

Document Title: CM\_FW external communication module  
design description of Safety Control System

Document Number: 15-Q04-000103

Project Number: CT-RD-1601

Project Name: First phase of Safety Control System  
Development Project

Material Number: N/A

Document Version: A

Classification Level: Highly secret

Document Status: CFC

Controlled Status: Under control

Prepared by: Wang Dong 2016-11-01

Checked by: Zhu Genghua 2016-11-30

Countersigned by: Li Qi, Liu Yang

Approved by: Wen Yiming 2016-12-30

## Revision History

No.	Relevant Chapter	Change Description	Date	Version Before Change	Version After Change	Prepared by	Checked by	Approved by
1		Document created	2016-11-1	None	A	Wang Dong	Zhu Genghua	Wen Yiming
2								
3								
4								
5								

**Relationship between this version and old versions: None.**

文件名称：安全控制系统 CM\_FW 外部通讯模块设计说明书

文件编号：15-Q04-000103

项目编号：SF-RD-1601

项目名称：安全控制系统开发项目一期

物料编号：

版本号/修改码：A

文件密级：机密

文件状态：CFC

受控标识：受控

拟制：王 东

2016 年 11 月 1 日

审核：朱耿华

2016 年 11 月 30 日

会签：李 琦 刘 阳

批准：温宜明

2016 年 12 月 30 日

## 修订页

编号	章节名称	修订内容简述	修订日期	订前版本	订后版本	拟制	审核	批准
1		创建	2016-11-1		A	王 东	朱耿华	温宜明
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								

本版本与旧文件（版本）的关系：

## Content 目录

1	Document overview 文档概述.....	1
1.1	Introduction 综述.....	1
1.2	Reference 参考文档.....	1
1.2.1	Project documents 内部参考文档.....	1
1.3	Terms and abbreviations 术语和缩略语.....	1
1.3.1	Terms 术语.....	1
1.3.2	Abbreviations 缩略语.....	2
2	Module overview 模块概述.....	3
3	Module design 模块设计.....	4
3.1	Function description 功能描述.....	4
3.2	Design concept 设计思路.....	4
3.2.1	Configuration management 配置信息管理.....	4
3.2.2	Maintain Status 维护状态.....	5
3.2.3	Accept connect request 接收连接请求.....	5
3.2.4	Receive data 接收数据.....	5
3.2.5	Send Data 发送数据.....	5
3.3	Interface function 接口函数.....	5
3.4	Global variable 全局变量.....	6
3.5	Data structure 数据结构.....	8
3.6	List of sub-function 子功能列表.....	9
4	Design of sub-function 子功能设计.....	10
4.1	Module initialization 模块初始化.....	10
4.1.1	ExternalCommInit.....	10
4.2	Module cycle running function 模块周期运行函数.....	10
4.2.1	ExternalCommCycle.....	10
4.2.2	HandleConfiguration.....	12
4.2.3	MaintainStatus.....	14
4.2.4	AcceptNewConnect.....	16
4.2.5	ReadNetMessage.....	17
4.3	Send data 发送数据.....	18
4.3.1	ExternalCommSend.....	18

## 1 Document overview 文档概述

### 1.1 Introduction 综述

This document describes the design description of external communication function of CM\_FW of Safety Control System. The document describes the overall concept of the function of the module, and then the sub-function of the modules are described in detail.

This document is the output of module design phase of CM\_FW, and is the input for the follow-up coding phase.

本文档描述了安全控制系统中 CM\_FW 外部通讯模块的设计方案。文档首先描述了模块功能的总体设计思路，然后将模块功能划分为若干子功能并进行详细说明。

本文档是 CM\_FW 模块设计的输出，也是后续编码的输入。

### 1.2 Reference 参考文档

#### 1.2.1 Project documents 内部参考文档

[1] Embedded software safety concept of Safety Control System [505], 15-Q02-000059

[1] 安全控制系统嵌入式软件安全概念说明书 [505], 15-Q02-000059

[2] PM\_FW software overall design description of safety control system [506], 15-Q02-000074

[2] 安全控制系统 PM\_FW 总体设计说明书 [506], 15-Q02-000074

### 1.3 Terms and abbreviations 术语和缩略语

#### 1.3.1 Terms 术语

Table 1-1 Terms

表 1-1 术语

No. 序号	Term 术语	Description 解释
1.	IP_BUS	Communication between PM and IO modules. PM 与 IO 模块之间的通讯总线。
2.	CM_BUS	Communication between PM and CM. PM 与 CM 之间的通讯总线。
3.	PM_BUS	Communication between PMs. PM 之间的通讯总线。
4.	System Net	Communication between control station and PC. 控制站与上位机之间的通讯网络。
5.	Safety Net	Safe communication between control stations.

		控制站之间的安全通讯。
6.	Control station 控制站	A set of triple redundant control system, which includes triple redundant PMs and IO modules under control. 一套三冗余的控制系统，包含三冗余 PM 和 PM 控制的各种 IO 模块。
7.	System response time 系统响应时间	Time interval from the moment that transition of demand signal generated at input ETP to the moment that transition of response signal generated at output ETP. 从系统输入端子板上产生需求信号跳变的时刻到输出端子板上产生相应的响应信号跳变之间的时间。
8.	Control cycle 控制周期	Time interval between adjacent two runs of user program execution. PM 两次执行用户程序间隔时间。
9.	Project 工程	Files which contain configuration information for control station and generated by IEC 61131 configuration software. These files contain all the information required by control station to implement control, including user control program (binaries) to be loaded and executed as well as configuration information of task, CM, PM and IO modules. IEC 61131 组态软件在完成编译后，为控制站生成的组态信息文件，该文件包含可加载执行的用户控制程序（二进制程序）、任务配置信息、CM 配置信息、PM 配置信息和 IO 模块配置信息等各种控制站完成控制所需的信息。
10.	Source project 源工程文件	Source file of the project before compiling. 工程在编译前的源文件。
11.	User program 用户程序	Part of project which contain user control program (binaries) to be loaded and executed and configuration information of task. 工程中的一部分：可加载执行的用户控制程序（二进制程序）和任务配置信息。

### 1.3.2 Abbreviations 缩略语

Table 1-2 Abbreviations

表 1-2 缩略语

No. 序号	Abbreviation 缩略语	English description 英文	Chinese description 中文
1.	PM	Processor Module	主处理器模块
2.	CM	Communication Module	通讯模块
3.	BI	Bus Interface Module	总线接口模块
4.	AI	Analog Input Module	模拟量输入模块
5.	AO	Analog Output Module	模拟量输出模块

6.	DI	Digital Input Module	数字量输入模块
7.	DO	Digital Output Module	数字量输出模块
8.	OSP	Over Speed Protect Module	超速保护模块
9.	SOE	Sequence Of Events	SOE 事件
10.	SIL	Safety Integrity Level	安全完整等级
11.	PW	Power Module	电源模块
12.	OPC	OLE for Process Control	用于过程控制的对象链接与嵌入式技术
13.	UP	User Program	用户程序

## 2 Module overview 模块概述

The location of the external communication module (marked red) in the software hierarchy is shown below.

外部通讯模块（标红）在软件层次中的位置如下图所示。

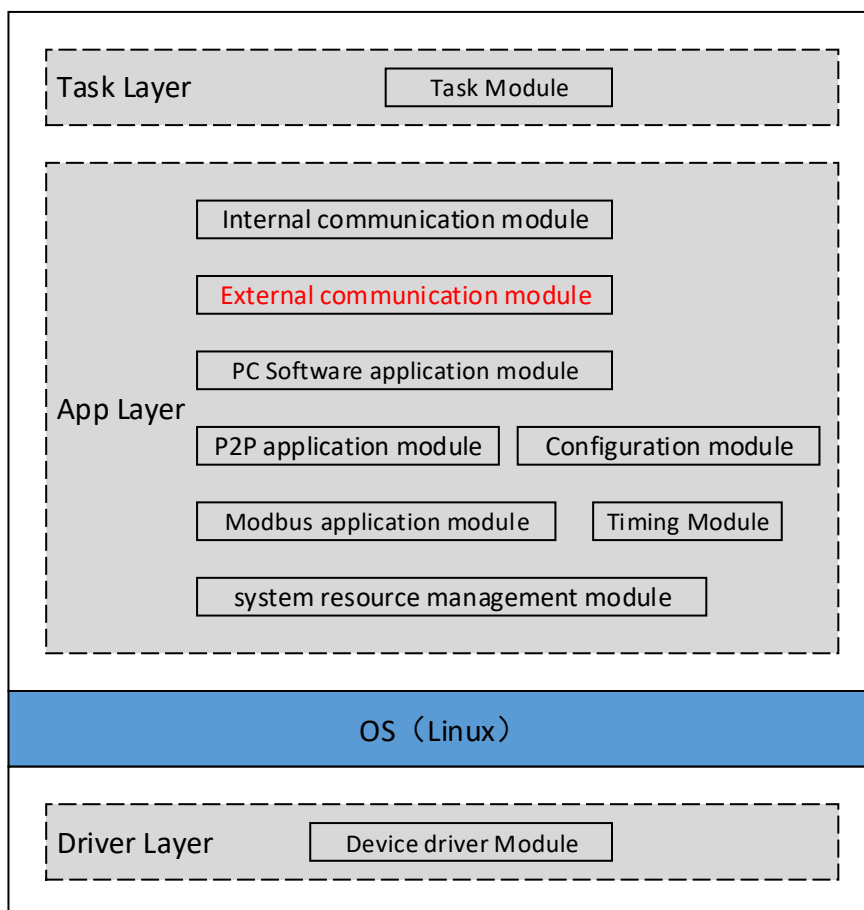


Figure 2-1 the location of the external communication module

图 2-1 模块位置

External communication module is mainly used to process network communication.



外部通讯模块主要用于实现网络通讯功能。

### 3 Module design 模块设计

#### 3.1 Function description 功能描述

The main functions are as follows:

主要功能如下：

- Manage configuration: Network, Modbus TCP, and Modbus master configuration;  
管理配置信息：网络配置、Modbus TCP 配置和 Modbus 主站配置；
- Maintain status: Maintain the connection status with Modbus TCP slave station and PC software;  
维护状态：维护与 Modbus TCP 从站和上位机软件的连接状态；
- Accept connect request: Accept connect request from PC software and Modbus TCP master station;  
接收连接请求：接收来自上位机软件和 Modbus TCP 主站的连接请求；
- Receive data: Receive network data from PC software, other control station and Modbus TCP master/slave station;  
接收数据：接收来自上位机软件，其他控制站和 Modbus TCP 主站/从站的网络数据；
- Send Data: Send data to PC software, other control station and Modbus TCP master/slave station.  
发送数据：将数据发送到上位机软件，其他控制站和 Modbus TCP 主站/从站。

#### 3.2 Design concept 设计思路

##### 3.2.1 Configuration management 配置信息管理

For each configuration, module stores two versions locally and records the version in use. In each period, the module compares the version stored in the system resource with the local version currently in use: If they are different, copy it to local and switch to the new version.

对于每种配置，模块内部均存储两个版本，并记录正在使用的版本。模块每周期均检查系统资源中的相应配置的版本是否发生了变化，如果变化，则拷贝到本地并切换。

The module handles the changed parameters during switching.

发生切换时，对变化的参数进行处理。

### 3.2.2 Maintain Status 维护状态

If the connection with the Modbus TCP slave station is abnormal, the module tries to reconnect until normal.

如果与 Modbus TCP 从站的连接异常，模块会尝试重连直至恢复正常。

If other modules notice to clear the information corresponding to the specific PC software, the module disconnects, clear the local information, and clear the message of the PC software.

如果其他模块通知清除某一上位机软件的信息，模块将与之断开连接，清除本地保存的相关信息并清除已接收到的相关消息。

### 3.2.3 Accept connect request 接收连接请求

In each period, the module listens to the connect request from PC software and Modbus TCP master station, and add the socket to the corresponding array and update the local information when accept a connect request.

模块每周期均监听来自上位机软件和 Modbus TCP 主站的连接请求。接收到连接请求时，将得到的套接字放入到相应的数组中，并更新本地记录的信息。

### 3.2.4 Receive data 接收数据

If received successfully, the module writes the network data to the corresponding buffer, otherwise clears the corresponding information in local and system resource.

如果接收成功，则将接收到的网络数据放入到相应的接收缓冲区中；否则清除本地和系统资源中的相应信息。

### 3.2.5 Send Data 发送数据

If send failed, the module clears the corresponding information in local and system resource.

如果发送失败，则清除本地和系统资源中的相应信息。

## 3.3 Interface function 接口函数

The interface functions which are provided by this module are shown as follows:

模块提供的接口函数如下：

1. void ExternalCommInit(void)

Input argument 输入参数	Output argument 输出参数	Description 描述
No. 无。	No. 无。	Module initialization. 模块初始化。

2. void ExternalCommCycle(void)

Input argument 输入参数	Output argument 输出参数	Description 描述
No. 无。	No. 无。	Module cycle function. 模块周期运行函数。

3. uint8\_t ExternalCommSend( uint8\_t const pucData[], uint16\_t usDataLen, uint32\_t uiIPAddr, uint16\_t usPort, NetworkPortType\_t emNetwork, CommType\_t emSendType, uint8\_t ucIndex )

Input argument 接口输入参数	Output argument 接口输出参数	Description 描述
pucData: Data to be send 待发送数据; usDataLen: Data length 数据长度; uiIPAddr: Destination IP address 目的 IP 地址; usPort: Destination port number 目的端口号; emNetwork: Local network number 本地网口号; emSendType: Send Type 发送类型; ucIndex: Index 索引号。	Error code. 错误码。	Send data. 发送数据。

### 3.4 Global variable 全局变量

Table 3-1 Global variable list

表 3-1 全局变量列表

No. 序号	Type 变量类型	Name 名称	Description 描述
1.	static bool_t	s_bCMHasCfg	CM has configuration flag. CM 是否有配置标志。
2.	static uint8_t	s_ucLocalStaID	Local station ID. 本控制站的 ID。
3.	static uint8_t	s_ucLocalCMSlotID	CM slot ID CM 模块的槽位号
4.	static NetworkSockInfo_t	s_stSockInfo	Network socket information. 网口套接字信息。

5.	static ConnSockInfo_t	s_stSOEConnSock	SOE connect information. SOE 连接信息。
6.	static ConnSockInfo_t	s_stAMSConSock	AMS connect information. AMS 连接信息。
7.	static ConnSockInfo_t	s_stCliConnSock	Diagnostic Software connect information. 诊断软件连接信息。
8.	static ConnSockInfo_t	s_stCS1131ConnSock	CS1131 (Configuration Software) connect information. CS1131 (诊断软件) 连接信息。
9.	static ConnSockInfo_t	s_stOPCConSock	OPC connect information. OPC 连接信息。
10.	static ConnSockInfo_t	s_stMBTCPMstrConnSock	Modbus TCP master connect information. Modbus TCP 主站连接信息。
11.	static CliConnSockInfo_t	s_stMBTCPSlaveConnSock	Modbus TCP slave connect information. Modbus TCP 从站连接信息。
12.	static ExtCommNetworkInfo_t	s_stNetInfo	Network configuration information. 网口配置信息。
13.	static ExtCommModbusTCPInfo_t	s_stMBTCPInfo	Modbus TCP configuration information. Modbus TCP 配置信息。
14.	static ModbusMstrCfgInfo_t	s_stMBMstrCfgInfo	Modbus master configuration information. Modbus 主站配置信

			息。
--	--	--	----

### 3.5 Data structure 数据结构

#### 1. Network socket information structure

```
typedef struct NetworkSockInfoTag
{
    SockInfo_t stLisCS1131Sock;
    SockInfo_t stLisOPCSock;
    SockInfo_t stLisSOESock;
    SockInfo_t stLisCliSock;
    SockInfo_t stLisAMSSock;
    SockInfo_t stLisMBSock;
    SockInfo_t stP2PSock;
}NetworkSockInfo_t;
```

#### 2. Connect socket information structure

```
typedef struct ConnSockInfoTag
{
    SOCKET hSocket;
    uint32_t uiIPAddr;
    uint16_t usPort;
    bool_t bConnFlag;
    uint8_t ucReserve;
    NetworkPortType_t emNetwork;
}ConnSockInfo_t;
```

#### 3. Client connect socket information structure

```
typedef struct CliConnSockInfoTag
{
    ConnSockInfo_t stConnSock;
    bool_t bWaitConn;
    uint8_t ucReserve;
    uint16_t usWaitCnt;
}CliConnSockInfo_t;
```

#### 4. External communication network information structure

```
typedef struct ExtCommNetworkInfoTag
{
    uint8_t ucIndex;
    bool_t bIPChange;
    uint8_t ucReserve[2];
}
```

```
uint32_t uiCMCfgCRC;  
uint32_t uiCMCfgVer;  
ExtCommNetConfigInfo_t stNetConfig[LOCAL_CFG_VER_CNT];  
}ExtCommNetworkInfo_t;
```

#### 5. External communication Modbus TCP information structure

```
typedef struct ExtCommModbusTCPInfoTag  
{  
    uint8_t ucIndex;  
    uint8_t ucReserve[3];  
    uint32_t uiCMCfgCRC;  
    uint32_t uiCMCfgVer;  
    RTDataVerInfo_t stRTDataVer;  
    ExtCommModbusTCPConfigInfo_t stMBTCPConfig[LOCAL_CFG_VER_CNT];  
}ExtCommModbusTCPInfo_t;
```

#### 6. Modbus master configuration information structure

```
typedef struct ModbusMasterCfgInfoTag  
{  
    uint8_t ucIndex;  
    bool_t bCopying;  
    bool_t bValid;  
    uint8_t ucReserve;  
    uint32_t uiCfgCRC;  
    uint32_t uiCfgVer;  
    RTDataVerInfo_t stRTDataVer;  
    ModbusMasterInfo_t stMasterCfg[LOCAL_CFG_VER_CNT];  
}ModbusMstrCfgInfo_t;
```

### 3.6 List of sub-function 子功能列表

The sub-functions list is shown as follows:

子功能列表如下：

Table 3-2 Sub function list

表 3-2 子功能列表

Sub function No. 子功能编号	Function description 功能描述
SWDD-CM-EC_NSafR_SecR_A_001	Module initialization 模块初始化
SWDD-CM-EC_NSafR_SecR_A_002	Module cycle function 模块周期运行函数

SWDD-CM-EC_NSafR_SecR_A_003	Send data 发送数据
-----------------------------	-------------------

## 4 Design of sub-function 子功能设计

### 4.1 Module initialization 模块初始化

SWDD-CM-EC\_NSafR\_SecR\_A\_001

#### 4.1.1 ExternalCommInit

##### 4.1.1.1 Function Description 功能描述

This function completes initialization of module.

该函数完成外部通讯模块的初始化。

##### 4.1.1.2 Argument Description 参数说明

###### ➤ Definition 函数定义

void ExternalCommInit(void)

###### ➤ Input argument 输入参数

No.

无。

###### ➤ Output argument 输出参数

No.

无。

##### 4.1.1.3 Processing flow 处理流程

This function has no branch and the processing flow is omitted.

此函数无分支，流程图省略。

### 4.2 Module cycle running function 模块周期运行函数

SWDD-CM-EC\_NSafR\_SecR\_A\_002

#### 4.2.1 ExternalCommCycle

##### 4.2.1.1 Function Description 功能描述

This function completes module cycle running functions: manage configuration, maintain status, accept connect request and receive network data.

该函数完成模块周期运行功能：管理配置信息、维护状态，接收连接请求和接收网络数据。

#### 4.2.1.2 Argument Description 参数说明

- Definition 函数定义

void ExternalCommCycle(void)

- Input argument 输入参数

No.

无。

- Output argument 输出参数

No.

无。

#### 4.2.1.3 Processing flow 处理流程

The processing flow is shown below, the main steps are as follows:

流程如下图所示，主要步骤如下：

1. Check if CM has configuration: if has, enter step 2, otherwise enter step 3;  
检查 CM 是否有配置：如果有，则进入步骤 2；否则进入步骤 3；
2. Handle configuration: see section 4.2.2 for details;  
管理配置：详见 4.2.2 节；
3. Clear local info.: clear local configuration and disconnect with Modbus TCP slave station;  
清除本地信息：清除本地配置信息，与 Modbus TCP 从站断开连接；
4. Maintain status: see section 4.2.3 for details;  
维护状态：详见 4.2.3 节；
5. Accept connect request: see section 4.2.4 for details;  
接收连接请求：详见 4.2.4 节；
6. Receive network data: see section 4.2.5 for details;  
接收网络数据：详见 4.2.5 节。



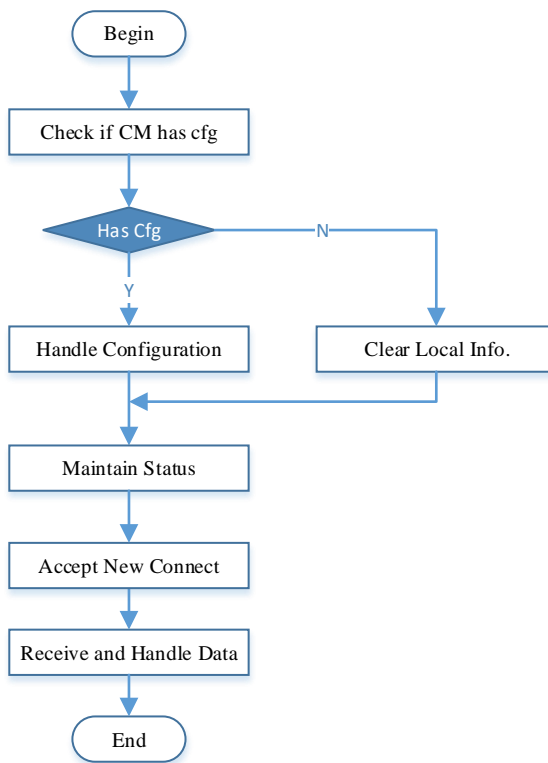


Figure 4-1 cycle running function

图 4-1 周期运行函数

## 4.2.2 HandleConfiguration

### 4.2.2.1 Function Description 功能描述

This function is used to manage module configuration cyclically.

该函数用于周期性管理与本模块相关的配置信息。

### 4.2.2.2 Argument Description 参数说明

#### ➤ Definition 函数定义

static void HandleConfiguration(void)

#### ➤ Input argument 输入参数

No.

无。

#### ➤ Output argument 输出参数

No.

无。

### 4.2.2.3 Processing flow 处理流程

The processing flow is shown below, the main steps are as follows:

流程如下图所示，主要步骤如下：

1. Handle network configuration: if switch, enter step 2, otherwise enter step 3;  
处理网络配置信息：如果切换，则进入步骤 2；否则进入步骤 3；
2. Handle network configuration change: update IP address, subnetmask and gateway if changed;  
处理网络变化参数：根据变化情况，更新网口的 IP 地址，子网掩码和网关；
3. Handle Modbus TCP configuration: if switch & IP address not changed, enter step 4, otherwise enter step 5;  
处理 Modbus TCP 配置：如果切换且 IP 地址未变化，进入步骤 4，否则进入步骤 5；
4. Handle Modbus TCP configuration change;  
处理 Modbus TCP 变化参数；
5. Check if IP address changed: if yes, enter step 6, otherwise enter step 7;  
处理 Modbus TCP 配置：如果变化，进入步骤 6，否则进入步骤 7；
6. Handle IP address change: Update receive information;  
处理 IP 变化：更新接收信息；
7. Handle Modbus master configuration: if switch, enter step 8, otherwise end;  
处理 Modbus 主站配置信息：如果切换，则进入步骤 8；否则结束；
8. Handle connect with Modbus TCP slave station: disconnect with deleted Modbus TCP slave station, and connect to the new added Modbus TCP slave station.  
处理与 Modbus TCP 从站的连接：与删除的从站断开连接，与新增的从站建立连接。

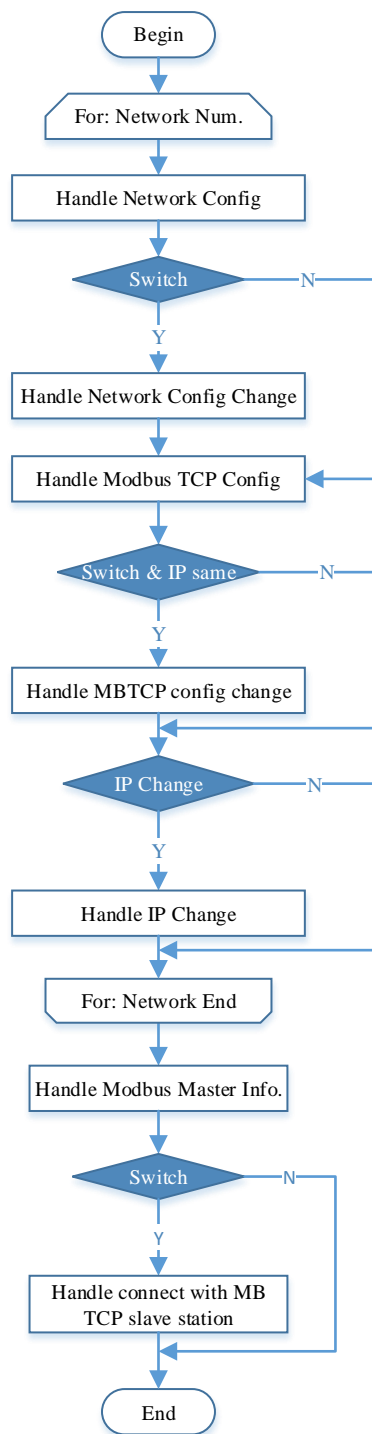


Figure 4-2 handle configuration

图 4-2 处理配置

## 4.2.3 MaintainStatus

### 4.2.3.1 Function Description 功能描述

This function is used to maintain connect status with the Modbus TCP slave station and the PC software cyclically.

该函数用于周期性维护与 Modbus TCP 从站和上位机软件的连接状态。

#### 4.2.3.2 Argument Description 参数说明

- Definition 函数定义

static void MaintainStatus(void)

- Input argument 输入参数

No.

无。

- Output argument 输出参数

No.

无。

#### 4.2.3.3 Processing flow 处理流程

The processing flow is shown below, the main steps are as follows:

流程如下图所示，主要步骤如下：

1. Check connect status with the Modbus TCP slave station: if abnormal, enter step 2, otherwise check the next slave station;

检查与 Modbus TCP 从站的连接状态：如果异常，则进入步骤 2；否则检查下一从站；

2. Check if connect error, if yes, reconnect, otherwise enter step 3;

检查连接是否出错：如果是，则重新建立连接，否则进入步骤 3；

3. Check connect operation: Check if connect finished and update local receive information according to the check result;

检查连接操作：检查连接操作是否已经完成，并根据检查结果更新本地接收信息；

4. Check if notice to clear: if yes, clear receive information of the specific PC software, otherwise check the next PC software.

检查是否通知清除：如果是，则断开连接并清除指定上位机软件的接收信息，否则检查下一上位机软件。

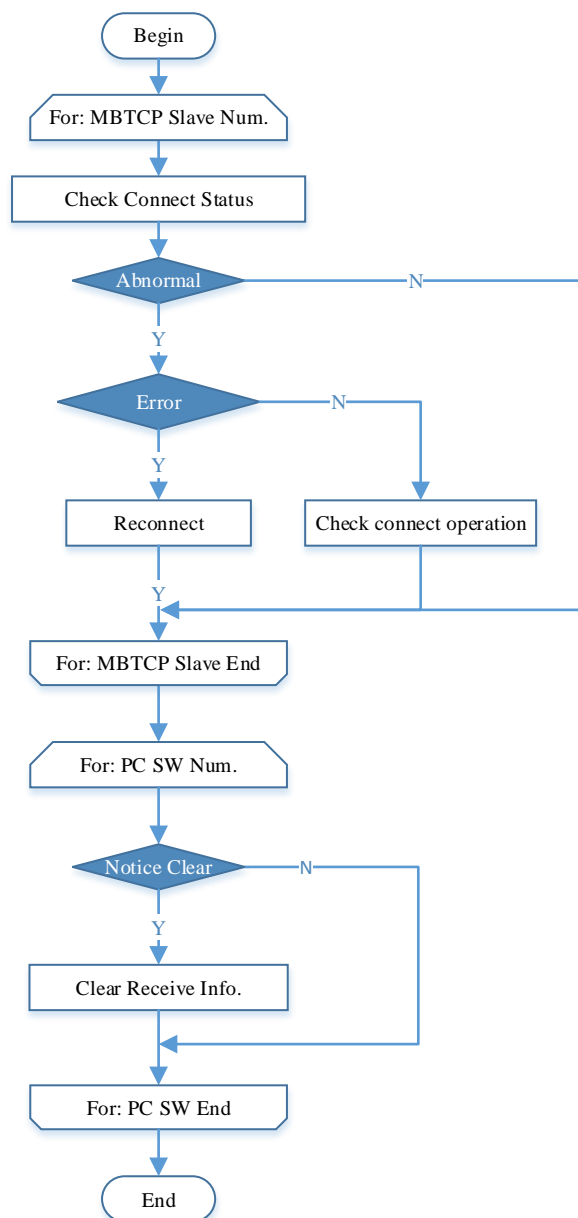


Figure 4-3 maintain status

图 4-3 维护状态

## 4.2.4 AcceptNewConnect

### 4.2.4.1 Function Description 功能描述

This function is used to listen the connect request from PC software and Modbus TCP master station cyclically. When accept a connect request, add the socket to the corresponding array and update the local information.

该函数用于周期性监听来自上位机软件和 Modbus TCP 主站的连接请求。接收到连接请求时，将得到的套接字放入到相应的数组中，并更新本地信息。

### 4.2.4.2 Argument Description 参数说明

➤ Definition 函数定义

---

static void AcceptNewConnect(void)

➤ Input argument 输入参数

No.

无。

➤ Output argument 输出参数

No.

无。

#### 4.2.4.3 Processing flow 处理流程

This function has no branch and the processing flow is omitted.

此函数无分支，流程图省略。

#### 4.2.5 ReadNetMessage

##### 4.2.5.1 Function Description 功能描述

This function is used to receive network data cyclically. If received successfully, write the network data to the corresponding buffer, otherwise clear the corresponding information in local and system resource.

该函数用于周期性接收网络数据。如果接收成功，则将接收到的网络数据放入到相应的接收缓冲区中，否则清除本地和系统资源中的相应信息。

##### 4.2.5.2 Argument Description 参数说明

➤ Definition 函数定义

static void ReadNetMessage( void )

➤ Input argument 输入参数

No.

无。

➤ Output argument 输出参数

No.

无。

##### 4.2.5.3 Processing flow 处理流程

This function has no branch and the processing flow is omitted.

此函数无分支，流程图省略。

### 4.3 Send data 发送数据

SWDD-CM-EC\_NSafR\_SecR\_A\_003

#### 4.3.1 ExternalCommSend

##### 4.3.1.1 Function Description 功能描述

This function is used to receive network data.

该函数用于发送网络数据。

##### 4.3.1.2 Argument Description 参数说明

###### ➤ Definition 函数定义

```
uint8_t ExternalCommSend(uint8_t const pucData[], uint16_t usDataLen,  
                          uint32_t uiIPAddr, uint16_t usPort, NetworkPortType_t emNetwork,  
                          CommType_t emSendType, uint8_t ucIndex)
```

###### ➤ Input argument 输入参数

pucData: Data to be send 待发送数据;

usDataLen: Data length 数据长度;

uiIPAddr: Destination IP address 目的 IP 地址;

usPort: Destination port number 目的端口号;

emNetwork: Local network number 本地网口号;

emSendType: Send Type 发送类型;

ucIndex: Index 索引号。

###### ➤ Output argument 输出参数

Error code.

错误码。

##### 4.3.1.3 Processing flow 处理流程

This function has no branch and the processing flow is omitted.

此函数无分支，流程图省略。

——以下无正文