

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

**产品方案说明书**

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](#_Toc30789)

[1.1. 开发目的 1](#_Toc25685)

[1.2. 限制与约束 1](#_Toc32111)

[1.3. 产品描述 1](#_Toc31025)

[2. 软件开发流程 2](#_Toc21484)

[2.1. 软件总体流程设计 2](#_Toc12322)

[2.1.1. Modbus Tcp 主站 2](#_Toc4859)

[2.1.2. Modbus Rtu 从站 3](#_Toc3572)

[2.2. Tcp主站主要模块 4](#_Toc21680)

[2.2.1. 建立连接 4](#_Toc13045)

[2.2.2. 数据帧生成 6](#_Toc13419)

[2.2.3. 发送、接收数据显示 8](#_Toc44)

[2.2.4. 响应报文解析 10](#_Toc32176)

[2.2.5. 超时显示 12](#_Toc12091)

[2.3. Rtu从站主要模块 13](#_Toc30469)

[2.3.1. 连接配置 13](#_Toc14935)

[2.3.2. 开线圈、寄存器 14](#_Toc20613)

[2.3.3. Crc校验 16](#_Toc7418)

[2.3.4. 查询报文解析 17](#_Toc15433)

[2.3.5. 接收、发送数据显示 18](#_Toc31554)

|  |  |  |  |
| --- | --- | --- | --- |
| 完成日期 | 版本号 | 审核人 | 作者 |
| 2020年8月29日 | V1.0 |  | Somuns |
| 2020年9月15日 | V2.0 |  | Somuns |
|  |  |  |  |
|  |  |  |  |

表2 产品方案书修改记录

# 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。

## 产品描述

Modbus是一种通信协议,诞生至今已有近40年，在随时间不断地发展当中，Modbus已经成为工业领域通信协议的业界标准。

Modbus协议目前存在用于串口、以太网以及其他支持互联网协议的网络的版本。

本软件将开发基于Modbus通讯协议的

①：TCP/IP主站

②：串口通信RTU从站

# 软件开发流程

## 软件总体流程设计

### Modbus Tcp 主站



图 Tcp主站总体流程

### Modbus Rtu 从站



图 Rtu从站总体流程

## Tcp主站主要模块

### 建立连接



图 Tcp建立连接

该模块主要包括

1：远端IP地址设置

2：远端端口Port设置

在与远端设备连接前，首先要设置远端Ip信息以及端口信息，这是建立TCP通信的必要参数。由此才可以正确连接。

同时还设置了接收超时时间限制，采用C#定时器控件，设定时间由使用者自行设置。

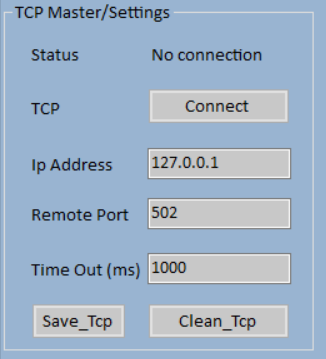


图 Tcp连接配置

### 数据帧生成



图 数据帧生成

Tcp主站的功能包括

0x01（读线圈）、0x03（读寄存器）、

0x0F（写线圈）、0x10（写寄存器）四个功能，

主从设备交互还需要包含设备标识、从机地址、线圈（寄存器）数量，

因此，本模块包含：

1：从机ID选择 （0-256，且248-256保留）

2：功能码选择 （0x01、0x03、0x0F、0x10）

3：从机地址选择

4：读、写线圈（寄存器）数量选择

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 | 2000以内 |
| 0x03 | 读保持寄存器 | 40001-49999 | 字操作 | 125以内 |
| 0x0F | 写多个线圈 | 00001-09999 | 位操作 | 2000以内 |
| 0x10 | 写多个保持寄存器 | 40001-49999 | 字操作 | 125以内 |

表 4-1 功能码与相关参数简图

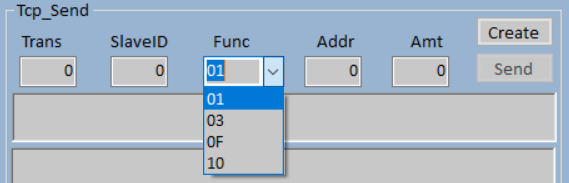


图 功能码选择界面展示

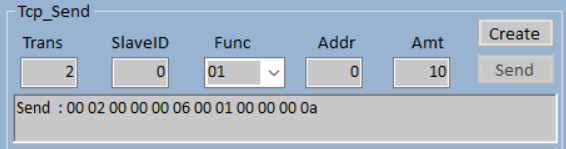


图 数据帧生成界面展示

### 响应报文解析

  
图 响应报文解析

在主站接收到响应数据帧后，应当对其进行解析，分析从站回应的数据帧是否正确，其中应当包括

1：标识（事物标识、传输标识）匹配

2：数据长度匹配

3：设备ID匹配

4：功能码匹配

5：响应的数据帧中，

数据地址、线圈（寄存器）是否与查询报文匹配

### 超时显示



图 Tcp接收数据超时

主站与从机在进行数据传输时，从机可能因延迟或其他异常导致接收数据时间产生异常，此时应对其传输时间进行判定，若超出规定时间，则有信息显示。

### 图形界面显示（UI）

主站与从机在进行数据传输时，为了方便用户查看数据，应当将数据进行展示，并让用户查看是否是想要的数据，从而决定是修改还是发送。数据太多想要重置时应当清除数据区，重要信息需要保存时也应能保存到本地。因此本模块包含如下功能：

1：发送、接收数据展示

2：清除Tcp信息文本框

3：保存Tcp数据信息至本地

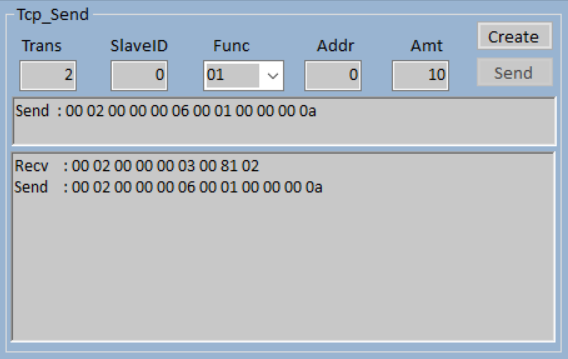


图 与远端Tcp从站交互信息展示



图 保存、清除信息界面展示

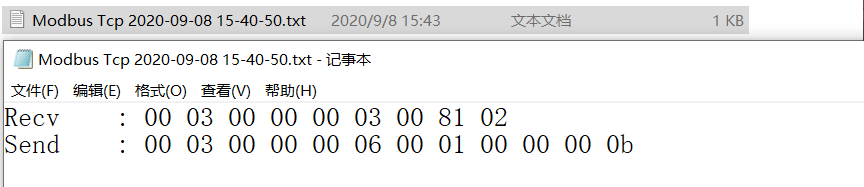


图 日志信息展示

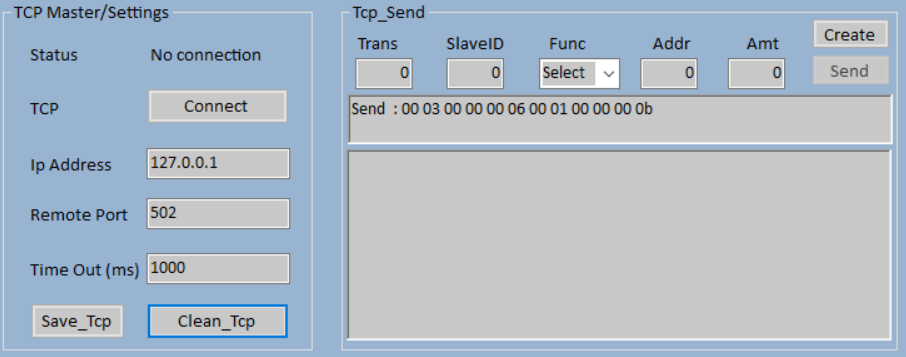


图 Tcp主站软件总体界面展示

## Rtu从站主要模块

### 串口连接配置



图 Rtu从站连接配置图

该模块主要包括：串口端口设置以及下表所示

|  |  |  |  |
| --- | --- | --- | --- |
| 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 4-2 Rtu连接配置

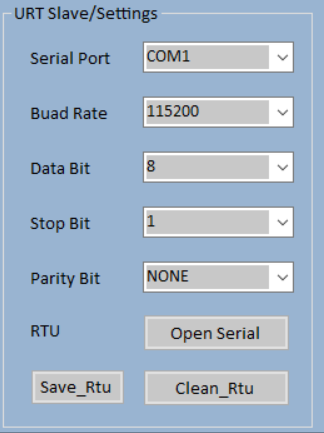


图 Rtu从站连接配置界面展示

### 开线圈、寄存器



图 Rtu从站开线圈、寄存器

在Modbus Rtu通信方式中，从站负责响应主站发送的报文、如果主站欲访问从站线圈，且从站开启主站访问地址的线圈，那么从站应当响应对应的数据。寄存器同理。

因此本模块包括：

1：本机ID选择，开线圈、寄存器及其地址、数量。

2：修改本地线圈、寄存器内数值。

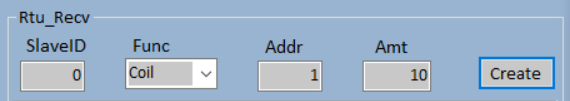


图 开线圈、寄存器界面展示

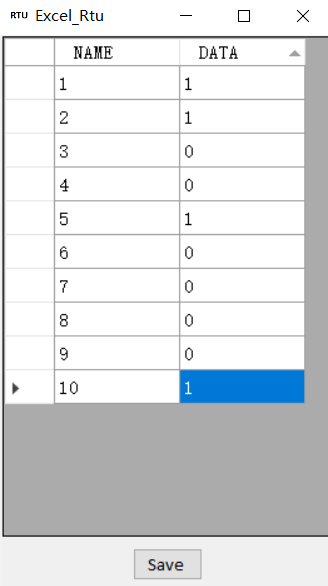


图 修改、保存本机线圈、寄存器界面展示

### Crc校验



图 Crc校验

Modbus协议中,采用了CRC-16标准校验方法。在RTU模式下，CRC自身由两个字节组成，即CRC是一个16位的值。CRC字段校验整个报文的内容，无论报文中的单个字节采用何种奇偶校验方式,整个通信报文均可应用CRC-16校验算法。CRC字段作为报文的最后字段添加到整个报文末尾。

### 查询报文解析



图 查询报文解析

在主站接收到响应数据帧后，应当对其进行解析，分析从站回应的数据帧是否正确，其中应当包括：

1：设备ID匹配；

2：功能码匹配

3：数据长度匹配

4：查询数据帧中，数据地址、线圈（寄存器）与实际是否匹配

### 2.3.5. 图形界面显示（UI）

从机与主站在进行数据传输时，为了方便用户查看数据，应当将数据进行展示。数据太多想要重置时应当清除数据区，重要信息需要保存时也应能保存到本地。因此本模块包含如下功能：

1：发送、接收数据展示

2：清除Rtu信息文本框（同2.2.3）

3：保存Rtu数据信息至本地（同2.2.3）

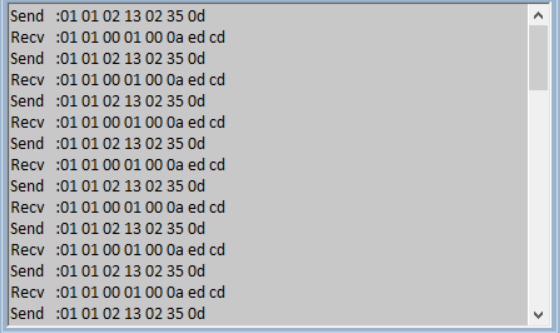


图 与Rtu主站交互信息展示

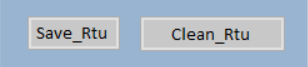


图 保存、清除信息界面展示

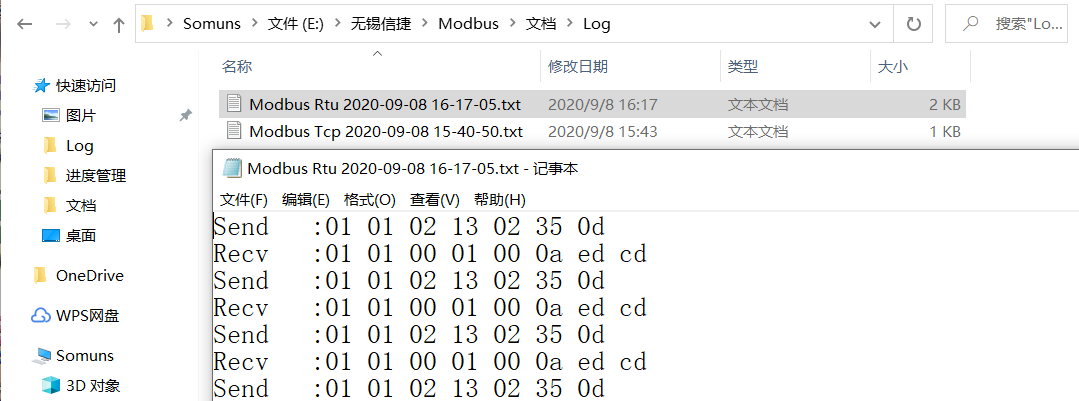


图 日志信息展示

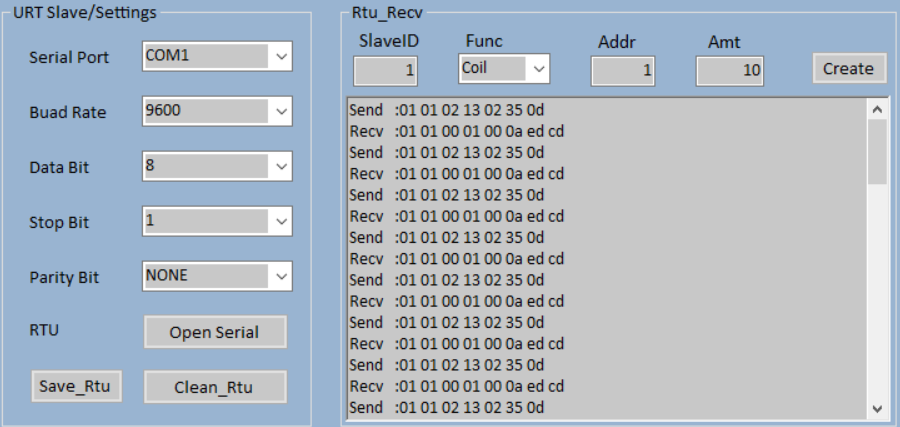


图 Rtu从站软件总体界面展示