Document Title: CM_FW general design description of Safety Control System

Document Number: 15-Q02-000098

Project Number: SF-RD-1501

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: Li Qi 2015-09-15

Checked by: Zhu Genghua 2015-10-15

Countersigned by:

Approved by: Wen Yiming 2015-10-20

Revision History

No.	Relevant Chapter	Change Description	Date	Version Before Change	Version After Change	Prepared by	Checked by	Approved by
1		Document created	2015-09-15	None	A	Li Qi	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 总体设计说明书

文件编号：15-Q02-000098

项目编号：SF-RD-1501

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：秘密

文件状态：CFC

受控标识：受控

拟制：李琦 2015 年 09 月 15 日

审核：朱耿华 2015 年 10 月 15 日

会签：

批准：温宜明 2015 年 10 月 20 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	2015-09-15		A	李琦	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：

目录

1 Document overview 文档概述

1.1 Introduction 综述

The document describes the software hierarchy of the CM_FW, divides the CM_FW into multiple modules, and explains the function of each module.

This document is the output of general design phase of CM_FW, and is the input for the module design phase.

本文是安全控制系统中 CM_FW 的总体设计。文档描述了 CM_FW 的软件层次结构，将 CM_FW 划分为多个模块，并对每个模块的功能加以说明。

本文档是 CM 嵌入式软件总体设计的输出，也是后续软件模块设计的输入。

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

1.3 Terms and abbreviations 术语及缩略语定义

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.	PM_FW	PM firmware	PM 固件
3.	CM	Communication Module	通讯模块
4.	CM_FW	CM firmware	CM 固件
5.	BI	Bus Interface Module	总线接口模块
6.	AI	Analog Input Module	模拟量输入模块
7.	AO	Analog Output Module	模拟量输出模块
8.	DI	Digital Input Module	数字量输入模块
9.	DO	Digital Output Module	数字量输出模块

10.	OSP	Over Speed Protect Module	超速保护模块
11.	SOE	Sequence Of Events	SOE 事件
12.	SIL	Safety Integrity Level	安全完整等级
13.	PW	Power Module	电源模块
14.	OPC	OLE for Process Control	用于过程控制的对象链接与嵌入式技术
15.	UP	User Program	用户程序

2 Software Organization Structure 软件组织结构

2.1 Software layer 软件层次

CM_FW is divided into three layers, including the task layer, the application module layer and the driver layer, as shown in the following figure. The OS is linux, which is not in the CM_FW development scope.

软件层次划分如下图所示，包括任务层，应用模块层和驱动层。OS 使用 linux，不在 CM_FW 开发范围内。

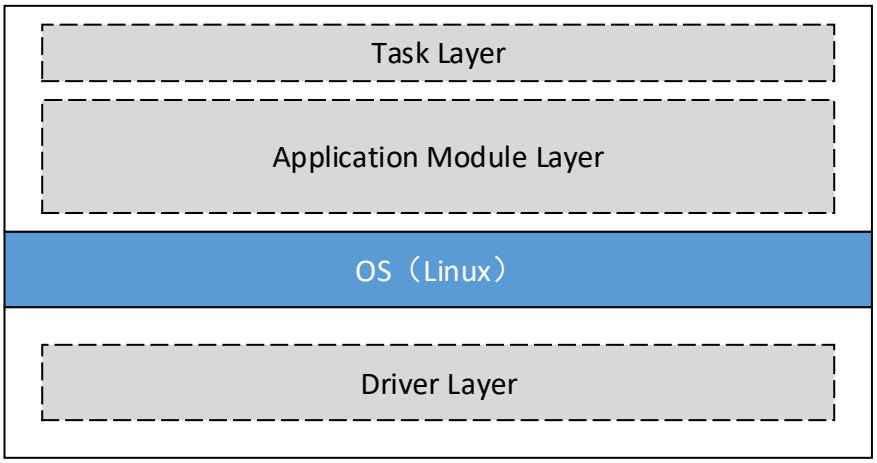

Figure 3-1 software layer

图 3-1 软件层次

2.2 Software module division 软件模块划分

The software module division is shown in the following figure:

软件模块划分如图 3-2 所示。

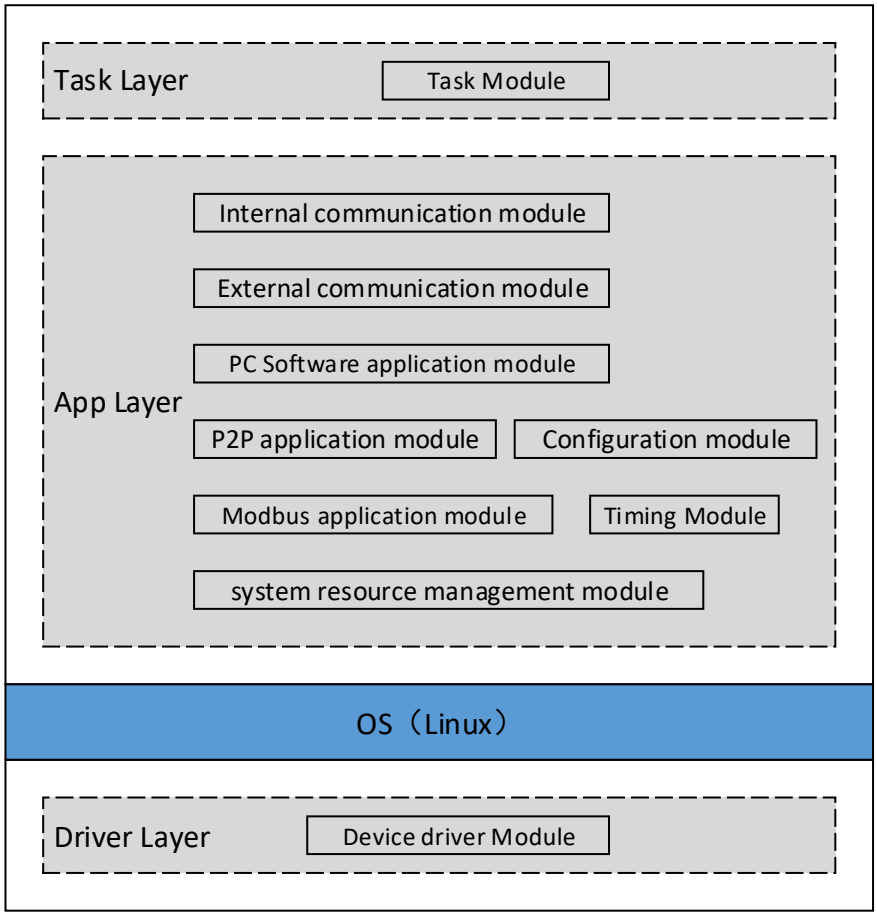

Figure 3-2 module division

图 3-2 模块划分

The task layer includes task module. The application module layer includes the internal communication module, the external communication module, the PC Software application module, the P2P application module, the Modbus application module, the configuration module, timing module, and system resource management module. The driver layer includes device driver module.

任务层包括任务模块。应用模块层包括内部通讯模块、外部通讯模块、上位机应用模块、P2P 应用模块、Modbus 应用模块、配置模块、校时模块及系统资源管理模块。驱动层包括设备驱动模块。

3 Module function division 模块功能划分

3.1 Task module 任务模块

SWOD-CM_NSafR_NSecR_A_001

Initialize each application module at startup, and if a fault is detected during initialization, record the fault and stop the system.

对各应用模块进行初始化，若初始化时检查出故障，则记录故障并停止系统运行。

Call the periodic function of each application module cyclically.

依次调用各应用模块的周期运行函数。

3.2 Internal communication module 内部通讯模块

SWOD-CM_NSafR_SecR_A_002

This module implements the periodic communication between PM and CM.

The module gets the data (PC software commands, CM status data, etc) from the system resource management module, packs the data and then sends it to the PM.

The module receives data packets from the PM and parses them. After the analysis, the data (real-time data, SOE data, Modbus data, etc.) will be put into the system resource management module.

本模块完成 PM 与 CM 间的周期通讯。模块从系统资源管理模块中取得需要发送给 PM 的数据、命令等，组包后发送给 PM。接收来自 PM 的数据包，并对其进行解析。解析后将数据（实时数据、SOE 数据、Modbus 数据等）放入系统资源管理模块中。

3.3 External communication module 外部通讯模块

SWOD-CM_NSafR_SecR_A_003

This module provides TCP/UDP protocol interface functions.

This module provides Modbus RTU protocol interface functions.

This module receives data packets from the PC software or a third party system, parse the data packets and put the data into the system resource management module.

提供 TCP/UDP 协议相关接口函数。

提供 Modbus RTU 协议相关接口函数。

接受来自上位机软件或第三方系统的数据包，对数据包解析后分类放入系统资源管理模块中。

3.4 PC Software application module 上位机软件应用模块

SWOD-CM_NSafR_SecR_A_004

This module processes the data from the PC software. According to the data type, the command that needs PM processing are written into the system resource management module, and the response data from the PM in the system resource management module are sent to the PC software. The commands that do not need PM processing are processed and responsed directly by this module.

PC software includes: SOE software, third-party AMS software, Diagnostic software, Configuration software, OPC Server.

该模块用于处理来自上位机软件的数据。根据数据类型，将需要 PM 处理的命令写入系统

资源管理模块中，并将系统资源管理模块中来自 PM 的应答数据发送给上位机软件；直接处理不需要 PM 处理的命令，并将发送应答给上位机软件。

上位机软件主要包括 SOE 软件，第三方 AMS 软件，诊断软件，组态软件，OPC Server。

3.5 P2P application module P2P 应用模块

SWOD-CM_NSafR_SecR_A_005

This module receives P2P data from other control stations, writes the data into the system resource management module, and forwards the response from the PM to the corresponding control station.

The module sends the P2P data in system resource module to other control stations and receives responses from other control stations and stores them in the system resource management module.

接收来自其它控制站的 P2P 数据，将数据存入系统资源管理模块中，并将来自 PM 的应答转发给相应控制站。

将系统资源模块中来自 PM 的 P2P 数据发送出去，接收来自其它控制站的应答并存入系统资源管理模块。

3.6 Modbus application module Modbus 应用模块

SWOD-CM_NSafR_SecR_A_006

Construct modbus request message, and send to the modbus slave station. Decode response message from the modbus slave station, and send data to PM module;

Decode request message from the modbus master station, and send data to PM module. Construct modbus response message, and send to the modbus master station.

构造 Modbus 请求帧，并发送给相应的 Modbus 从站；解析来自 Modbus 从站的应答帧，将来自 Modbus 从站的数据转发到 PM 模块；

解析来自 Modbus 主站的请求帧，将来自 Modbus 主站的数据转发到 PM 模块；构造 Modbus 应答帧，并应答给相应的 Modbus 主站。

3.7 Timing module 校时模块

SWOD-CM_NSafR_NSecR_A_007

This module is used to realize timing function.

本模块主要用于实现校时功能。

3.8 System resource management module 系统资源管理模块

SWOD-CM_NSafR_NSecR_A_008

The system resource management module stores system status and configuration information, and is used to transfer data between modules.

系统资源管理模块储存系统状态及各种配置信息，并用于模块间传递数据。

The module is also responsible for setting the status of the LED lights, providing the CM version and providing common library functions.

模块同时负责设置 LED 灯的状态、提供 CM 的版本及提供公共库函数。

3.9 Configuration module 配置模块

SWOD-CM_NSafR_NSecR_A_009

The module obtains the configuration information of the CM from the PM, and puts the parsing result into the system resource management module.

该模块从 PM 获取 CM 的配置信息，解析后放入系统资源管理模块。

3.10 Device driver module 设备驱动模块

SWOD-CM_SafR_NSecR_A_010

This module provides device drivers, such as FPGA driver, PCIE driver. Nor Flash driver, SPI Flash driver. The network Storm Protection functionality is also implemented in this module.

本模块提供设备驱动，包括：FPGA driver，PCIE 驱动等。防网络风暴功能也在本模块实现。

——以下无正文