 | 数量 | CRC校验 |
| 数据（HEX） | 07 | 01 | 00 00 | 00 0A | 2（字节） |

**响应报文**

**（从机此时开的寄存器）**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | S\_ADDR | FUNC | ERR\_CODE | CRC |
|  | 从机地址 | 功能码 | 异常码 | CRC校验 |
| 字节 | 1 | 1 | 1 | 2 |
| 数据 | 07 | 81 | 01 | CRC（2字节） |

### 异常码0x02

**查询报文（读、写）**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | S\_ADDR | FUNC | R\_ADDR | R\_AMOUNT | CRC |
|  | 从机地址 | 功能码 | 地址 | 数量 | CRC校验 |
| 数据（HEX） | 07 | 01 | 00 01 | FF FF | 2（字节） |

**响应报文**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | S\_ADDR | FUNC | ERR\_CODE | CRC |
|  | 从机地址 | 功能码 | 异常码 | CRC校验 |
| 字节 | 1 | 1 | 1 | 2 |
| 数据 | 07 | 81 | 02 | CRC（2字节） |

### 异常码0x03

**查询报文（读、写）**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | S\_ADDR | FUNC | R\_ADDR | R\_AMOUNT | CRC |
|  | 从机地址 | 功能码 | 地址 | 数量 | CRC校验 |
| 数据（HEX） | 07 | 01 | 00 01 | 00 00 | 2（字节） |

**响应报文**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | S\_ADDR | FUNC | ERR\_CODE | CRC |
|  | 从机地址 | 功能码 | 异常码 | CRC校验 |
| 字节 | 1 | 1 | 1 | 2 |
| 数据 | 07 | 81 | 03 | CRC（2字节） |