Document Title: PM_FW general design description of Safety Control System

Document Number: 15-Q02-000074

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 PM_FW 总体设计说明书

文件编号：15-Q02-000074

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 PM_FW, divides the PM_FW into multiple modules, and explains the function of each module.

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

本文是安全控制系统中 PM_FW 的总体设计。文档描述了 PM_FW 的软件层次结构，将 PM_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 PM_FW 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.	RTS	Real-Time System	实时系统
16.	UP	User Program	用户程序

2 Software Organization Structure 软件组织结构

2.1 Software layer and module division 软件层次及模块划分

PM_FW is divided into three layers according to the hierarchy, application layer, service layer and driver layer (HAL layer). The software module division is shown in the following figure:

PM_FW 按层次划分为三层，分别是应用层，服务层及硬件抽象层。模块划分如图 3-1 所示。

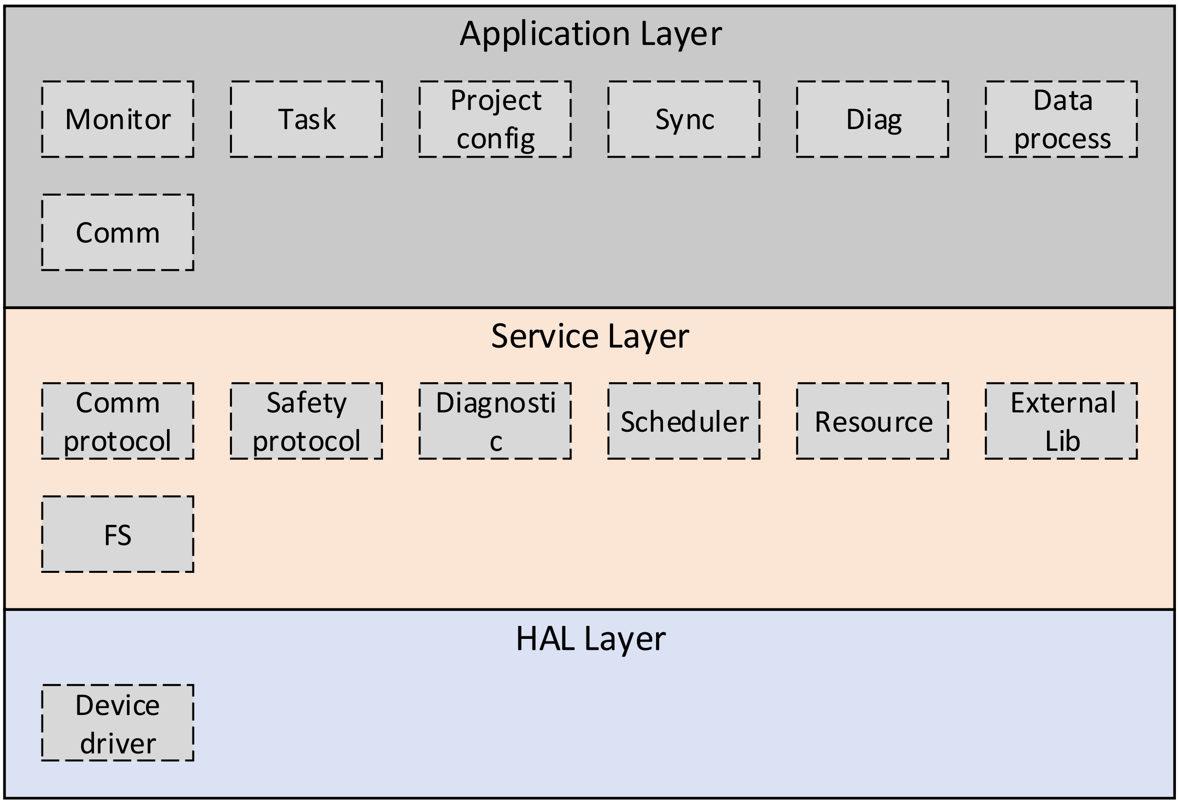

Figure 3-1 module division

图 3-1 模块划分

3 Module function division 模块功能划分

3.1 Application layer 应用层

3.1.1 Task module 任务模块

SWOD-PM_SafR_NSecR_A_001

This module is responsible for initializing the system at power-on, calling the RTS task, UP1 task and UP2 task cyclically in different time slices on core0, and calling the RTS task, communication task and file management task cyclically in different time slices on core1.

模块负责系统上电时的初始化，调用 core0 上的 RTS 任务、UP1 任务和 UP2 任务按照时间片周期运行，调用 core1 上的 RTS 任务、通讯任务和文件管理任务分时间片周期运行。

3.1.2 Monitor module 监视模块

SWOD-PM_SafR_NSecR_A_002

In core0, this module is mainly responsible for controlling the UP operation and monitoring command queue. The module calculates the IEC cycles of each UP_Task and controls the start of the logical operation. At the same time, it monitors the command queue. If the queue is not empty, then it gets the command to process. Commands mainly include operations of run, stop, single step operation and OPC, Modbus and P2P write variable operation. The data retention function is also implemented in this module.

该模块主要负责控制 UP 运行和监视命令队列。模块计算各 UP_Task 的 IEC 周期，控制逻辑运算的开始。同时，监视命令队列，若队列非空，则获取命令进行处理。命令主要包括控制 UP 的运行、停止、单步运行等操作和 OPC、Modbus 和 P2P 的写变量操作。掉电保持功能也在本模块实现。

In core1, this module is responsible for monitoring system temperature, power supply voltages, PM online state, the location of the key switch, the existence of project files and so on. The monitoring results are written into the system resource management module, and the other modules can obtain the monitoring results from the system resource management module.

主要负责周期监视系统的温度，电源电压，PM 在线状态，钥匙开关的位置，工程文件是否存在等。监视结果写入系统资源管理模块中，其它模块从系统资源管理模块中获取监视结果

3.1.3 Data process module 数据处理模块

SWOD-PM_SafR_NSecR_A_003

This module is responsible for exchanging the input/output data with the IO module, exchanging the input/output data with other PM, and then completing the data voting. The Module obtains hard SOE data, IO diagnostic data from the IO module, and stored it in the system resource management module.

Soft SOE data processing is also implemented in this module.

该模块负责和 IO 模块之间交换输入/输出数据，并和其他 PM 交换输入输出数据，然后完成数据表决。模块从 IO 模块获取硬 SOE 数据，IO 诊断数据，并存入系统资源管理模块。

软 SOE 数据的处理也在本模块实现。

3.1.4 Diagnostics module 自检模块

SWOD-PM_SafR_NSecR_A_004

The module completes the power-on diagnostics, cyclic diagnostics and first error restart function.

该模块完成上电自检，周期自检及故障重启功能。

3.1.5 Sync module 同步模块

SWOD-PM_SafR_NSecR_A_005

The module is responsible for the PM state managerment and the synchronization between the PMs, which include user project information synchronization, user operation synchronization, system state synchronization and so on.

同步模块负责控制器的状态管理及控制器间的同步操作。主要包括：用户工程信息同步；用户操作同步；系统运行状态同步。

3.1.6 Project configuration module 工程配置模块

SWOD-PM_SafR_NSecR_A_006

The module is responsible for user project configuration and IO configuration.

主要负责工程配置和 IO 配置。

3.1.7 Comm module 通讯模块

SWOD-PM_NSafR_SecR_A_007

The module is responsible for the communication between PM and CM. The communication data includes timing data, user project data, user operation, real-time data, SOE data, log information and fault alarming information.

通讯模块负责主处理器模块 PM 与通讯模块 CM 间的通讯，通讯内容包括校时、用户工程数据、用户操作、实时数据周期发送、SOE 数据、日志信息、故障报警信息等。

3.2 Service layer 服务层

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

SWOD-PM_NSafR_NSecR_A_008

This 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 operation to log, providing the PM version and providing common library functions.

模块同时负责设置 LED 灯的状态、支持对日志的操作、提供 PM 的版本及提供公共库函数。

3.2.2 Safty protocol module 安全协议模块

SWOD-PM_NSafR_NSecR_A_009

This module is responsible for implementing the safety communication protocol. This protocol is used in the communications which between the PM and IO modules, between the PMs and between the control stations.

本模块负责实现安全通讯协议，该协议会在 PM 与 I/O 模块通讯、PM 间通讯以及控制站间通讯时使用的。

3.2.3 Communication protocol module 通讯协议模块

SWOD-PM_NSafR_SecR_A_010

This module is responsible for realizing three kinds of communication protocols: CM_BUS, PM_BUS, and IP_BUS.

本模块负责实现三种通讯协议：CM_BUS，PM_BUS，IP_BUS。

3.2.4 Diagnostics module 自检模块

SWOD-PM_SafR_NSecR_A_011

This module is responsible for the self-test of the address line, data line, CPU instructions, registers, cache, exception handling mechanism, DDR memory and so on. This module is called by the diagostics module in the application layer.

本模块主要实现：对地址线、数据线自检；对 CPU 的指令、寄存器、cache、异常处理机制等自检；对 DDR 内存自检等等。此模块供应用层自检模块使用。

3.2.5 External lib module 外部库模块

SWOD-PM_SafR_NSecR_A_012

This module provides external library for user project, such as RS function block.

本模块提供外部库供用户工程使用，如 RS 功能块。

3.2.6 Scheduler module 调度模块

SWOD-PM_SafR_NSecR_A_013

The module is responsible for multi-task creation and scheduling strategy.

本模块实现多任务的创建及调度策略。

3.2.7 FS module 文件系统模块

SWOD-PM_NSafR_NSecR_A_014

The module provides file operations, such as creation, read/write, delete, etc.

本模块提供对文件的创建、读/写、删除等操作。

3.3 Driver layer 驱动层

3.3.1 Device driver module 设备驱动模块

SWOD-PM_NSafR_NSecR_A_015

This module provides device drivers, including: SPI driver, IP_BUS driver, CM_BUS driver, FPGA driver, PCIE driver, Nor Flash driver, SPI Flash driver.

本模块提供设备驱动，包括：SPI 驱动，IP_BUS 驱动，CM_BUS 驱动，FPGA 驱动，PCIE 驱动，Nor Flash 驱动，SPI Flash 驱动。

——以下无正文