Document Title: Embedded Software Safety Concept of Safety Control System

Document Number: 15-Q02-000059

Project Number: SF-RD-1501

Project Number: First phase of Safety Control System Development Project

Material Number: N/A

Document Version: A.3

Classification Level: Highly secret

Document Status: CFC

Controlled Status: Under control

Prepared by: Zhu Genghua	2016 年 12 月 26 日
Checked by: Wen Yiming	2016 年 12 月 29 日
Countersigned by: Wang Dong, Li Qi, Liu Yang, Liu Yue	2016 年 12 月 29 日
Approved by: Ji Jun	2016 年 12 月 30 日

Revision History

No.	Relevant Chapter	Change Description	Date	Version Before Change	Version After Change	Prepared by	Checked by	Approved by
1		Document created	2015-10-19		A	Zhu Genghua	Wen Yiming	Ji Jun
2	2.2 2.3.1 2.5.1 2.5.2 2.5.4 2.6 3.1 3.6	2.2: Modify Figure 2-4 and 2-5 and scope of PC software. Modify the description of data flow 14, and add it into figure 2-5. 2.3.1: Modify the PM operation to DO and AO modules when it is in "Stop state" 2.5.1: Modify the diagnostic measure for Data cache. 2.5.2: Modify the diagnostic measure for SRAM. 2.5.4: Modify the description of "First error restart". 2.6: Modify the description of operation time for single PM 3.1: Add "PM_FW flow diagram". 3.6: Modify the figure 3-3, 3-4; Add "User confirmation" after "user operation".	2016-2-15	A	A.1	Zhu Genghua	Wen Yiming	Ji Jun
3	2.2 5.1、5.2、5.4 5.1 5.3 5.7	2.2: Modify the 'SWSC_SafR_NSecR_B_041' to 'SWSC_SafR_SecR_C_041'. Modify the 'SWSC_SafR_NSecR_B_055' to 'SWSC_SafR_SecR_C_055'.	2016-8-15	A.1	A.2	Zhu Genghua	Wen Yiming	Ji Jun

		Modify the 'SWSC_SafR_NSecR_B_056' to 'SWSC_SafR_SecR_C_056'. Modify the 'SWSC_SafR_NSecR_B_057' to 'SWSC_SafR_SecR_C_057'. Modify the 'SWSC_SafR_NSecR_B_058' to 'SWSC_SafR_SecR_C_058'. 5.1、5.2、5.4: Modify the word 'password' to 'control station password'. 5.1: Add a description. 5.3: Add a description. 5.7: Add a description of TCP/IP.						
4	3.7 4.2 4.3 5.4	3.7: Modify the description of Control station log. Modify the description of SOE. 4.2: Modify the frame structure of the IPBUS 4.3: Modify the frame structure of the Peer To Peer. 5.4: Modify the measure to protect data confidentiality.	2016-12-26	A.2	A.3	Zhu Genghua	Wen Yiming	Ji Jun
5								
6								
7								

Relationship between this version and old version:

文件名称：安全控制系统嵌入式软件安全概念说明书

文件编号：15-Q02-000059

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.3

文件密级：机密

文件状态：CFC

受控标识：受控

拟制：朱耿华 2016 年 12 月 26 日

审核：温宜明 2016 年 12 月 29 日

会签：王东、李琦、刘阳、刘跃 2016 年 12 月 29 日

批准：季俊 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		首次创建	2015-6-17		A	朱耿华	温宜明	季俊
2	2.2 2.3.1 2.5.1 2.5.2 2.5.4 2.6 3.1 3.6	2.2：修改图 2-4 和 2-5 中的上位机软件范围。修改数据流 14 的描述并增加到图 2-5 中。 2.3.1：修改”Stop state”时 PM 对 DO 和 AO 模块的操作 2.5.1：修改 Data cache 的诊断方法。 2.5.2：修改 SRAM 的诊断方法。 2.5.4：修改故障重启章节的描述. 2.6：修改单个 PM 时关于运行时间的描述 3.1：增加 PM_FW 流程图。 3.6：修改图 3-3、图 3-4，在用户下装操作后增加确认环节	2016-2-15	A	A.1	朱耿华	温宜明	季俊
3	2.2 5.1、5.2、5.4 5.1 5.3 5.7	2.2： 将 SWSC_SafR_NSecR_B_041 改为 SWSC_SafR_SecR_C_041 将 SWSC_SafR_NSecR_B_055 改为 SWSC_SafR_SecR_C_055 将 SWSC_SafR_NSecR_B_056 改为 SWSC_SafR_SecR_C_056 将 SWSC_SafR_NSecR_B_057 改为 SWSC_SafR_SecR_C_057	2016-8-15	A.1	A.2	朱耿华	温宜明	季俊

		将 SWSC_SafR_NSecR_B_058 改为 SWSC_SafR_SecR_C_058 5.1、5.2、5.4：连接密码改为控制站密码。 5.1：增加不支持远程访问。 5.3：增加描述。 5.7：增加对 TCPIP 的描述。						
4	3.7 4.2 4.3 5.4	3.7：修改控制器日志的描述 修改 SOE 的描述 4.2：修改 IP_BUS 帧结构 4.3：修改 peer to peer 帧结构 5.4：修改保护数据保密性的措施	2016-12-26	A.2	A.3	朱耿华	温宜明	季俊
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

This document describes the PM and CM embedded software safety concept of Safety Control System in detail based on the embedded software safety requirement specification. This document is the input of PM and CM embedded software subsystem design.

本文档依据《安全控制系统嵌入式软件安全需求规格书》的要求，详细描述了安全控制系统中 PM 和 CM 嵌入式软件架构设计方案，也是后续 PM 和 CM 嵌入式软件各子系统设计的输入。

1.2 Reference 参考文档

1.2.1 Project documents 内部参考文档

Table 1-1 Referenced project documents

表 1-1 内部参考文档

No. 序号	Document number 文档编号	Document title 名称
501	15-Q01-000058	Embedded Software Safety Requirements Specification of Safety Control System 安全控制系统嵌入式软件安全需求规格书

1.3 Terms and abbreviations 术语和缩略语

1.3.1 Terms 术语

Table 1-2 Terms

表 1-2 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	The original project file before compiling. 工程在编译前的原始文件。
11	User program	Part of project which contain user control program (binaries) to be loaded and

	用户程序	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 1-3 Abbreviations

表 1-3 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	SOE	Sequence Of Events	SOE 事件
9	SIL	Safety Integrity Level	安全完整等级
10	PW	Power Module	电源模块
11	OPC	OLE for Process Control	用于过程控制的对象链接与嵌入式技术
12	FW	Firmware	固件
13	OS	Operating System	操作系统
14	RTS	Real-time System	实时系统
15	UP	User Program	用户程序

2 Software architecture 软件架构

2.1 Software subsystem division 软件子系统划分

SWSC_SafR_NSecR_A_029

The PM and CM embedded software can be divided into three parts, as shown in figure 2-1:

系统中 PM 和 CM 的嵌入式软件可分为三个部分，如下图所示：

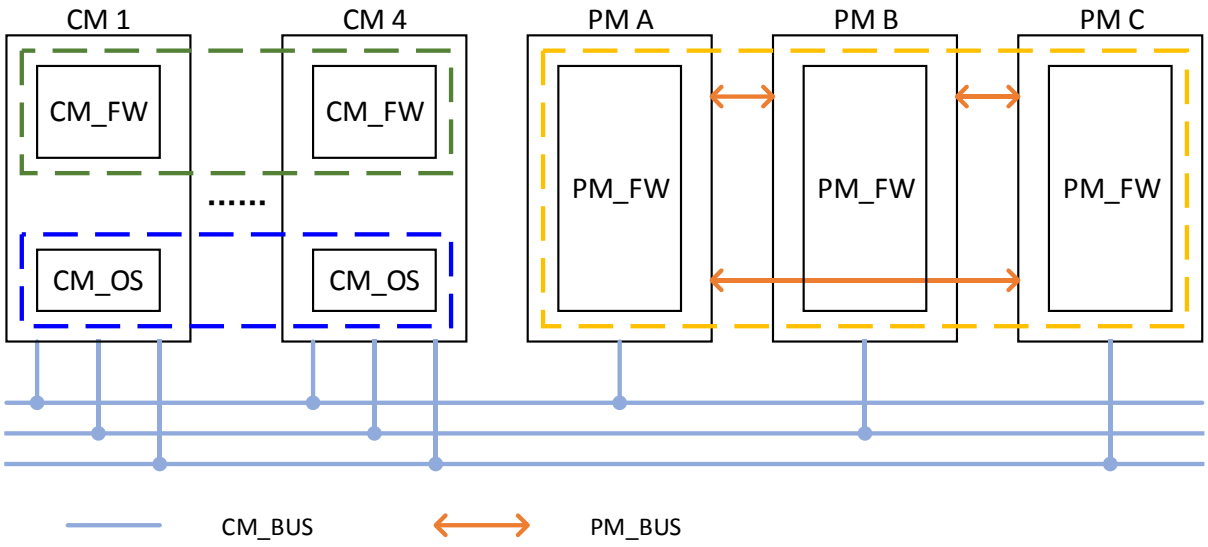

Figure 2-1 Software architecture

图 2-1 软件架构

- CM_FW: the part in the green dashed box is CM_FW. It is non-safety-related, but related to security.
- CM_OS: the part in the blue dashed box is CM_OS. It is non-safety-related, but related to security.
- PM_FW: the part in the yellow dashed box is PM_FW. It is safety-related, and related to security.
- CM_FW：图中绿色虚线框包含部分。CM_FW 为非安全相关部分，但涉及信息安全。
- CM_OS：图中蓝色虚线框包含部分。该软件为非安全相关部分，但涉及信息安全。
- PM_FW：图中黄色虚线框包含部分。PM_FW 为安全相关部分，同时涉及信息安全。

SWSC_SafR_NSecR_A_030

The functions of the above parts are shown as follows:

上述各子系统的具体功能如下图所示：

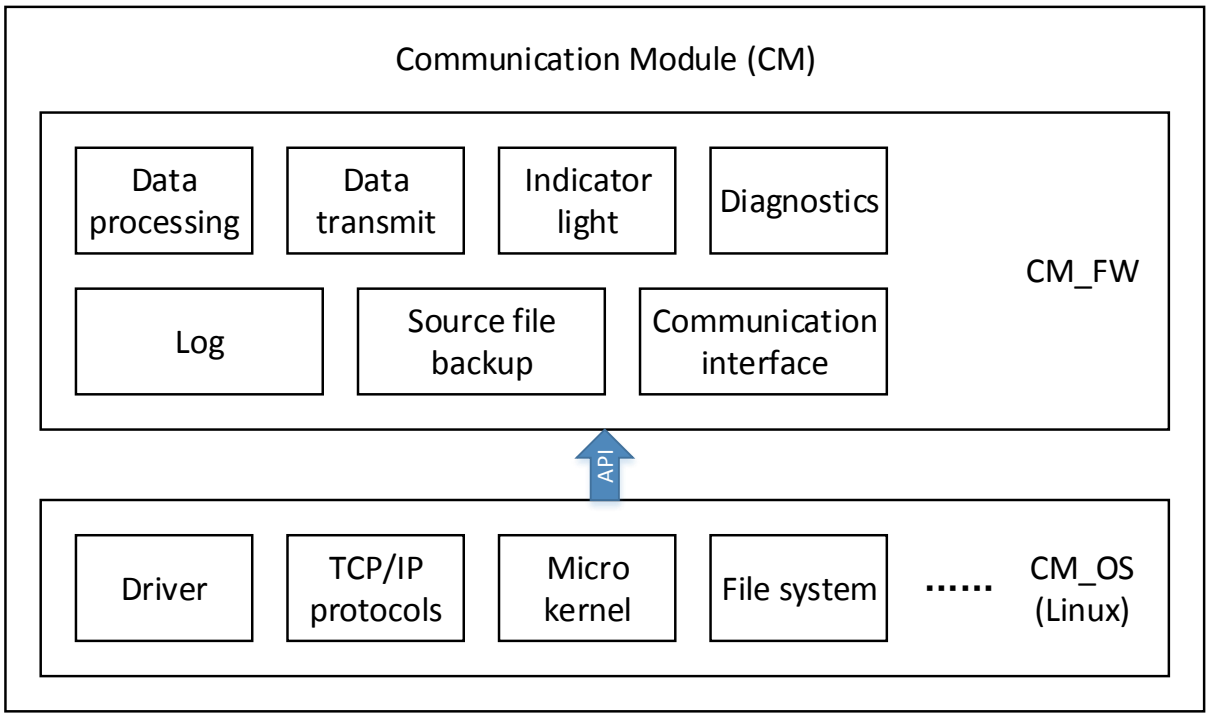

Figure 2-2 CM functions

图 2-2 CM 嵌入式软件功能

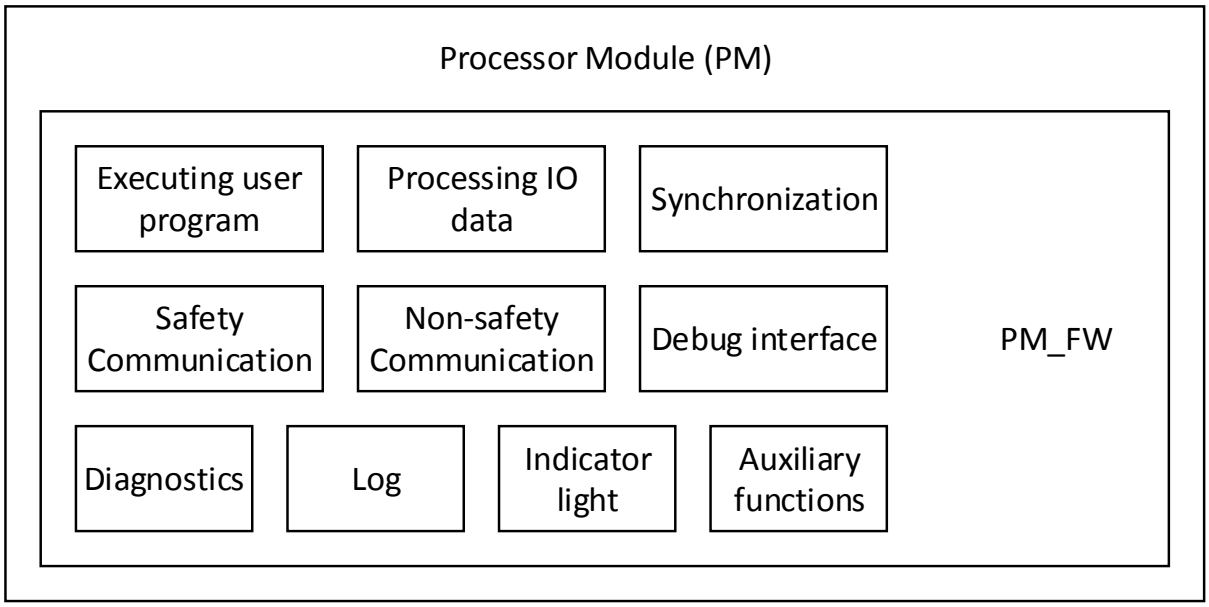

Figure 2-3 PM functions

图 2-3 PM 嵌入式软件功能

2.2 Data flow 数据流

SWSC_SafR_SecR_C_058

The control station uses System Net to communicate with PC software, uses Modbus

RTU/ASCII/TCP to communicate with the third-party device, and uses Safety Net to communicate with other control stations.

控制站对外通过 System Net 与各个上位机软件进行通讯，通过 Modbus RTU/ASCII/TCP 和第三方设备通讯，通过 Safety Net 与其他控制站进行通讯。

In the interior of the control station, CM_BUS is used for communication between CM and PM, PM_BUS is used for data exchange between PMs, and IP_BUS is the communication link between PM and IO modules.

控制站内部，PM 和 CM 之间通过 CM_BUS 通讯，PM 与 PM 之间通过 PM_BUS 进行通讯，PM 和 IO 模块之间通过 IP_BUS 通讯。

The communication links are shown in Figure 2-4:

各通讯链路如下图所示：

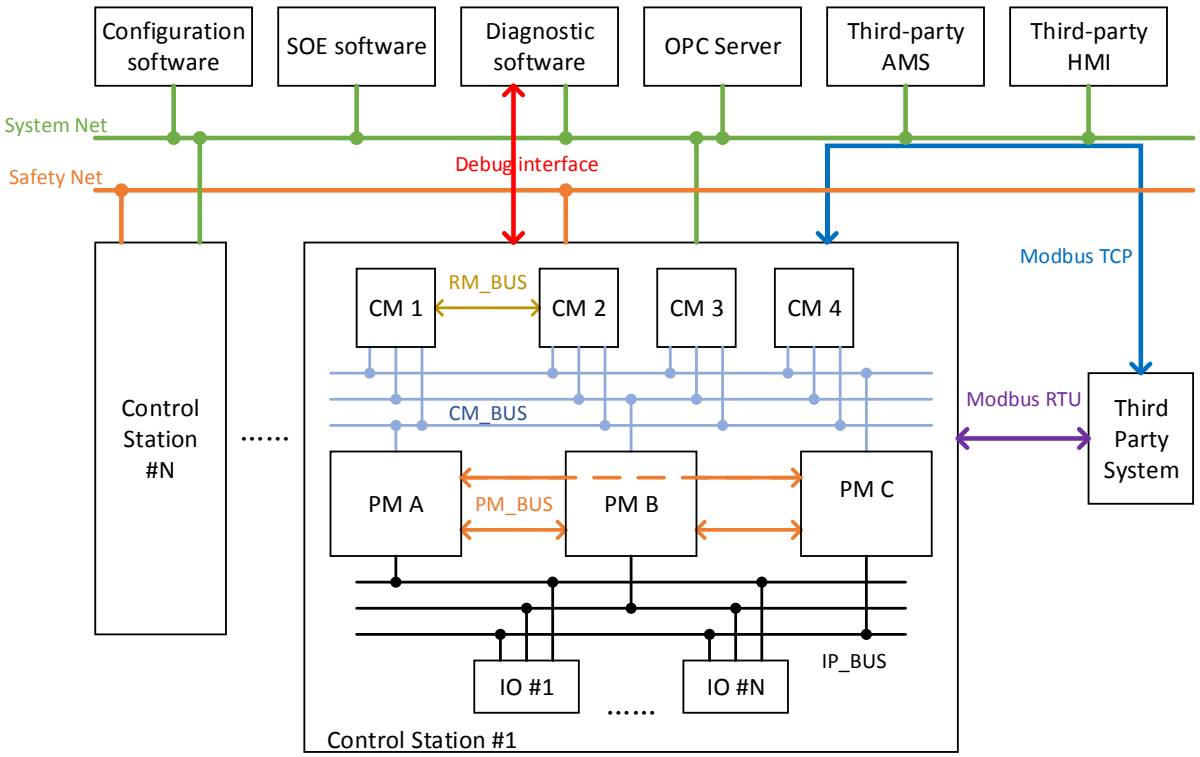

Figure 2-4 Control station communication links

图 2-4 控制站通讯示意图

The data streams related to the embedded software are shown in figure 2-5:

和嵌入式软件相关的数据流如下图所示：

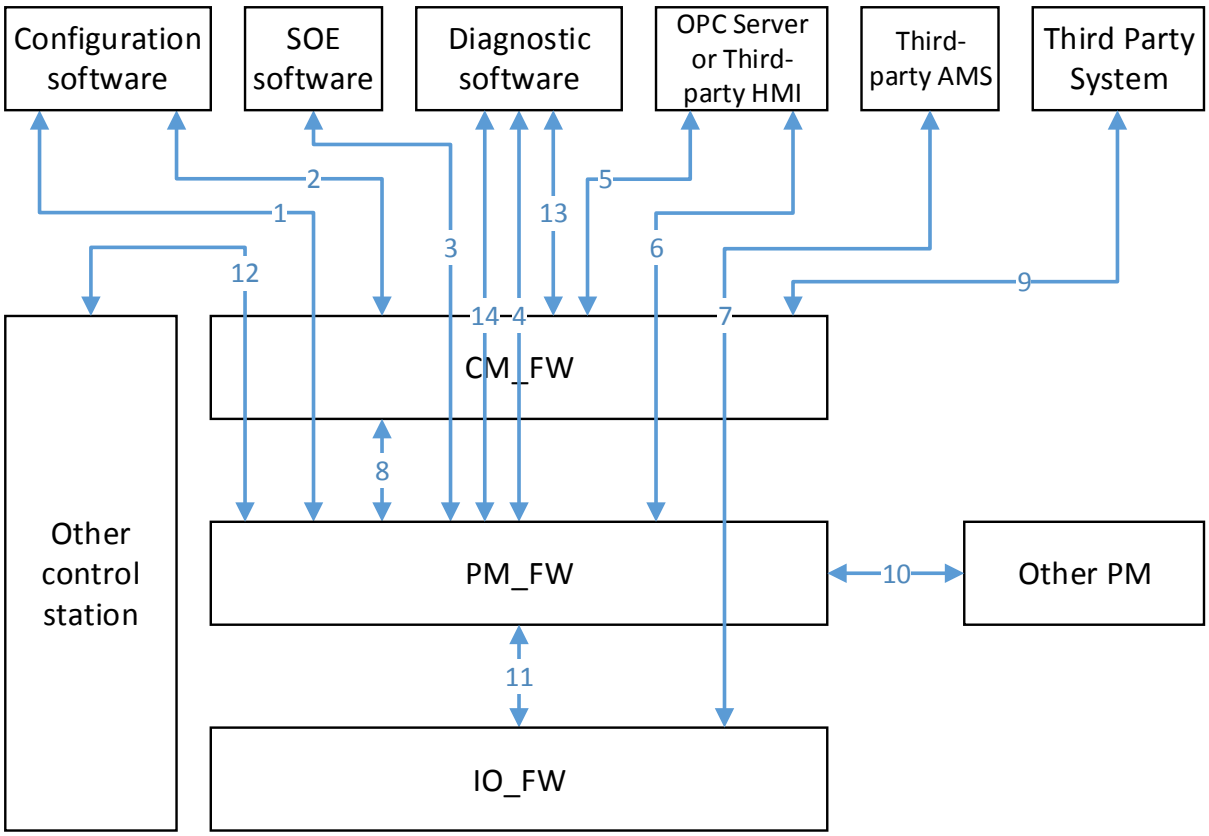

Figure 2-5 Communication data flow

图 2-5 数据流示意图

Data flow 1: Download or other debug operations by the Configuration software. CM forwards the data only, but not process the data. The data is protected by CRC to prevent any data corruption.

数据流 1：组态软件对控制站进行下装及调试。CM 只转发数据，不进行处理。该数据流使用 CRC 来保护数据的正确性。

Data flow 2: The configuration software reads variable from the control station. This command is directly processed by CM and not related to PM. The data is protected by CRC to prevent any data corruption.

数据流 2：组态软件从控制站读取实时数据。该数据流不经过 PM，使用 CRC 来保护数据的正确性。

Data flow 3: SOE software reads SOE records from control station. CM forwards the data only, but not process the data. The data is protected by CRC to prevent any data corruption.

数据流 3：SOE 软件从控制站读取 SOE 数据。CM 只进行转发，不进行处理。该数据流使用 CRC 来保护数据的正确性。

Data flow 4: Diagnostic software reads diagnostic data from the control station. CM forward the data only, but not process the data. The data is protected by CRC to prevent any data corruption.

数据流 4：诊断软件从控制站读取诊断数据。CM 只进行转发，不进行处理。该数据流使用 CRC 来保护数据的正确性。

Data flow 5: The OPC server (or third party HMI) reads variable from the control station. This command is directly processed by CM and not related to PM. The data is protected by CRC to prevent any data corruption.

数据流 5：OPC Server（或第三方 HMI）从控制站读取实时数据。该数据流不经过 PM，使用 CRC 来保护数据的正确性。

Data flow 6: Writing variable operation by the he OPC server (or third party HMI). CM forward the data only, but not process the data. The data is protected by CRC to prevent any data corruption.

数据流 6：OPC Server（或第三方 HMI）对控制站进行写变量操作。CM 只进行转发，不进行处理。该数据流使用 CRC 来保护数据的正确性。

Data flow 7: third party AMS software collects HART data from the IO modules and sends debug command to the IO modules. CM and PM forward the data only, but not process the data. The data is protected by CRC to prevent any data corruption.

数据流 7：第三方 AMS 软件从控制站采集 HART 数据及进行 HART 调试。CM、PM 只进行转发，不进行处理。该数据流使用 CRC 来保护数据的正确性。

Data flow 8: PM uploads variable value to the CM cyclically, sends configuration data to CM, and collects status information from the CM. The data is protected by CRC to prevent any data corruption.

数据流 8：PM 周期向 CM 上传实时数据、向 CM 发送配置数据以及从 CM 得到状态信息。该数据流使用 CRC 来保护数据的正确性。

Data flow 9: The communication with the third party systems through Modbus TCP or Modbus RTU/ASCII.

数据流 9：和第三方设备通过 Modbus TCP 或者 Modbus RTU/ASCII 进行数据通讯。

Data flow 10: Data exchanging between PMs through PM_BUS. The data flow uses proprietary safety protocol.

数据流 10：PM 之间通过 PM_BUS 通讯。该数据流采用安全协议。

Data flow 11: The communication between the control station and IO module through IP_BUS includes: Process data exchange, configuration information downloading, and diagnostic data uploading, etc. The data flow uses proprietary safety protocol.

数据流 11：该数据流用于控制站和 IO 模块之间的通讯，包括组态配置、实时数据交换、收集 IO 诊断数据等。该数据流采用安全协议。

Data flow 12: The data exchange between control stations. CM forwards the data only, but not process the data. The data flow uses proprietary safety protocol.

数据流 12：多个控制站之间的站间安全通讯。CM 只进行转发，不进行处理。该数据流采用安全协议。

Data flow 13: The CM debug interface is mainly used for reading internal fault information and internal log information of CM. This debug interface only can be used by developers. The interface uses serial port as a medium.

数据流 13：CM 的私有调试接口，主要用于对 CM 内部调试以及读取内部故障信息和内部日志，这些信息并不开放给用户。私有调试接口采用串口作为介质。

Data flow 14: The PM debug interface is mainly used for reading internal fault information and internal log information of PM. This debug interface only can be used by developers. The interface uses serial port as a medium.

数据流 14：PM 的私有调试接口，主要用于对 PM 内部调试以及读取内部故障信息和内部日志，这些信息并不开放给用户。私有调试接口采用串口作为介质。

The resource that is assigned to each data flow shall meet the maximum scale of control station.

分配给上述各数据流的资源大小应能满足系统最大规模的要求。

The data flow 1, 2, 3, 4, 5, 6, 7 and 9 will use System Net. If the maximum load is 40%, the data transmitted via System Net shall be less than 5MB per second. Therefore, it is necessary to limit the size of communication variables in the project.

数据流 1、2、3、4、5、、7、9 使用 System Net，按最大 40%负荷计算，在正常运行过程中，控制站每秒钟通过 System Net 发送和接收的数据应小于 5MB，因此，需要限制用户工程中通讯点的规模。

2.3 Running process 运行流程

2.3.1 Software state transition 软件状态转化

SWSC_SafR_NSecR_B_031

CM is mainly used for communications, which is not affected by the state of the system. The software states of PM and state transition conditions are shown in the following figure:

CM 主要用于通讯，不受系统状态的影响。PM 软件状态的状态描述以及状态转换条件如下图所示：

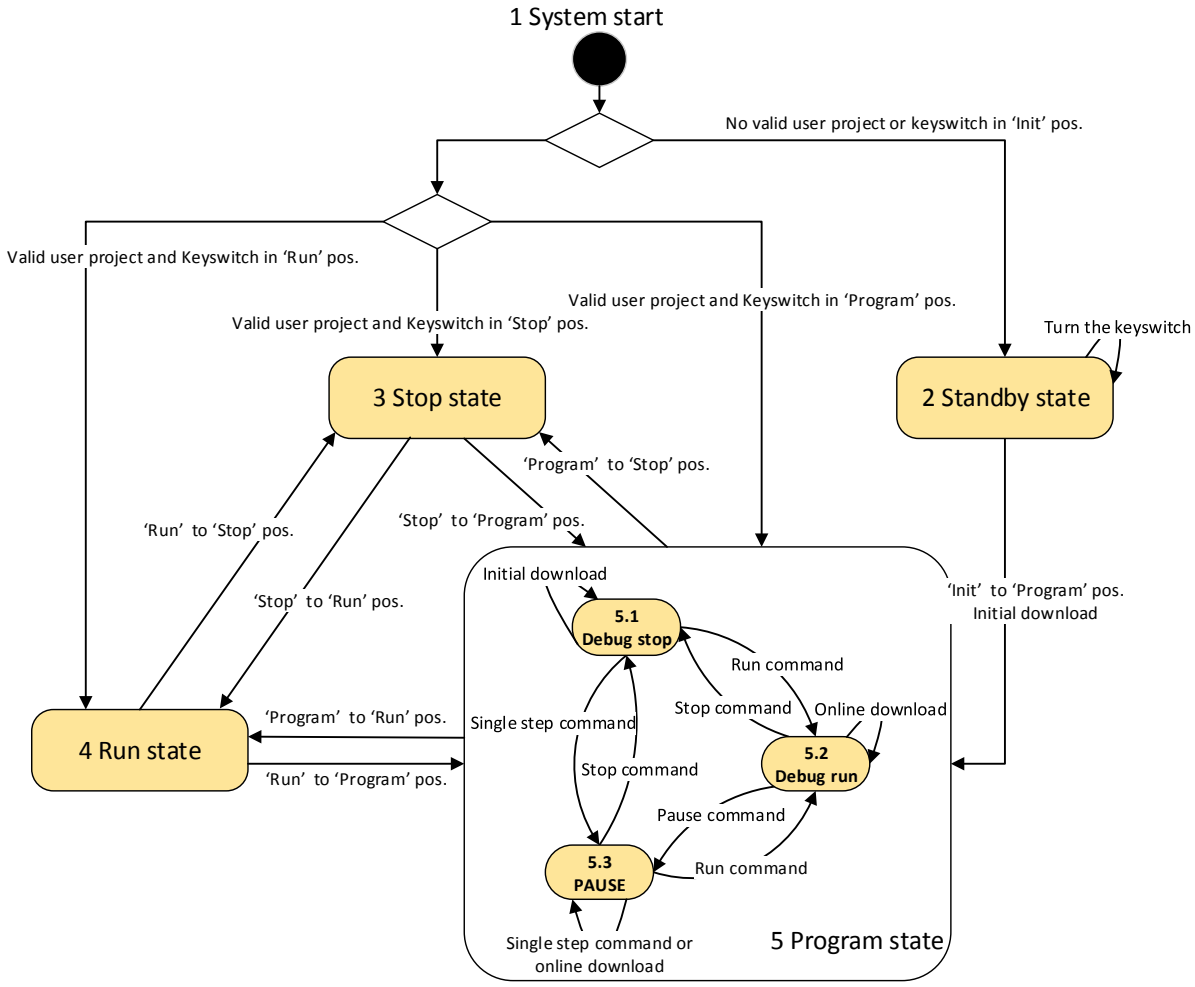

Figure 2-6 Transition of software states

图 2-6 软件状态转换图

When the PM has a valid project, the Stop, Run, Program states of PM software are consistent with the 'Stop', 'Run', 'Prog' position of the key switch, and also correspond to the system states. The 'Init' position means the project and configuration information in PM will be purged after power on.

当 PM 中有有效工程时，PM 软件的 Stop、Run、Program 状态和钥匙开关的 STOP、RUN、PROG 三个档位一一对应，也和系统的三个状态一一对应。钥匙开关中的 Init 档位代表上电时清空工程及配置信息。

Detailed descriptions of the states are as follows:

状态具体描述如下：

- System start: System start into a different state according to the validity of project and the positon of key switch. When the project is valid and the key switch is in the 'Prog' position, the software enters into Debug run state.
- System start：系统启动，根据工程的有效性及钥匙开关的档位进入不同的状态。当工程有效，并且钥匙开关在 PROG 档位时，软件进入 Debug run 状态。

- Stop state: In this state, PM has a project, but neither execute the user program, nor support user debug operation. PM set the DO and AO modules in this channel into safe state. In this state, if the key switch turn from ‘Stop’ to ‘Prog’ position, the software enters into Debug stop state.
- Stop state：PM 有用户工程，但不执行用户程序，也不支持用户进行调试操作。PM 置对应系的 DO 和 AO 模块为安全状态。在此状态下，钥匙开关从 STOP 到 PROG 档位，软件进入 Debug stop 状态。
- Run state: In this state, PM executes user program and exchanges data with IO modules, but does not support user debug operation. In this state, if the key switch turn from ‘Run’ to ‘Prog’ position, the software enters into Debug run state.
- Run state：PM 执行用户程序，实时输出，不支持用户进行调试操作。在此状态下，钥匙开关从 RUN 到 PROG 档位，软件进入 Debug run 状态。
- Standby state: There is no valid project in PM.
- Standby state：PM 中无用户工程。
- Program state: In this state, PM has a project and supports user debug operation.
- Program state：PM 有用户工程，支持用户进行调试操作。
- Pause: PM has a user project, but does not execute the user program. PM exchanges data with IO modules but the outputs is the last execution result before the pause operation. If the user program has not been executed before the pause operation, the output is the initial value.
- Pause：PM 有用户工程，但不执行用户程序。保持和 IO 模块交换数据，输出为暂停前最后一次运算的结果，如暂停前没有经过一次运算，输出为初始值。
- Debug run: In this state, PM executes user program, exchanges data with IO modules, and supports user debug operation.
- Debug run：PM 执行用户程序，实时输出，可进行其他调试操作。
- Debug stop: In this state, PM has a project, but does not execute the user program, does not exchange data with IO modules, but supports user debug operation.
- Debug stop：PM 有用户工程，但不执行用户程序，停止和 IO 模块交换数据，可进行其他调试操作。

The states of three PMs are consistent. The reason is show as follows:

- The three PMs can get the key switch position simultaneously.
- The new-inserted PM can be synchronized automatically by other running PMs for the

running data, running state and the project.

三系 PM 状态一致，原因如下：

- 钥匙开关同时作用于三系 PM。
- 当 PM 上电时，会从工作 PM 同步工程及状态。

2.3.2 PM synchronization PM同步

2.3.2.1 Running synchronization 同步运行

SWSC_SafR_NSecR_A_032

Hardware synchronization clock ensures that each PM_FW can obtain the same time from the clock, and three PMs agreed to start executing the user program at some fixed time (such as T1 + nT). For the above reason, the user program can be executed synchronously.

硬件同步时钟保证各系 PM_FW 从该时钟得到的数值一致，三系 PM_FW 约定在固定时刻（如下图中的 T1+nT）开始执行用户程序，最终保证用户程序三系同步执行。

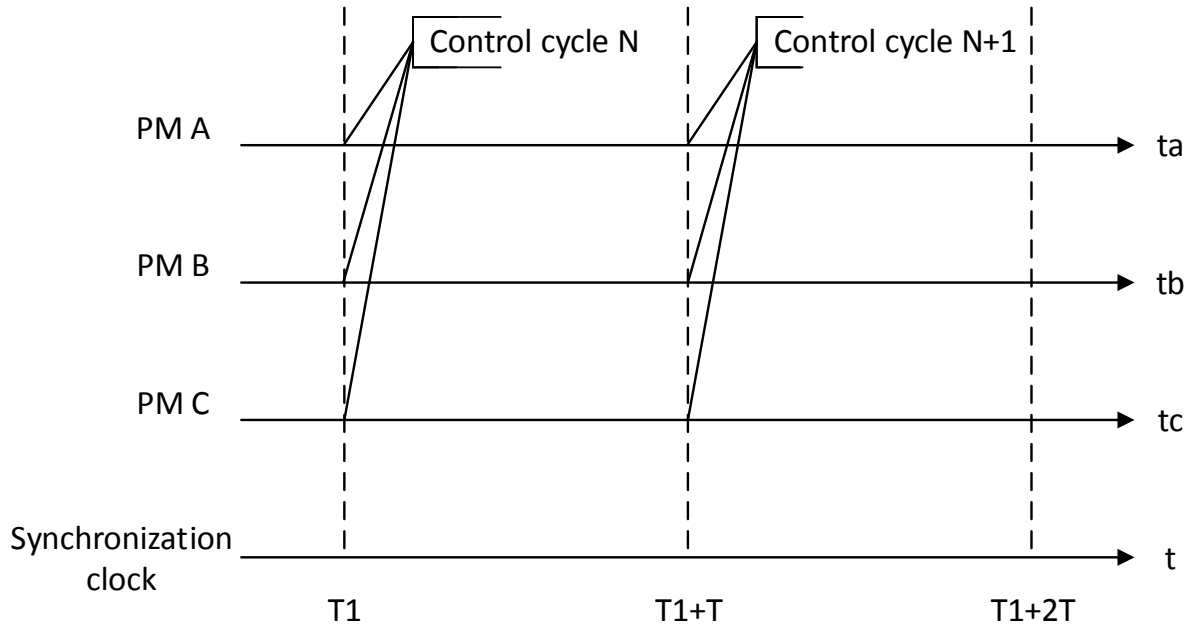

Figure 2-7 Running synchronization

图 2-7 同步运行

The user program can be configured as both stop and alarm or only alarm when executing timeout occurs. This property is configured by the user through configuration software for each user program. When safety application is selected by the user, this property can be only configured to ‘stop executing the user program and alarm’; when control application is selected by the user, both “stop executing the user program and alarm” and “only alarm” can be configured.

当执行用户任务超时，可配置停止执行此用户程序并报警或仅报警。该属性由使用者通过

组态软件基于每个任务配置。用户选择 safety 应用时，该属性只能配置为停止执行此用户程序并报警；用户选择 control 应用时，都可以配置。

The new-inserted PM will synchronize project, real time data and running states from other running PMs automatically, and the new-inserted PM will be automatically running after the synchronization. The user program execution will be delayed due to real time data synchronization, and the delayed time is related to the size of real time data. According to data size of the actual user project, the maximum delayed time is no more than three control cycles.

新插入的 PM 会自动从其他工作 PM 上同步工程、运行数据及运行状态，同步完成后新 PM 自动运行，不需要人工干涉。在同步实时数据会暂停工作 PM 执行用户工程，暂停时间与工程的数据量相关，根据对实际工程数据量的估算，该延后时间不大于 3 个控制周期。

2.3.2.2 Operation synchronization 命令同步

SWSC_SafR_NSecR_A_033

The PMs shall synchronize the operations from the PC software. Operation, which is responded directly by CM, such as read variable, does not need synchronization.

PM 接收到的上位机软件的操作命令需要同步处理，但是如读变量命令等由 CM 直接应答的命令不需要同步。

2.3.3 Function assignment of dual CPU cores 双核任务分配

SWSC_SafR_NSecR_A_034

The PM is processing in AMP (Asymmetric multi-processing) mode, and the assignment of the functions of dual CPU cores is shown in follows:

PM 双核按照 AMP 模式运行，双核功能划分如下所示：

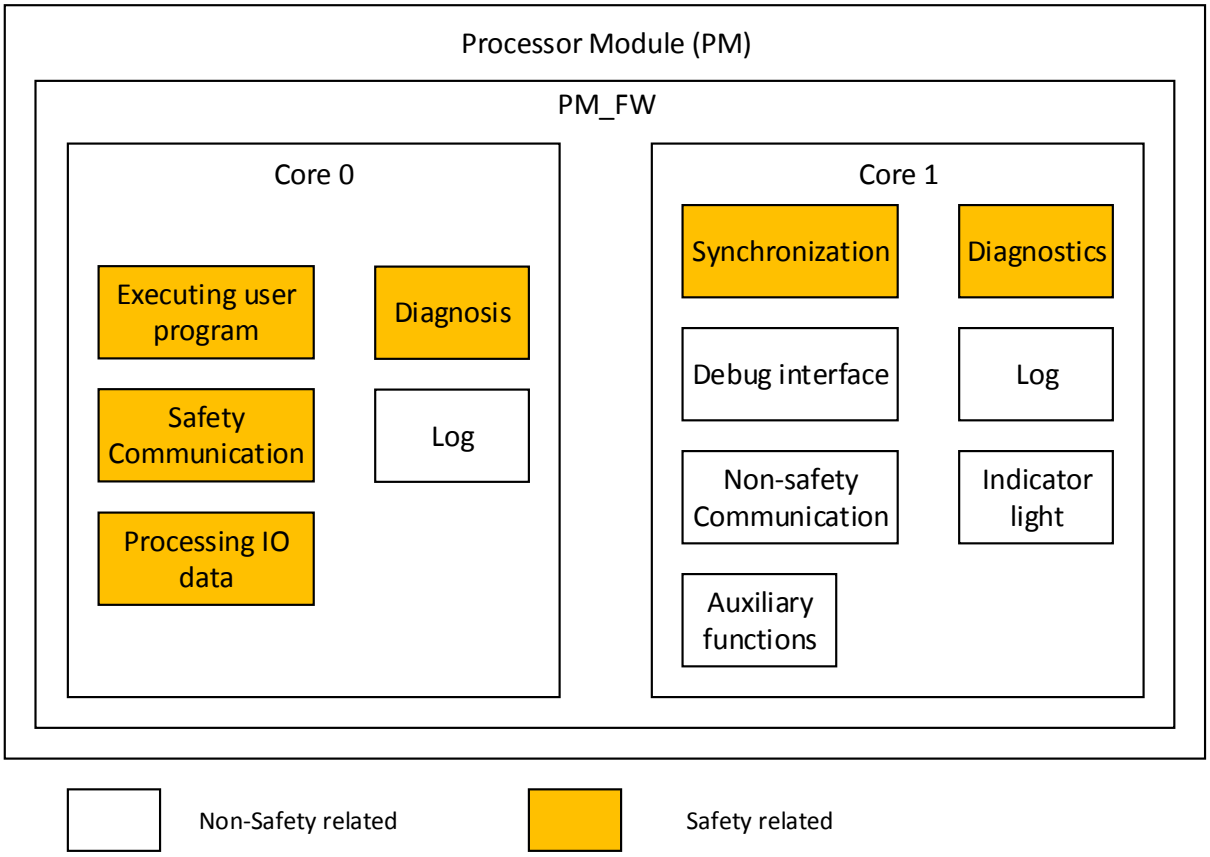

Figure 2-8 Function assignment of dual CPU cores

图 2-8 PM 双核功能划分

2.4 Multitasking 多任务

2.4.1 Task scheduling 任务调度

SWSC_SafR_NSecR_A_035

Multitasking refers to the maximum capability of the system is two user programs. Therefore, PM_FW in Core0 includes three processes, one is the basic functions (i.e. RTS), another one is UP1, and the last one is UP2.

多任务指的是系统最多支持执行 2 个用户程序，因此，PM_FW 中 Core1 分为三个进程，基本功能为一个进程（简称 RTS），UP1 为一个进程，UP2 为一个进程。

The final minimum control cycle is the maximum of the minimum control cycle (consider the execution time only) and the minimum control cycle (consider the polling time only) described below.

最终的最小控制周期是下述最小控制周期（只考虑执行时间）和最小控制周期（只考虑 IO 轮询时间）中的最大值。

Core0 uses round-robin mechanism, the size of the time slice is 0.25ms. The switch of time slice relies on clock interrupt, which is provided by hardware synchronization clock, in order to ensure that the three PMs are synchronous.

Core0 采用时间片轮转机制，时间片的大小为 0.25ms。时间片的轮转依靠时钟中断实现，为了保证三系同步，时钟中断由三系的同步时钟提供。

CPU cycle is 5ms, including RTS time, UP1 time and UP2 time. The allocated time for RTS is 3.5ms. The sum of allocated time for the UP1 and UP2 is 1.5ms, and the default division is 1ms (UP1) + 0.5ms (UP2). Users can adjust the division, and the division proportion moves between 20% - 90%.

CPU cycle 为 5ms，包括 RTS 时间、UP1 时间和 UP2 时间。其中，分配给 RTS 的时间片之和为 3.5ms，分配给 UP1 和 UP2 的时间片之和为 1.5ms，默认按照 1ms（UP1）+0.5ms（UP2）划分。用户可以调整 UP1 和 UP2 的时间片分配，分配比例在 20%-90%之间移动。

Each UP can be executed in one CPU cycle or split into more than one CPU cycle to execute, and the control cycle is a multiple of 5ms. Based on the estimated execution time and the size of the allocated time slice, the minimum control cycle (consider the execution time only) of UP can be obtained. If the actual control cycle set by user is greater than the minimum control cycle, extra time is idle.

UP1、UP2 可以在一个 CPU cycle 内执行或者拆分到多个 CPU cycle 内执行，UP1、UP2 的控制周期为 5ms 的倍数。对单个 UP，根据估算的执行时间以及分配的时间片大小，可以得到最小控制周期（只考虑执行时间），如果用户实际配置的控制周期大于最小控制周期，多余的时间内为空闲。

An example is shown in Figure 2-9:

例子如图 2-9 所示：

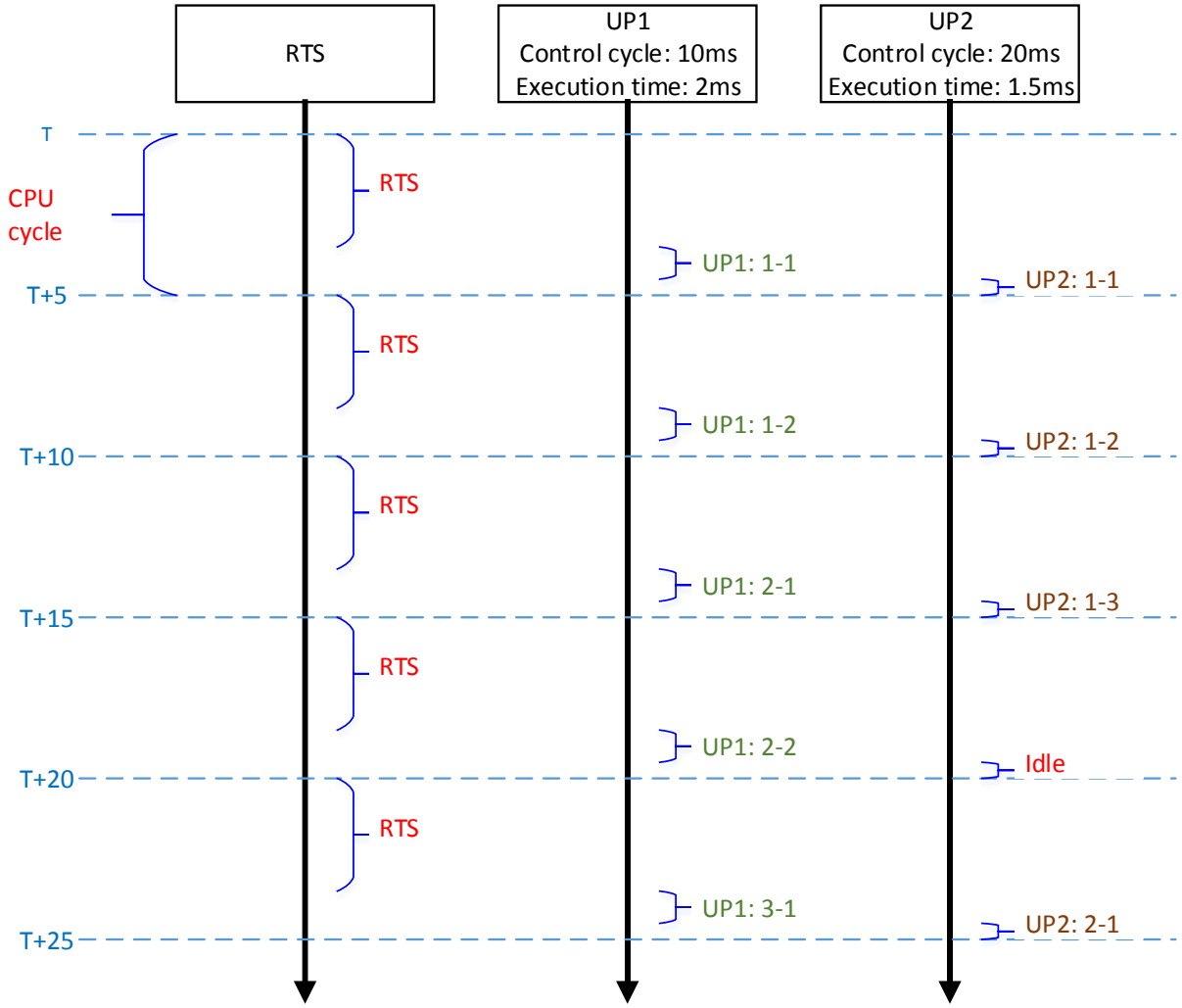

Figure 2-9 PM task scheduling

图 2-9 PM 任务调度

2.4.2 IO polling IO轮询

SWSC_SafR_NSecR_A_036

The IO modules, which shall be polled by the master of IP_BUS in the current CPU cycle, are assigned by the PM. According to the requirement of the control cycle when the system scale is 300 points, the master shall poll 13 IO modules per cycle. It also meet the requirement of the control cycle when the system scale is 1000 points. The division proportion of the 13 IO modules for each user program is the same as the division proportion of allocated time (1.5ms).

主站当前 CPU 周期轮询的从站由 PM 指定。根据系统规模 300 点时对控制周期的要求，每周期需要轮询 13 个 IO 从站。该从站个数同时能够满足系统规模 1000 点时对控制周期的要求。每周期轮询的 IO 从站的比例分配和任务的比例分配一致。

An example is shown in Figure 2-10:

例子如图 2-10 所示：

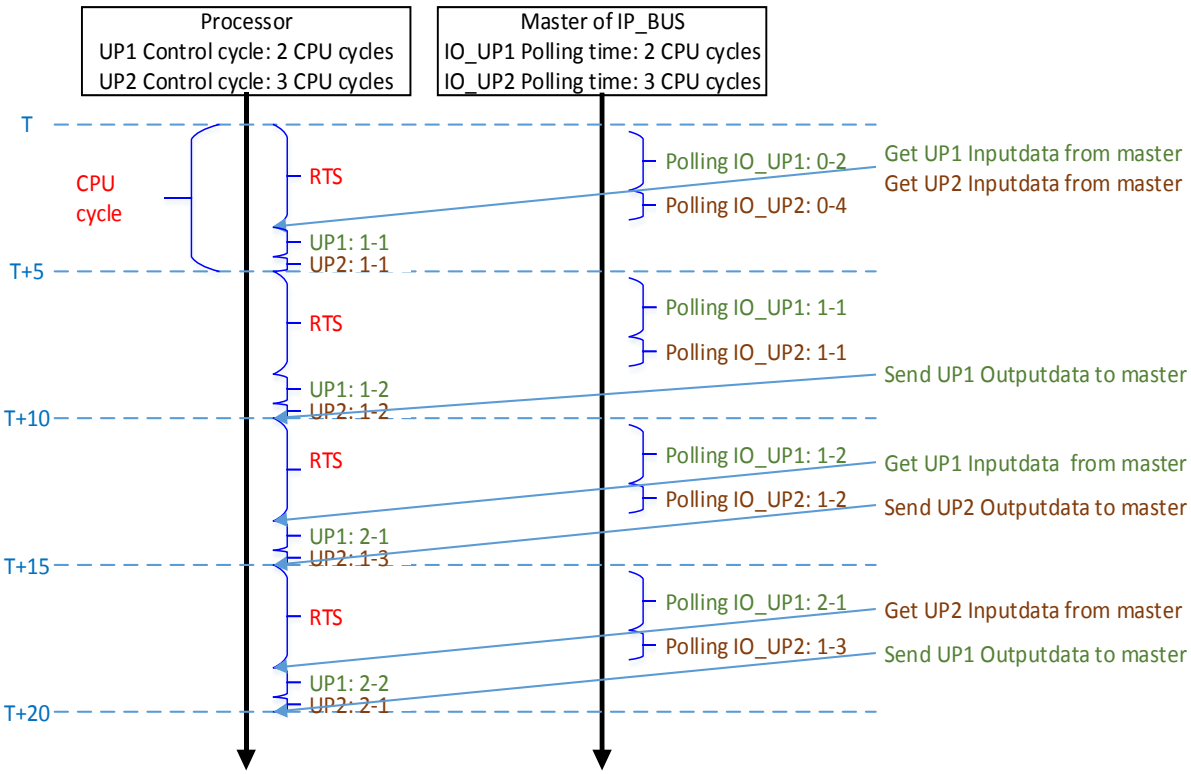

Figure 2-10 IO polling

图 2-10 IO 轮询

Based on the total number of IO modules and polling number per cycle, the minimum control cycle (consider the polling time only) of UP can be obtained. If the actual control cycle set by user is greater than the minimum control cycle, extra time is idle.

对单个 UP，根据总的 IO 个数以及每周期轮询的模块个数，可以得到最小控制周期（只考虑 IO 轮询时间），如果用户实际配置的控制周期大于最小控制周期，多余的时间内为空闲。

2.4.3 Variable area definition & mapping 变量定义与映射

SWSC_SafR_NSecR_A_037

In the configuration software, users can define variables for each user programs, and there is no common variables between user programs.

在组态软件中，用户可以为 UP1 和 UP2 各自定义变量，UP1 和 UP2 之间无共用的变量。

Users can specify which user program an IO module belongs to, and each user program can only access their own IO variables. The maximum size of the I Area and Q Area based on the system maximum scale.

用户可以为每个 IO 模块指定属于哪个任务，每个任务只能访问属于自己的 IO 变量。输

入输出数据区大小的应能满足系统最大规模的要求。

Each user program has its own variable area. Two variable areas are independent, and do not overlap. Each user programs can only access their own variable area.

每个任务有自己的变量区，两个变量区独立成片的，互不交叉，每个任务的变量只能在本任务中被访问。

The variable mapping is designed instead of using common variable. For example: variable A is defined in user program 1, if user program 2 wants to use this variable, it can define a variable B, and designated the variable mapping as A -> B.

如果任务间有共用的数据，可以通过变量映射的方式来代替。例如：UP1 中有变量 A，如果 UP2 想要使用该变量，可以定义变量 B，并且指定为 A->B。

The division of variable area is shown in figure 2-11:

变量区划分如下图所示：

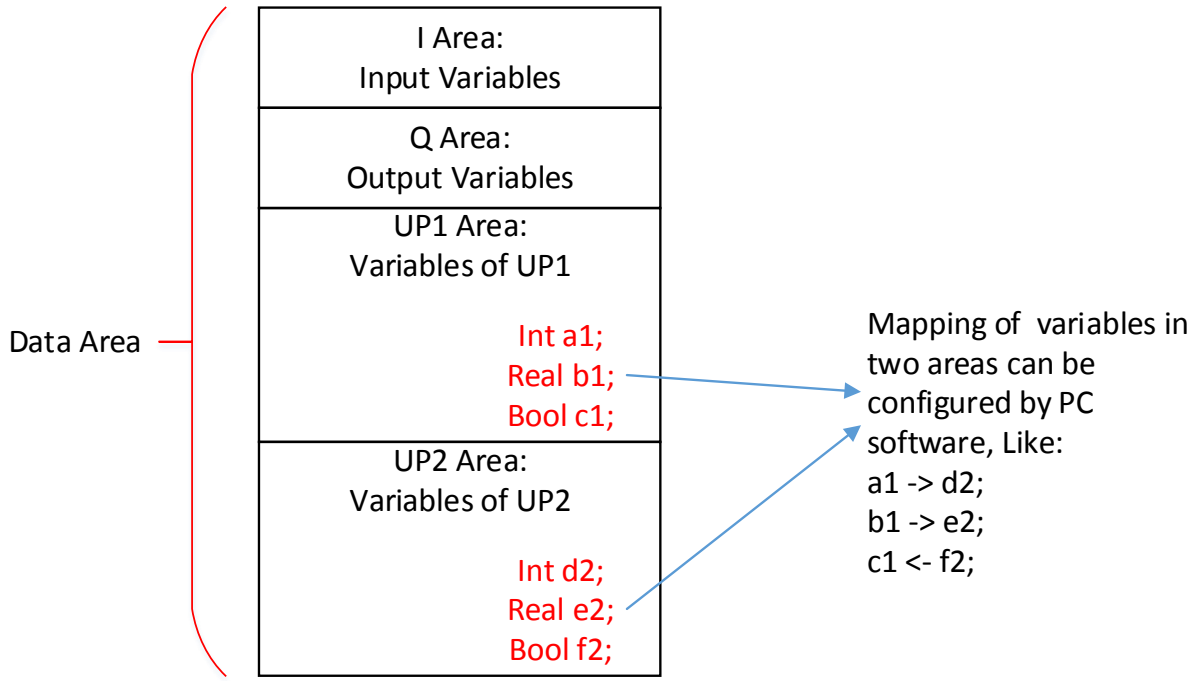

Figure 2-11 Variable area definition & mapping

图 2-11 变量定义与映射

2.4.4 Data consistency 数据一致性

SWSC_SafR_NSecR_A_038

Data area is divided into three parts: Data_UP1, Data_UP2 and Data_FW. The user program 1 task uses Data_UP1, user program 2 task uses Data_UP2, and RTS task uses Data_FW. UP1 task copies data in area I of Data_FW to area I in Data_UP1 before executing the user program, and copies

data in area Q and G of Data_UP to Data_FW respectively after the user program has been completely executed. The whole process is the same for UP2 task.

数据区分为 Data_UP1，Data_UP2 和 Data_FW 三个区，UP1 使用 Data_UP1，UP2 使用 Data_UP2，RTS 使用 Data_FW。UP 在执行用户程序前将输入数据从 Data_FW 的 I 区拷贝至 Data_UP 的 I 区，执行用户程序后将 Data_UP 的 Q 区和 G 区拷贝至 Data_FW 的 Q 区和 G 区。

The debug operation is only handled after the user program has been completely executed.

对每个 UP 的调试变量操作在用户程序执行结束后进行，执行过程中不执行写变量操作。

The diagram is shown in Figure 2-12 and Figure 2-13:

过程如图 2-12 和 2-13 所示：

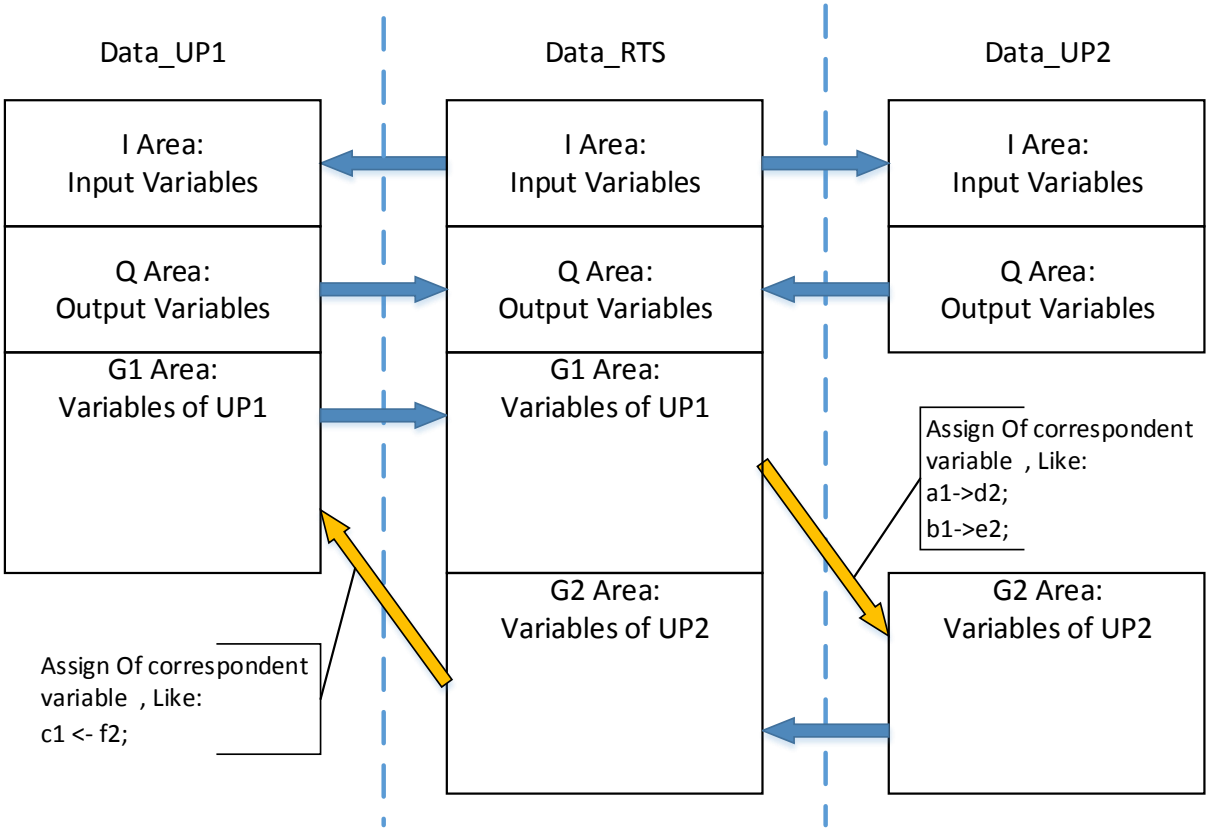

Figure 2-12 Data flow of data consistency

图 2-12 数据一致性数据拷贝

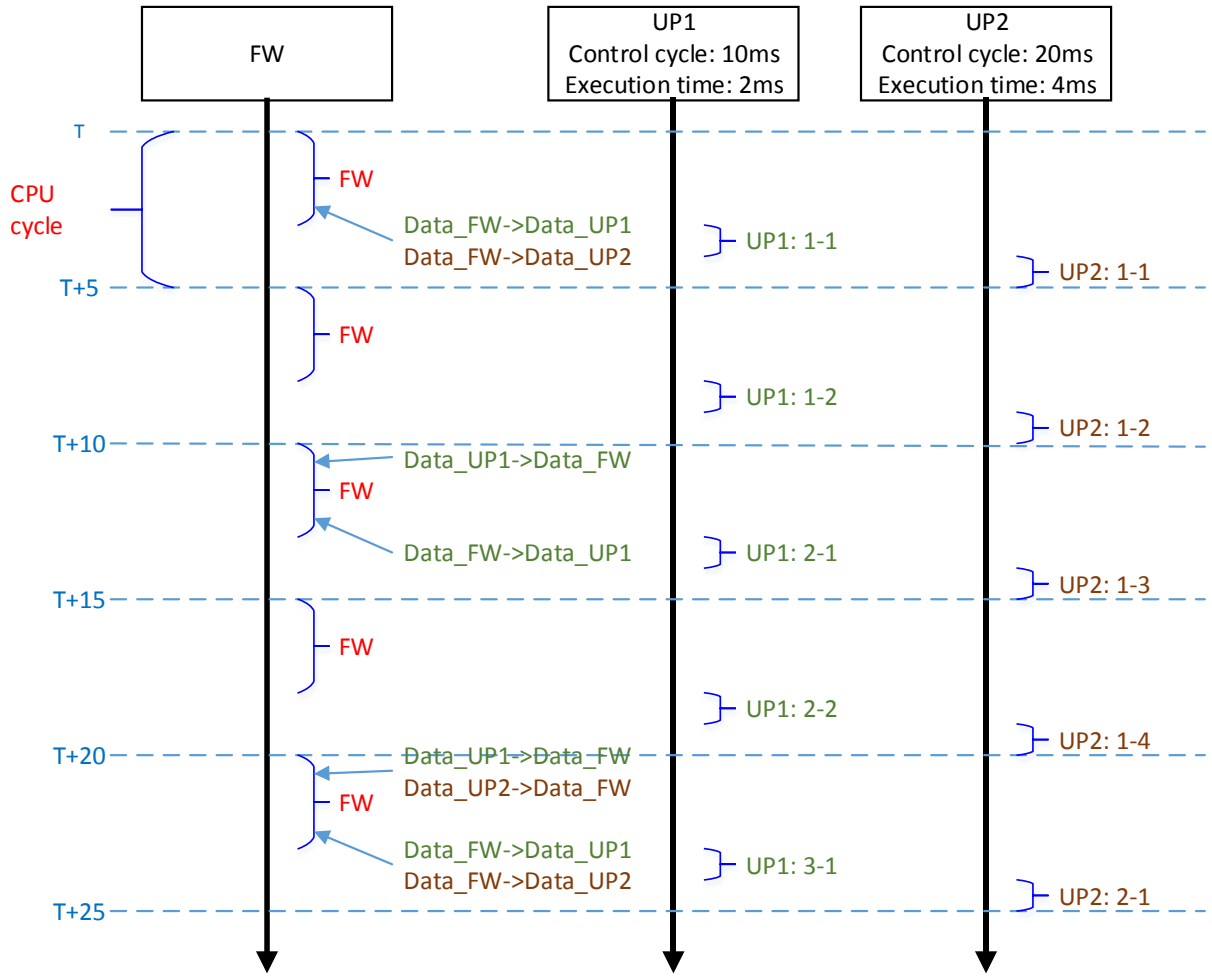

Figure 2-13 Sequence of data consistency

图 2-13 数据拷贝时序

2.4.5 The object of operation 操作命令对象

SWSC_SafR_NSecR_A_039

Operation from PC software can be handled by specific user program or handled by both user programs, as shown in table 2-1:

上位机软件的操作命令支持对单个任务或者多个任务操作，区分如下表所示：

Table 2-1 Operation object

表 2-1 操作命令对象

Operation 操作命令	Source 来源	Support handled by specific user program 是否支持对单个任务操作
Stop 停止	Configuration software 组态软件	Supported. 支持。

Pause 暂停	Configuration software 组态软件	Supported. 支持。
Single step 单步运行	Configuration software 组态软件	Supported. 支持。
Run 运行	Configuration software 组态软件	Supported. 支持。
Download 初始化下装	Configuration software 组态软件	Not supported. 不支持。
Online download 在线下装	Configuration software 组态软件	Not supported. 不支持。
Write variable 写变量	Configuration software 组态软件	Unrelated 不相关。
Write variable 写变量	HMI	Unrelated 不相关。
Write variable 写变量	OPC Server	Unrelated 不相关。
Enable/disable 使能/禁止	Configuration software 组态软件	Unrelated 不相关。

2.5 Diagnostics 诊断

2.5.1 CPU

SWSC_SafR_NSecR_B_040

Diagnostic measures for CPU in PM is listed in Table 2-2.

对于 PM 的 CPU，诊断措施列在表 2-2 中。

Table 2-2 Diagnostic measures for CPU in PM

表 2-2 PM CPU 诊断措施列表

CPU	**Complexity/ HFT 复杂度/HFT**	**Fault considered [DC] 考虑的故障[DC]**	**Safety critical? 是否安全相关**	**Diagnostics (normal operation) 诊断方法（正常运行）**	**Diag. interval/ DC 诊断间隔/诊断覆盖率**	**Diagnostics (power-on) 诊断方法（上电）**	**Action after detection of failure 故障处理措施**	**Detection and report of "failure of a diagnostic to execute" 对诊断措施未执行的检测和上报措施**
CPU register, internal RAM CPU 寄存器与内部 RAM	Type B HFT=1	DC fault (data & address) [Medium] DC 故障（数据和地址）[中]	Yes 是	Internal RAM is not used. March SS for CPU registers. Instruction cache is checked using dedicated instruction patterns. Data cache is checked by March SS. SFRs are periodically readback or readback after writes	< 24h DC is medium DC 为中	The same as in normal operation 同正常运行时	Alarm and adopt "first error restart" mechanism 故障报警，并使用"首发错误重启"机制	Temporal and logical program sequence monitoring is used for diagnostic related programs. 对实现诊断功能的 CPU 软件做基于逻辑和时间的程序流检测

				不使用内部 RAM； 对寄存器进行 March SS； 对指令 Cache 进行设定的指令操作并检查； 对数据 Cache 进行 March SS； 对 SFR 周期回读或在写入后回读				
		Soft error [Medium] 软失效[中]	Yes 是	Temporal and logical monitoring of program sequence including program sequence monitoring and check for validataion before execution. Other diagnostics regarding corresponding SFR. 基于逻辑和时间的程序流监测，如程序顺序监测、执行前的合法性检查等； SFR 还可在其他与其功能相关的诊断时同时诊断	Continuous for program sequence monitoring; <24h for other measures 对程序顺序监测为连续； 对其他措施为<24h DC is medium DC 为中	The same as in normal operation 同正常运行时	Alarm and adopt “first error restart” mechanism 故障报警，并使用“首发错误重启”机制	Temporal and logical program sequence monitoring is used for diagnostic related programs. 对实现诊断功能的 CPU 软件做基于逻辑和时间的程序流检测
CPU coding & execution CPU 编码与执行	Type B HFT=1	Wrong coding or wrong execution (including flag registers) [Medium] 错误的编码与执行（包括标志寄存器）[中]	Yes 是	Full instruction set test. Check the flag registers by test patterns resulting in register transition. CPU illegal operation and instruction trapping. Periodic software readback of static configuration registers.	Continuous for exception handling and watchdog. <24h for other measures 对异常处理和看门狗为连续； 对其他措施为<	The same as in normal operation 同正常运行时	Alarm and adopt “first error restart” mechanism 故障报警，并使用“首发错误重启”机制	Temporal and logical program sequence monitoring is used for diagnostic related programs. Redundant status pulse added from CPU to watchdog to

				External watchdog (in FPGA) with separate time base (Clock of FPGA) and time window. 全指令集检测； 制造标志寄存器复位/置位条件并检查结果； CPU 异常处理； 周期回读静态的配置寄存器； 带时间窗和独立时基（FPGA 诊断时钟）的外部看门狗（FPGA 中）	24h DC is medium DC 为中			indicate whether CPU is properly reset. Self-diagnostics of watchdog logic inside FPGA. 对实现诊断功能的 CPU 软件做基于逻辑和时间的程序流检测； CPU 到看门狗增加冗余状态脉冲指示是否被复位； FPGA 内的看门狗逻辑自诊断
Address calculation 地址计算	Type B HFT=1	DC fault [Medium] DC 故障[中]	Yes 是	March SS of address lines in unused memory space. Other diagnostics regarding CPU registers, variable memories and invariable memories. 在未使用的存储空间内，对地址线进行 March SS； 在进行 CPU 寄存器、可变存储器、不可变存储器诊断时同时诊断	< 24h DC is medium DC 为中	The same as in normal operation 同正常运行时	Alarm and adopt “first error restart” mechanism 故障报警，并使用“首发错误重启”机制	Temporal and logical program sequence monitoring is used for diagnostic related programs. 对实现诊断功能的 CPU 软件做基于逻辑和时间的程序流检测
		Soft error [Medium] 软失效[中]	Yes 是	Temporal and logical monitoring of program	Continuous 连续	The same as in normal operation	Alarm and adopt “first	Temporal and logical program sequence

				sequence including program sequence monitoring and check for validataion before execution. 基于逻辑和时间的程序流监测，如程序顺序监测、执行前的合法性检查等	DC is medium DC 为中	同正常运行时	error restart" mechanism 故障报警，并使用“首发错误重启”机制	monitoring is used for diagnostic related programs. 对实现诊断功能的 CPU 软件做基于逻辑和时间的程序流检测
Program counter, stack pointer 程序计数器，堆栈指针	Type B HFT=1	DC fault [Medium] DC 故障[中]	Yes 是	Diagnostics regarding CPU coding and execution. Check during stack push and pop. Stack range detection. March SS for stack pointer registers. 在进行 CPU 编码与执行诊断时同时诊断； 对堆栈指针做压栈、出栈和范围检测； 对堆栈指针寄存器做 March SS	Continuous for stack diagnostics; <24h for other measures 对堆栈诊断为连续； 对其他措施为 < 24h DC is medium DC 为中	The same as in normal operation 同正常运行时	Alarm and adopt "first error restart" mechanism 故障报警，并使用“首发错误重启”机制	Temporal and logical program sequence monitoring is used for diagnostic related programs. 对实现诊断功能的 CPU 软件做基于逻辑和时间的程序流检测
		Soft error [Medium] 软失效[中]	Yes 是	Temporal and logical monitoring of program sequence including program sequence monitoring and check for validataion before execution. 基于逻辑和时间的程序流监测，如程序顺序监测、执行前	Continuous 连续 DC is medium DC 为中	The same as in normal operation 同正常运行时	Alarm and adopt "first error restart" mechanism 故障报警，并使用“首发错误重启”机制	Temporal and logical program sequence monitoring is used for diagnostic related programs. 对实现诊断功能的 CPU 软件做基于逻辑和时间的程序流

				的合法性检查等				检测
Interrupt 中断	Type B HFT=1	No, continuous or crossover of interruptions [Medium] 无中断、Continuous 连续中断或中断串扰[中]	Yes 是	Temporal monitoring of multi-tasking interrupt. Watchdog of PM_BUS communication protocol. Software check by creating interrupt condition (except the multi-tasking interrupt) Disable and monitoring of unused interrupt. 对多任务中断，使用基于时间的程序流监测； PM_BUS 通讯协议的看门狗； 制造中断条件并检查（除多任务中断外）； 禁用并监视未使用的中断	<24h DC is medium DC 为中	The same as in normal operation 同正常运行时	Alarm and adopt “first error restart” mechanism 故障报警，并使用“首发错误重启”机制	Temporal and logical program sequence monitoring is used for diagnostic related programs. 对实现诊断功能的 CPU 软件做基于逻辑和时间的程序流检测
Reset circuitry 复位电路	Type B HFT=1	DC fault; Drift & oscillation; individual components do not initialize to reset state [Medium] DC 故障；漂移和振荡； 单个器件未初始化到复位状态[中]	Yes 是	Abnormal operation of PM due to the fault of reset circuitry can be detected by other PMs. Periodic software readback of reset related configuration registers. 复位电路故障导致的 PM 运行异常可被其他 PM 检测到； 周期读取复位相关寄存器状态并检查	< 24h DC is medium DC 为中	The same as in normal operation, and software check of info of last reset after power-on. 同正常运行时，且在上电后读取上次复位信息并检查	Alarm and adopt “first error restart” mechanism 故障报警，并使用“首发错误重启”机制	Temporal and logical program sequence monitoring is used for diagnostic related programs. 对实现诊断功能的 CPU 软件做基于逻辑和时间的程序流检测
Program	Not relevant	Systematic failure	Yes	External watchdog (in FPGA)	Continuous	The same as in	Alarm and	Temporal and logical

sequence 程序顺序	不相关	系统性失效	是	with separate time base (Clock of FPGA) and time window. Checked by set program sequence monitoring varibles in the program. 带时间窗和独立时基（FPGA 诊断时钟）的外部看门狗（FPGA 中）； 程序中设置顺序检测变量进行记录并检查	连续 DC is medium DC 为中	normal operation 同正常运行时	adopt “first error restart” mechanism 故障报警，并使用“首发错误重启”机制	program sequence monitoring is used for diagnostic related programs. Redundant status pulse added from CPU to watchdog to indicate whether CPU is properly reset. Self-diagnostics of watchdog logic inside FPGA. 对实现诊断功能的 CPU 软件做基于逻辑和时间的程序流检测； CPU 到看门狗增加冗余状态脉冲指示是否被复位； FPGA 内的看门狗逻辑自诊断
ECC ECC 功能	Type B HFT=1	DC fault [Medium] DC 故障[中]	Yes 是	Test by forcing ECC errors on memory bus writes (CPU built-in) 在存储器总线写入时制造故障并测试 ECC 功能（CPU 自带）	< 24h DC is medium DC 为中	The same as in normal operation 同正常运行时	Alarm and adopt “first error restart” mechanism 故障报警，并使用“首发错	Temporal and logical program sequence monitoring is used for diagnostic related programs. 对实现诊断功能的

							误重启”机制	CPU 软件做基于逻辑和时间的程序流检测
Exception handling 异常处理	Type B HFT=1	DC fault [Medium] DC 故障[中]	No 否	Check of CPU exception handling by test patterns resulting in exception 制造条件触发异常处理并检查	< 24h DC is medium DC 为中	The same as in normal operation 同正常运行时	Alarm 故障报警	Not required 无，不需考虑
MMU DMA				Not checked because not used 未使用，不诊断				
Bus arbitration 总线仲裁	Type B HFT=1	No, continuous or wrong arbitration [Medium] 无仲裁、Continuous 连续仲裁或错误仲裁[中]	Yes 是	Checked by set program sequence monitoring varibles in the program. Other diagnostics regarding functions related to bus arbitration. 程序中设置顺序检测变量进行记录并检查； 还可在其他与其功能相关的诊断时同时诊断	< 24h DC is medium DC 为中	The same as in normal operation 同正常运行时	Alarm and adopt “first error restart” mechanism 故障报警，并使用“首发错误重启”机制	Temporal and logical program sequence monitoring is used for diagnostic related programs. 对实现诊断功能的 CPU 软件做基于逻辑和时间的程序流检测

2.5.2 Variable memory 可变存储器

SWSC_SafR_SecR_C_041

Diagnostic measures for variable memories are listed in Table 2-3.

PM 的可变存储器的诊断方法列在表 2-3 中。

Table 2-3 Diagnostic measures for variable memories in PM

表 2-3 PM 可变存储器诊断措施列表

Variable memory 可变存储器	**Complexity/ HFT 复杂度/HFT**	**Fault considered [DC] 考虑的故障[DC]**	**Safety critical? 是否安全相关**	**Diagnostics (normal operation) 诊断方法（正常运行）**	**Diag. interval/ DC 诊断间隔/诊断覆盖率**	**Diagnostics (power-on) 诊断方法（上电）**	**Action after detection of failure 故障处理措施**	**Detection and report of "failure of a diagnostic to execute" 对诊断措施未执行的检测和上报措施**
DDR dynamic data DDR 数据区（非全局和静态数据）	Type B HFT=1	DC fault (data & address) [Medium] DC 故障(数据和地址）[中]	Yes 是	The data area is divided into three parts, one part will be used and the other two will be tested with March SS, and the three parts rotation will be completed in the diagnostic test interval. March SS of address lines in unused memory space. DDR data ECC. Periodic scrubbing of DDR contents. 将数据区分为三片，每次使用其中一片，对另外两片进行 March SS，在诊断间隔内完成三片轮换。 在未使用的存储空间内，对地址线进行 March SS； DDR 数据 ECC； 周期刷新 DDR 内容	Continuous for ECC. < 24h for other measures 对 ECC 为连续； 对其他措施为< 24h DC is medium DC 为中	The same as in normal operation 同正常运行时	Alarm and adopt "first error restart" mechanism 故障报警，并使用"首发错误重启"机制	Temporal and logical program sequence monitoring is used for diagnostic related programs. Test by forcing ECC errors on memory bus writes (CPU built-in) 对实现诊断功能的 CPU 软件做基于逻辑和时间的程序流检测； 在存储器总线写入时制造故障并测试 ECC 功能（CPU 自带）
		Soft error [Medium] 软失效[中]	Yes 是	DDR data ECC. Correctable ECC profiling. Data and ECC stored in multiple physical DDR chips. DDR 数据 ECC；	Continuous 连续 DC is medium DC 为中	The same as in normal operation 同正常运行时	Alarm and adopt "first error restart" mechanism 故障报警，并使	Test by forcing ECC errors on memory bus writes (CPU built-in) 在存储器总线写入时制造故障并测试 ECC 功

				可纠错 ECC 计数； ECC 和受保护的数据存储在不同物理 DDR 芯片中			用“首发错误重启”机制	能（CPU 自带）
DDR static and global data, PM firmware code DDR 数据区（CPU 运行代码、全局和静态数据）	Type B HFT=1	DC fault (data & address) [Medium] DC 故障(数据和地址）[中]	Yes 是	Protected by CRC-32. DDR data ECC. 计算 CRC-32 并检查； DDR 数据 ECC；	Continuous for ECC. < 24h for other measures 对 ECC 为连续； 对其他措施为< 24h DC is high DC 为高	The same as in normal operation 同正常运行时	Alarm and adopt “first error restart” mechanism 故障报警，并使用“首发错误重启”机制	Test by forcing ECC errors on memory bus writes (CPU built-in). CPU uses the same CRC polynomial in calculation as the one used to protect invariable memory contents 在存储器总线写入时制造故障并测试 ECC 功能（CPU 自带）； CPU 嵌入式软件使用相同多项式计算 CRC 并与存储的数据 CRC 进行比较
		Soft error [Medium] 软失效[中]	Yes 是	DDR data ECC DDR 数据 ECC	Continuous 连续 DC is medium DC 为中	The same as in normal operation 同正常运行时	Alarm and adopt “first error restart” mechanism 故障报警，并使用“首发错误重启”机制	Test by forcing ECC errors on memory bus writes (CPU built-in). 在存储器总线写入时制造故障并测试 ECC 功能（CPU 自带）
SRAM			Yes 是	The retention data was protected by CRC-32. 掉电保护数据计算 CRC-32 并检查。	Not relevant 不相关 DC is high	CRC-32 is calculated and checked for	Alarm and adopt “first error restart”	CPU uses the same CRC polynomial in calculation as the one

					DC 为高	retention data 对掉电保护数据计算 CRC-32 并检查	mechanism 故障报警，并使用“首发错误重启”机制	used to protect invariable memory contents CPU 嵌入式软件使用相同多项式计算 CRC 并与存储的数据 CRC 进行比较

2.5.3 Invariable memory 不可变存储器

SWSC_SafR_NSecR_A_042

Diagnostic measures for invariable memories are listed in Table 2-4.

PM 的不可变存储器的诊断方法列在表 2-4 中，。

Table 2-4 Diagnostic measures for invariable memories in PM

表 2-4 PM 不可变存储器诊断措施列表

Invariable memory 不可变存储器	**Complexity/ HFT 复杂度/HFT**	**Fault considered [DC] 考虑的故障 [DC]**	**Safety critical? 是否安全相关**	**Diagnostics (normal operation) 诊断方法（正常运行）**	**Diag. interval/ DC 诊断间隔/诊断覆盖率**	**Diagnostics (power-on) 诊断方法（上电）**	**Action after detection of failure 故障处理措施**	**Detection and report of “failure of a diagnostic to execute” 对诊断措施未执行的检测和上报措施**
Nor FLASH for PM firmware code and FPGA configuration information Nor FLASH（存储 CPU 代码、FPGA 配	Type B HFT=1	DC fault (data & address) [Medium] DC 故障（数据和地址）[中]	Yes 是	Not checked because CPU firmware code is running in DDR, and FPGA configuration information is not relevant during run time.	Not relevant 不相关 DC is high DC 为高	CRC-32 is calculated and checked for CPU firmware code and FPGA configuration information 对 CPU 代码、FPGA 配	Alarm and adopt “first error restart” mechanism 故障报警，并使用“首发错误重启”机制	CPU uses the same CRC polynomial in calculation as the one used to protect invariable memory contents

置信息）				CPU 代码运行在 DDR 中，且 FPGA 运行时与配置信息无关，因此不诊断		置信息计算 CRC-32 并检查		CPU 嵌入式软件使用相同多项式计算 CRC 并与存储的数据 CRC 进行比较
SPI FLASH for project SPI FLASH（存储工程）	Type B HFT=1	DC fault (data & address) [Medium] DC 故障（数据和地址）[中]	Yes 是	CRC-32 is calculated and checked after each download and online download 每次全下装或在线下装后对工程计算 CRC-32 并检查	Not relevant 不相关 DC is high DC 为高	CRC-32 is calculated and checked for project 对工程计算 CRC-32 并检查	Alarm and synchronization of project from other PMs if failure occurs during download. Alarm and run the original project continuously if failure occurs during online download 全下装时故障，故障报警，并从其他 PM 同步工程； 在线下装时故障，故障报警，系统正常运行原工程	CPU uses the same CRC polynomial in calculation as the one used to protect invariable memory contents CPU 嵌入式软件使用相同多项式计算 CRC 并与存储的数据 CRC 进行比较

2.5.4 First error restart 故障重启

SWSC_SafR_NSecR_B_059

After an error restart, if an error is detected in the power on diagnose, the CPU will keep in reset state; if no error is detected, the CPU will enter into the normal CPU cycle. This feature can be set by user in the configuration software, and if this feature is not configured, PM is not allowed to restart but keep in reset state.

故障重启后，如果在上电自检时发现故障则保持复位，不再重启；如果未发现故障则进入正常运行周期。该功能可由用户在组态软件中配置，如

果未配置，则故障后直接保持复位，不重启。

2.6 PM degradation mode PM 降级模式

SWSC_SafR_NSecR_B_043

The PM supports degradation mode of 3-2-1-0, 2-1-0, as shown in follow:

PM 降级模式为 3-2-1-0，2-1-0，如下图所示。

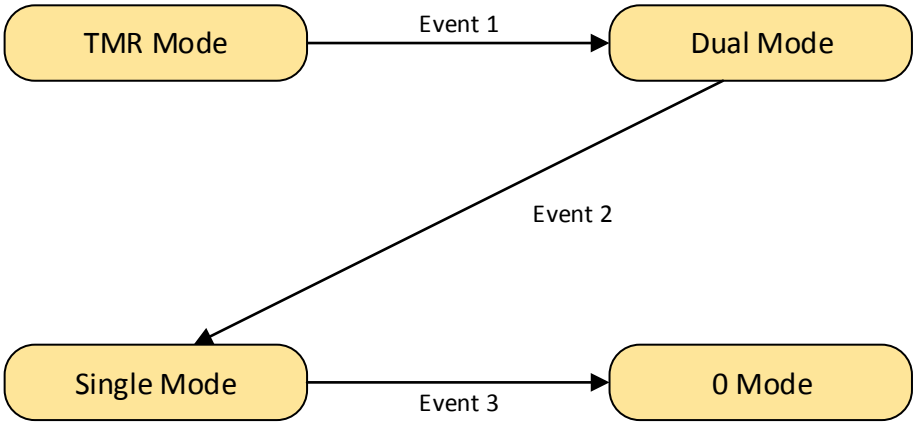

Figure 2-14 PM degradation mode

图 2-14 PM 降级模式示意图

Detailed description of the states as follows:

图中状态及事件具体描述如下：

- TMR Mode: Three channels work normally.
- Dual Mode: Only two channels work normally. When a task is configured as “Control” property, the task can be configured as 1oo2 or 2oo2 voting. When a task is configured as “Safety” property, only 1oo2 voting can be configured. The property can be set in the configuration software for each task.
- Single Mode: Only one channel works normally. When the operation time exceeded the MRT used in PFH/PFD calculation for SIL3, the calculation results are not valid anymore.
- Event 1: One PM has a fault, the system occurs 3-2 degradation.
- Event 2: One of the remaining PMs has a fault, therefore the system occurs 2-1 degradation.
- Event 3: The last PM has a fault.
- TMR Mode：三系正常运行。
- Dual Mode：两系正常运行。用户配置成 control 应用时，可选择按照 1oo2 或者 2oo2 方式表决；配置成 safety 应用时，只能按照 1oo2 方式表决。control 应用、safety 应用的选择在组态软件中配置，可基于每个任务配置。
- Single Mode：单系运行。Single Mode 下，运行时间超过用于计算 SIL3 PFH/PFD 使

用的 MRT 时，计算结果不再有效。

- Event 1：一系 PM 出现故障，发生 3-2 降级。
- Event 2：一系 PM 出现故障后，又有一系 PM 出现故障，发生 2-1 降级。
- Event 3：单系 PM 运行，剩余该系 PM 出现故障。

2.7 COTS component 商用软件

SWSC_SafR_NSecR_A_044

No.

无。

2.8 Reused component 复用部分

SWSC_SafR_NSecR_A_045

No.

无。

3 Software function 软件具体功能

3.1 Control loop 控制回路

SWSC_SafR_NSecR_B_046

The flow diagram of PM_FW is shown in follows.

PM_FW 流程图如下图所示。

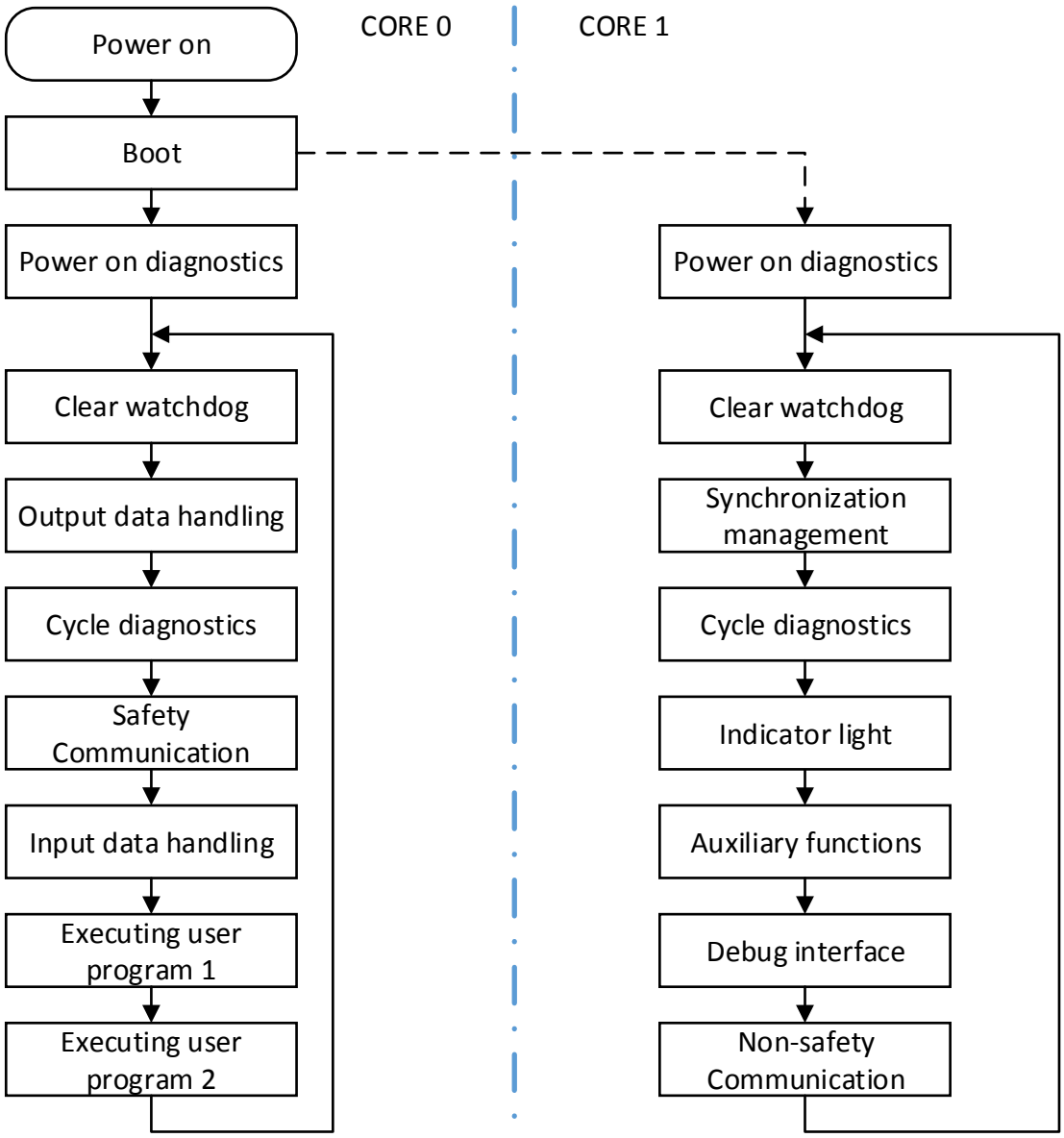

Figure 3-5 PM_FW flow diagram

图 3-5 PM_FW 流程图

The control loop relevant to PM_FW includes the following steps, as shown in follows:

控制回路和 PM_FW 相关部分主要包括以下几个步骤，如下图所示：

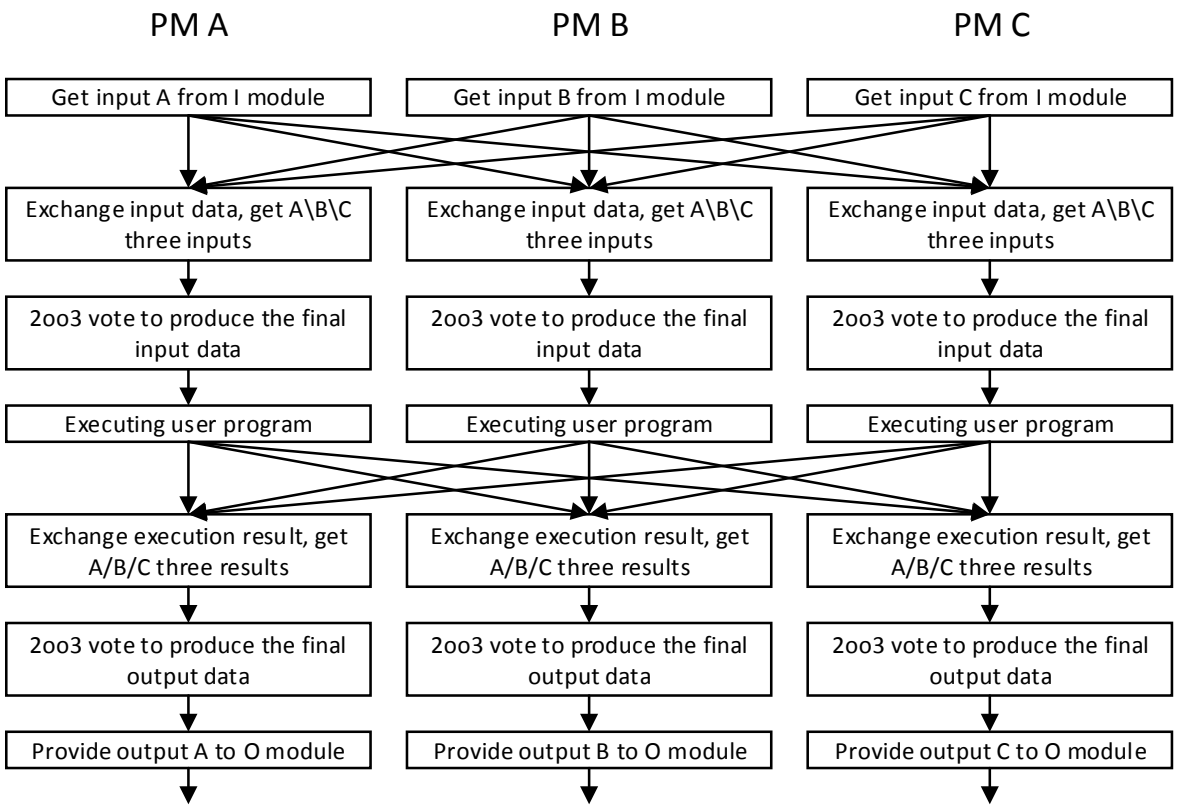

Figure 3-1 Control loop in PM

图 3-1 PM 控制回路示意图

The control loop is not relevant to CM_FW and CM_OS.

控制回路和 CM_FW 和 CM_OS 不相关。

For the executing user program, the enable of 'Divided-by-zero error protection, array bounds exceeded error protection and exception handling' can be selected by user. This property can be configured via configuration software for each user program. The property must be configured to enabled, if user selects the safety application mode; the property can be configured to enabled or disabled, if user selects the control application mode. If the user chooses to enable 'Divided-by-zero error protection, array bounds exceeded error protection and exception handling', when an exception occurs, the current statement will be skipped, and a function block can report this error.

对于执行用户程序，用户可选择是否开启"除零和数组越界的错误保护及异常处理"，该属性由使用者通过组态软件基于每个任务配置。用户选择 safety 应用时，该属性只能配置为开启；用户选择 control 应用时，都可以配置。如果用户选择开启"除零和数组越界的错误保护及异常处理"，当有错误发生时，跳过当前语句继续执行，并可通过功能块报出此错误。

3.2 Data retention 数据掉电保持

SWSRS_SafR_NSecR_A_060

The variables that need to be retained can be defined by the user in configuration software. The embedded software stores these variables in the SRAM after each control cycle. After power on, if the key switch is not in the 'Init' position, the embedded software copies these variables from SRAM to the data area in DDR.

期望掉电保持的变量由使用者通过组态软件指定，嵌入式软件在每个控制周期后将这些数据保存在 SRAM 上。再次上电后，如果开关不在 init 档位，这些变量会从 SRAM 恢复到内存上。

3.3 Voting mechanism 表决机制

SWSC_SafR_NSecR_A_047

The voting mechanism is shown in the following table:

表决机制如下表所示：

Table 3-1 voting mechanism

表 3-1 表决机制

	Quality Channel A	Quality Channel B	Quality Channel C	Voting Configuration	Voting Result
DI	Normal	Normal	Normal	—	Result of 2oo3
	Normal	Normal	Bad	2oo2	Result of 2oo2
				1oo2	Result of 1oo2
	Normal	Bad	Bad	—	Channel A's value
	Bad	Bad	Bad	—	Value set by user
DO	Normal	Normal	Normal	—	Result of 2oo3
	Normal	Normal	Bad	2oo2	Result of 2oo2
				1oo2	Result of 1oo2
	Normal	Bad	Bad	—	Channel A's value
	Bad	Bad	Bad	—	Safety value
AI	Normal	Normal	Normal	—	Median
	Normal	Normal	Bad	—	Mean
	Normal	Bad	Bad	—	Channel A's value
	Bad	Bad	Bad	—	Value set by user
AO	Normal	Normal	Normal	—	Median
	Normal	Normal	Bad	—	Mean
	Normal	Bad	Bad	—	Channel A's value
	Bad	Bad	Bad	—	Safety value
PI	Normal	Normal	Normal	—	Median

	Normal	Normal	Bad	—	Maximum
	Normal	Bad	Bad	—	Channel A's value
	Bad	Bad	Bad	—	Value set by user

- The quality of input channel is Normal only when the quality of data, the quality of IP_BUS and the quality of PM_BUS are all Normal
- The quality of output channel is Normal only when quality of data and the quality of PM_BUS are both Normal
- If an analog data is out of the tolerance, the quality is bad.
- When a task is configured as “Control” property, the task can be configured as 1oo2 or 2oo2 voting. When a task is configured as “Safety” property, only 1oo2 voting can be configured.
- 对于输入数据来说，某系数据的质量取决于数据本身的质量、IP_BUS 的质量和 PM_BUS 的质量。如果这三个质量有一个为坏，则该系质量为坏，即该系输入数据无效。
- 对于输出数据来说，数据质量取决于数据本身的质量和 PM_BUS 的质量。如果这两个质量有一个为坏，则该系质量为坏，即该系输出数据无效。
- 对于模拟量输入来说，如果其中某一系的值超过偏差允许的范围，则该系质量为坏，即该系输入数据无效。
- 对于数字量数据来说，在 control 方式下，用户可配置两系质量好时按照 1oo2 或 2oo2 表决；在 safety 运行方式下，两系质量好时只能按照 1oo2 表决。

3.4 Data monitoring 数据监视

SWSC_NSafR_NSecR_A_048

The data monitoring function refers to PC software (OPC software, HMI software and configuration software) monitor run-time data of PM. All the PMs sent the run-time data to CM cyclically, and CM handles the read variable request from the PC software and sends response with run-time data.

数据监视主要指上位机软件（OPC Server、HMI 软件和组态软件）监视 PM 的实时数据。PM 周期主动将实时数据发送给 CM，CM 接受上位机软件的请求，按照不同的要求进行应答。

Therefore, the request from PC software is directly handled by the CM, and PM is not affected.

因此，数据监视功能和 PM 无直接关系，不会对 PM 的运行造成影响。

3.5 Online operation 在线操作

SWSC_NSafR_NSecR_A_049

Online operation function refers to that the user sends the debug command to the PM through the

configuration software. The debug command includes STOP, RUN, PAUSE, Single step, Set variable, Disable/Enable variable, etc. This function only can be used in Program state. The diagram is shown in Figure 3-2:

在线操作主要指用户通过组态软件下发写调试命令给 PM，主要包括停止命令、运行命令、暂停命令、单步命令、写变量命令、使能/禁止命令。在线操作只有在调试状态下才能运行。这些在线操作命令的流程如下图所示：

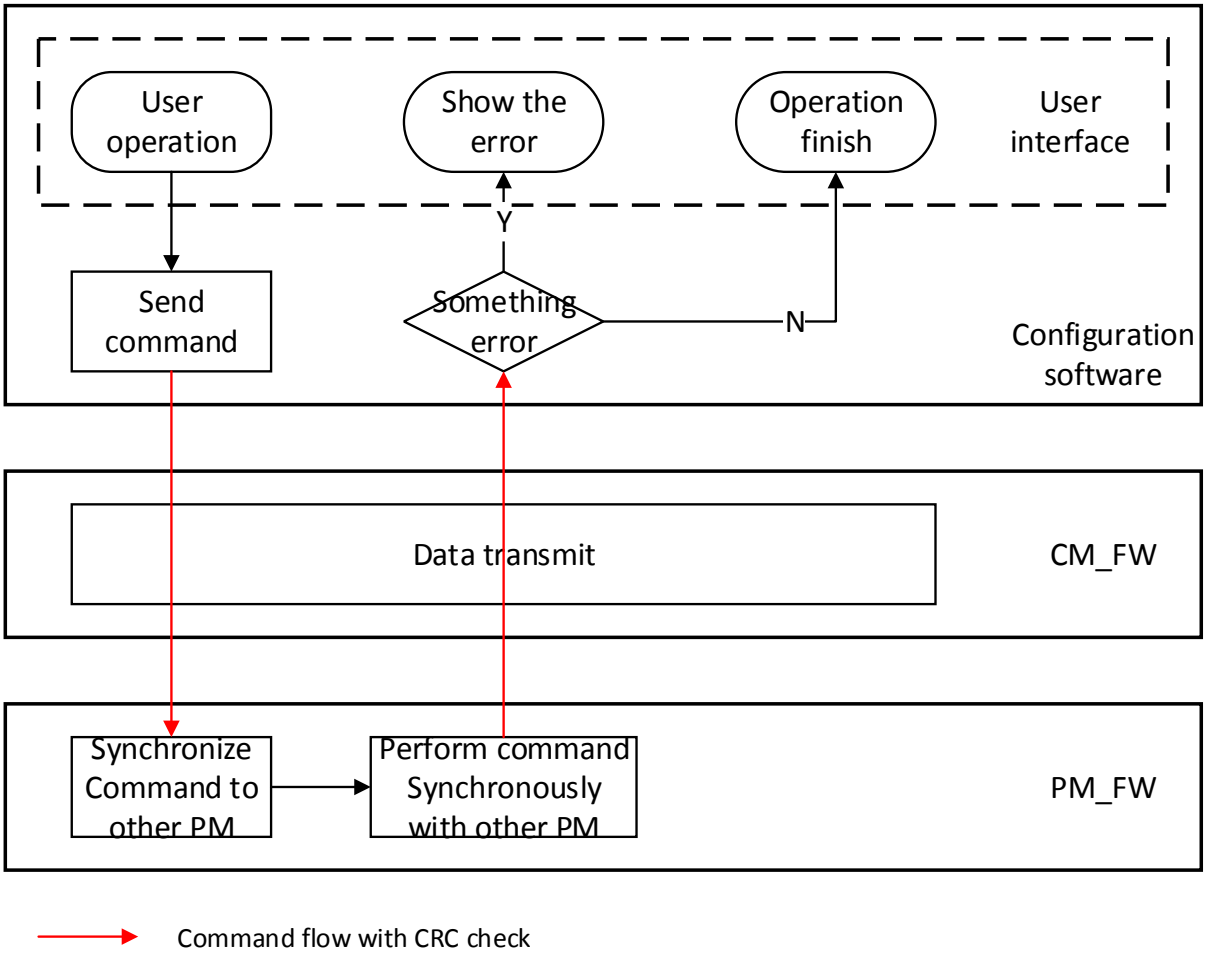

Figure 3-2 Diagram of online operation

图 3-2 在线操作示意图

3.6 Download 下装

3.6.1 Initialization download 初始化下装

SWSC_NSafR_NSecR_B_050

There are two types of download: initialization download and online download. This function only can be allowed in debug stop state or standby state. After the initialization download, all the variables will be initialized, and control station will use the new project. The diagram is shown in Figure 3-3:

下装分为初始化下装和在线下装。初始化下装只能在 debug stop state 或者 standby state 下进行，下装后，控制站中的用户程序从初始状态运行。初始化下装的流程如下图所示：

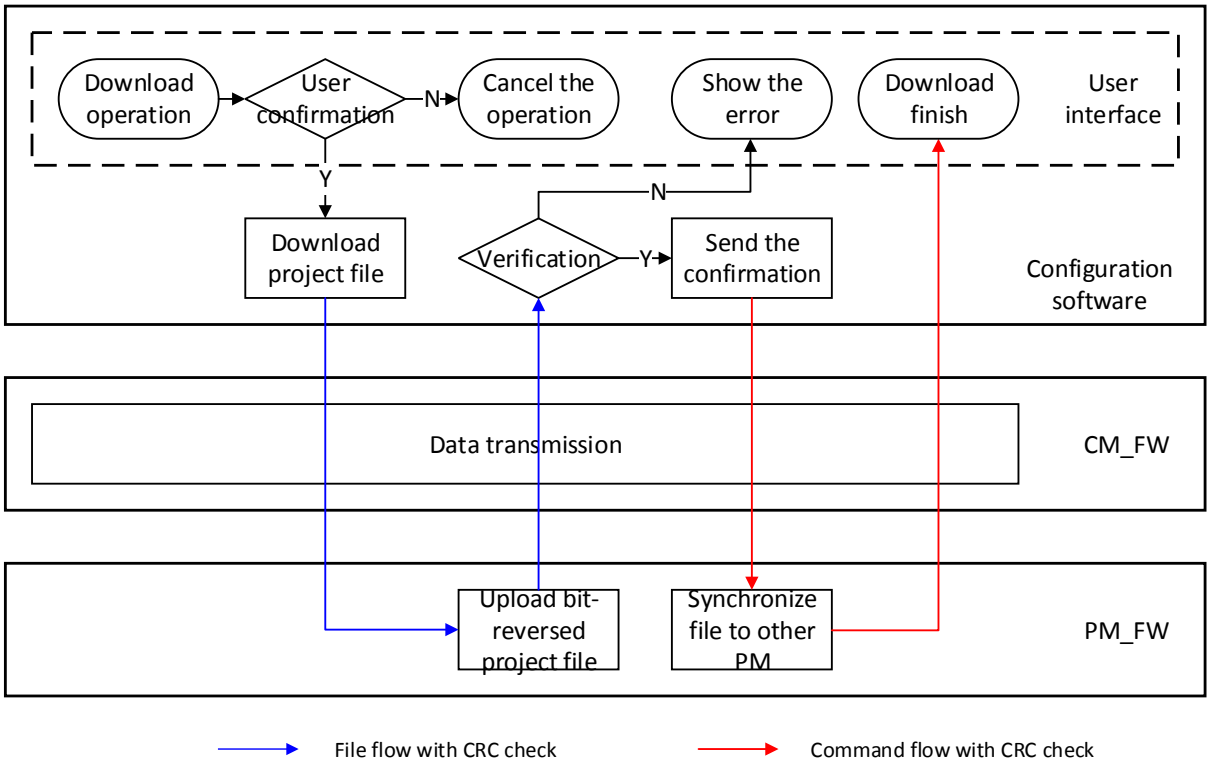

Figure 3-3 Diagram of initialization download

图 3-3 初始化下装示意图

3.6.2 Online download 在线下装

SWSC_NSafR_NSecR_B_051

The online download function only can be allowed in debug run state or pause state. During the online download process, the control station still used the old project until the completion of the online download. After the online download, the changed variables or new variables will be initialized, and the remaining variables will remain unchanged. The diagram is shown in Figure 3-4:

当 PM 处于 debug run state 或者 pause state 时，允许组态软件进行在线下装。在线下装时，控制站一直运行上次下装的用户程序，直到在线下装完成。在线下装后，新增变量或者修改的变量会被初始化，其余变量值保持不变。在线下装的流程如下图所示：

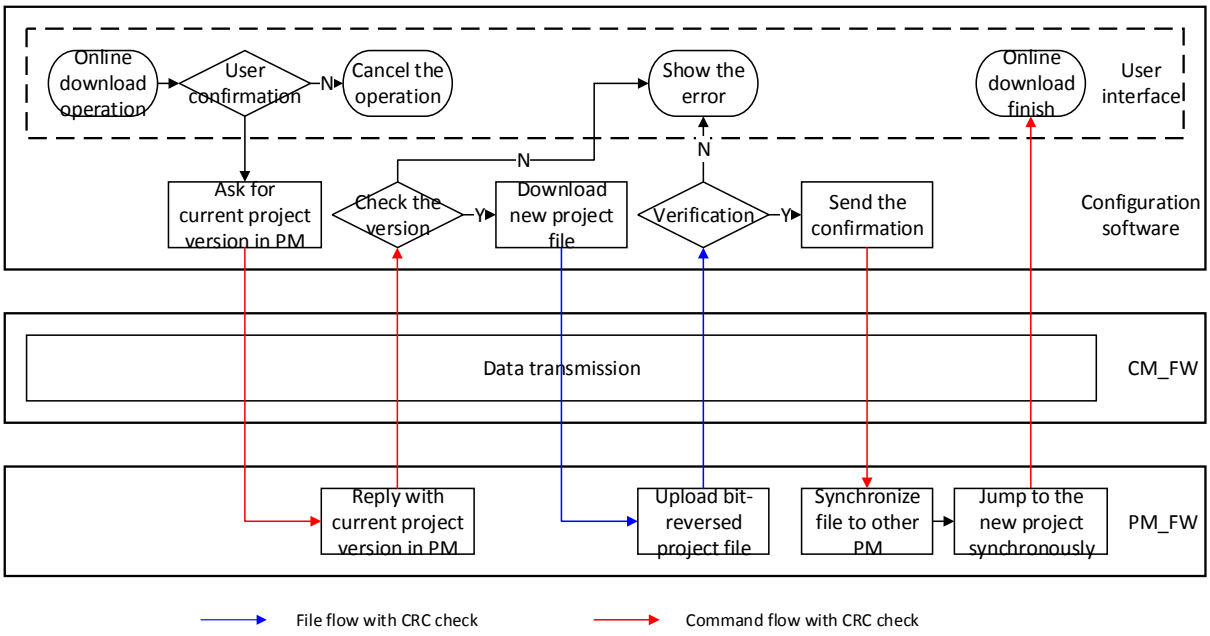

Figure 3-4 Diagram of online download

图 3-4 在线下装示意图

3.7 Running information record 运行信息记录

3.7.1 SOE

SWSC_NSafR_NSecR_B_052

SOE function is realized by DI module, AI module, OSP module, PM, CM and configuration software. Each PM stores SOE records and provides the records to the SOE software respectively.

系统的 SOE 功能由 DI 模块、AI 模块、OSP 模块、PM、CM、组态软件共同完成，三系 PM 各自存储 SOE，并能分别将 SOE 记录提供给上位机 SOE 软件。

The sources of SOE records are shown as follows:

SOE 记录的来源如下：

- DI module, which is hard SOE. DI module records status change of input signal. The SOE accuracy resolution is 1ms if the modules belong to one control station, and it is 2ms if the modules belong to different stations.
- DI 模块，该类型属于硬 SOE。DI 模块记录输入开关量信号的状态变化，控制站内 DI 的 SOE 精度优于分辨率为 1ms，控制站间 DI 的 SOE 精度优于分辨率为 2ms。
- AI module, which is hard SOE. AI module generates a SOE record if the point value exceeds the threshold values. Up to four threshold values can be set by configuration software. The SOE resolution of AI is 2ms if the modules belong to one control station, and it is 4ms if the modules belong to different stations.

- AI 模块，该类型属于硬 SOE。AI 模块在通道采集值超过阈值门限时进行 SOE 记录，通道阈值可组态配置，最大支持 4 个通道阈值。AI 模块 SOE 分辨率站内为 2ms，站间为 4ms
- OSP module, which is hard SOE. OSP module generates SOE records when PI signal reaches trip threshold and transition in DI signals.
- OSP 模块，该类型属于硬 SOE。OSP 模块在 PI 信号达到 trip 阈值时、以及 DI 信号发生跳变时记录 SOE。
- Internal BOOL variable, which is soft SOE. PM monitors the status change of the special variables that are labeled as 'SOE variable' by configuration software. The accuracy of soft SOE is one control cycle.
- 内部 BOOL 类型变量，该类型属于软 SOE。PM 监视组态为 SOE 点的 BOOL 类型变量的状态变化，精度要求为一个控制周期。BOOL 类型变量是否为 SOE 点由工程人员在组态软件上组态完成。

The SOE record is rolling recorded, and the maximum number is ~~60000~~120000. The latest ~~5000~~20000 records can be maintained after power-off.

SOE 记录总数为 ~~6~~12 万条，其中，掉电保持的 SOE 条数为 ~~5000~~20000 条。

SOE records can be grouped by configuration software, and each group can be set individually for the capacity, recording method and whether need to be maintained after power-off. Hard SOE and soft SOE cannot be in one group. The maximum number of soft SOE groups is 16, and the number of hard SOE groups is 1.

组态软件可以对 SOE 记录的来源进行分组，并设置每组的记录容量、记录方式及是否掉电保护，但硬 SOE 和软 SOE 不能设置在一个组内。最多支持 16 组软 SOE，硬 SOE 单独一组。

3.7.2 Control station log 日志

SWSC_NSafR_SecR_B_053

~~PM and CM can save 10000 latest log records respectively, the latest 1000 records have power loss retain function.~~

~~PM、CM 保存各自最近的 10000 条日志记录，其中各自最近的 1000 条日志具有掉电保持功能。~~

PM can save the lateset 30000 log records. CM can save the lateset 10000 log records. The records have power loss retain function.

PM 保存最近的 30000 条日志记录，CM 保存最近的 10000 条日志记录。日志具有掉电保持功能。

The log records contain power on event, fault event, configuration download and debug event.

日志记录内容包括：上电事件、故障事件、组态下装及调试事件。

The diagnostic software can read all the log records from PM and CM.

诊断软件能够从 PM 和 CM 读取所有的日志记录。

3.7.3 Status monitoring 状态监视

SWSC_SafR_NSecR_A_054

The status, which is monitored and recorded by PM, includes PM status, Safety Net status, IP_BUS status, IO module status, PM temperature, CM_BUS status.

The status, which is monitored and recorded by CM, includes CM status, CM memory usage, CM CPU load, CM temperature, System Net status, Modbus communication status.

All the CMs send the status data to the PM cyclically. PM handles the request of the diagnostic software, and send a response to it with status data. The system supports the function that the user can use the diagnostic software to clear the IO module diagnostic information in Program state.

PM 需要记录的状态数据包括 PM 状态、Safety Net 状态、IP_BUS 状态、IO 模块状态、PM 温度、CM_BUS 状态。

CM 需要记录的状态数据包括 CM 状态、CM 内存使用率、CM 的 CPU 负荷、CM 温度、System Net 状态、Modbus 通讯状态

CM 周期主动将状态数据发送给 PM，PM 响应诊断软件的请求，按照不同的要求进行应答。系统支持用户在调试模式下通过诊断软件清除 IO 模块故障信息。

4 Safety communication protocol 安全通讯协议

4.1 PM_BUS

SWSC_SafR_SecR_B_055

PM_BUS is used for data exchange between PMs. The embedded software is responsible for handling safety layer, and the communication link between PMs is the black channel.

PM_BUS 用于三系 PM 间交换数据，PM 中的嵌入式软件负责处理安全层数据，PM 之间的通信链路为安全通信对应的黑通道。

Network topology is shown in Figure 4-1:

网络拓扑如图 4-1 所示：

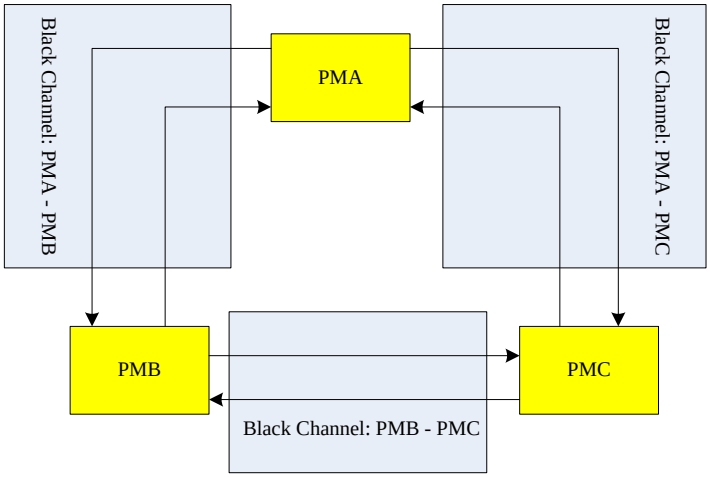

Figure 4-1 Communication topology of PM_BUS

图 4-1 PM_BUS 网络拓扑结构示意图

4.1.1 Safety layer function 安全层功能

The measures including Sequence number, Time expectation - Watchdog, Connection authentication, Data integrity assurance - CRC are implemented to avoid communication errors.

使用序列号、时间预期、连接验证、CRC 防御通讯威胁。

The fault control matrix is shown in the table 4-1:

安全层提供的保护如表 4-1 所示：

Table 4-1 Fault Control Matrix

表 4-1 威胁/防御矩阵

Communication failure 通信错误	Safety measure 安全措施			
	Sequence number 序号	Watchdog 看门狗	CRC	Connection authentication 连接验证
Data Corruption 数据损坏			X	
Repetition 重复	X			
Incorrect sequence 不正确的序列	X			
Loss 丢失	X			
Unacceptable delay 不可接受的延迟		X		
Insertion 插入	X			X
Masquerade				X

伪装				
Addressing 寻址异常				X

4.1.2 Protocol message structure 协议消息结构

Table 4-2 Frame structure

表 4-2 帧结构

Header	Safety relevant data	CRC-32-0	Non-safety relevant data
14 bytes	variable	4 bytes	variable

Table 4-3 Header structure

表 4-3 头结构

	Data Type	Length	Value	Description
Total Length	unsigned int	4 bytes		Total length including Header. 数据帧总长度，包括帧头
SrcAddr	unsigned char	1 byte	0-2	ID of source PM: 0->PMA; 1->PMB; 2->PMC 源 PM 编号：0->PMA；1->PMB；2->PMC
DstAddr	unsigned char	1 byte	0-2	ID of destination PM: 0->PMA; 1->PMB; 2->PMC 目的 PM 编号：0->PMA；1->PMB；2->PMC
Sequence Number	unsigned short	2 bytes		Increment after each send. 每发送一次，数值增加 1
Block Number	unsigned short	2 bytes	n	Number of safety relevant data blocks. 安全相关数据中数据块的个数
Safety Length	unsigned int	4 bytes		Number of safety relevant data bytes. 安全相关数据的长度（字节）

4.2 IP_BUS

SWSC_SafR_SecR_C_056

IP_BUS is used for data exchange between PM and IO module. The embedded software and the firmware in IO module are responsible for handling safety layer, and the communication link between them is the black channel.

IP_BUS 用于 PM 和 IO 模块之间交换数据，PM 中的嵌入式软件和 IO 模块固件负责处理安全层数据，两者之间的通信链路为安全通信对应的黑通道。

Network topology is shown in Figure 4-2:

网络拓扑如图 4-2 所示：

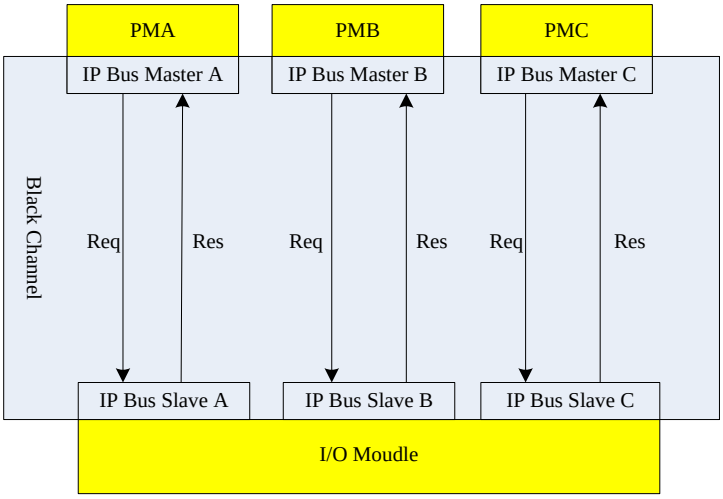

Figure 4-2 Communication topology of IP_BUS

图 4-2 IP_BUS 网络拓扑结构示意图

4.2.1 Safety layer function 安全层功能

The measures including Sequence number, Time expectation - Watchdog, Connection authentication, Data integrity assurance – CRC, Feedback message are implemented to avoid communication errors.

使用序列号、时间预期、连接验证、CRC、应答包等技术防御通讯威胁。

The fault control matrix is shown in the table 4-4:

安全层提供的保护如表 4-4 所示：

Table 4-4 Fault Control Matrix

表 4-4 威胁/防御矩阵

Communication failure 通信错误	Safety measure 安全措施				
	Sequence number 序号	Watchdog 看门狗	CRC	Feedback message 应答包	Connection authentication 连接验证
Data Corruption 数据损坏			X		
Repetition 重复	X				
Incorrect sequence 不正确的序列	X				
Loss 丢失	X			X	
Unacceptable delay 不可接受的延迟		X		X	

Insertion 插入	X			X	X
Masquerade 伪装					X
Addressing 寻址异常					X

4.2.2 Protocol message structure 协议消息结构

Table 4-5 Frame structure

表 4-5 帧结构

~~Header 1~~	~~Header 2~~	~~Safety IO data 1~~	~~Safety IO data 2~~	~~CRC 1~~	~~CRC 2~~
~~8 bytes~~	~~8 bytes~~	~~variable~~	~~variable~~	~~4 bytes~~	~~4 bytes~~

Header 1	Safety IO data 1	CRC 1	Header 2	Safety IO data 2	CRC 2
8 bytes	variable	4 bytes	8 bytes	variable	4 bytes

As show in Table 4-5, ‘Header 2’ is the bit-reversed data of ‘Header 1’, ‘Safety IO data 2’ is the bit-reversed data of ‘Safety IO data 1’, and ‘CRC 2’ is the bit-reversed data of ‘CRC 1’.

上述结构中，第二份数据是第一份数据的反转。

Table 4-6 Header structure

表 4-6 头结构

	Data Type	Length	Value	Desc
Codename	unsigned int	4 bytes		Unique relationship between master and slave obtained by (PM ID << 16) | Slave address 代表主从唯一的对应关系：PM 号<<16 | 从站地址
Sequence Number	unsigned short	2 bytes		Increment after each REQ in master, and Slave ACK uses the identical number as REQ 主站每发送一次增加 1，从站应答时序号与请求帧一致
Control/Status	unsigned char	1 byte		Control byte / Status byte 控制/状态字节
Frame Length	unsigned char	1 byte		Number of total bytes in frame without Header 此数据帧的总长度（字节），不包括帧头

Table 4-7 Control byte

表 4-7 控制字节

Bit	Value 值	Description 描述
0	Active_FV: Fail-safe values to be activated	Set to '1' when using fail-safe value 使用故障安全值时，置 1：
1	iPar_En: parameter is ready	Set to '1' when master is ready to send slave module parameters 主站准备下发从站模块参数时，置 1
2~7	Reserved	

Table 4-8 Status byte

表 4-8 状态字节

Bit	Value 值	Description 描述
0	Failure exists	Set to '1' when detected faults. 存在失效时，置 1。
1	Communication failure: Codename	Set to '1' when Codename failure. Codename 错误时，置 1。
2	Communication failure: CRC or Sequence Number	Set to '1' when CRC or Sequence number failure. CRC 或序号错误时，置 1。
3	Communication failure: WD-timeout	Set to '1' when Watchdog timeout. 看门狗超时，置 1。
4	Fail-safe values (FV) activated	Set to '1' when slave using FV. 从站使用故障安全值时，置 1。 After IP_BUS interruption, the necessity of the user confirmation for re-connection can be configured in the configuration software. If the user confirmation is necessary, this value remains at 1 before the user confirms. IP_BUS 中断后，使用者通过组态软件配置再次建立连接是否需要用户确认。如配置为需确认，在用户确认前，该值保持为 1.
5	new i-Parameter OK(iPar_OK)	Set to '1' when slave has adopted the new parameter. 从站采用主站下发的新参数后，置 1。
6-7	Reserved	

4.3 Peer to Peer safety communication between control stations 站间安全通讯

SWSC_SafR_SecR_C_057

Safety communication between control stations (Peer-to-Peer) is used for the safety data exchange between control stations. Whole link of Peer-to-Peer includes the following parts: the PM of the source control station, the CM_BUS of the source control station, the CM of the source control station, Safety Net, the CM of the destination control station, the CM_BUS of the destination control station, and the PM of the destination control station. The safety layer protocol of Peer-to-Peer is implemented by PM. The data flow is shown in Figure 4-3:

控制站间安全通讯功能（Peer to Peer）用于多个控制站之间的安全数据通讯，整个链路包括以下几部分：源控制站的 PM、源控制站的 CM_BUS、源控制站的 CM、Safety Net、目的控制站的 CM、目的控制站的 CM_BUS、目的控制站的 PM。PM 实现通讯安全层。数据流如图 4-3 所示：

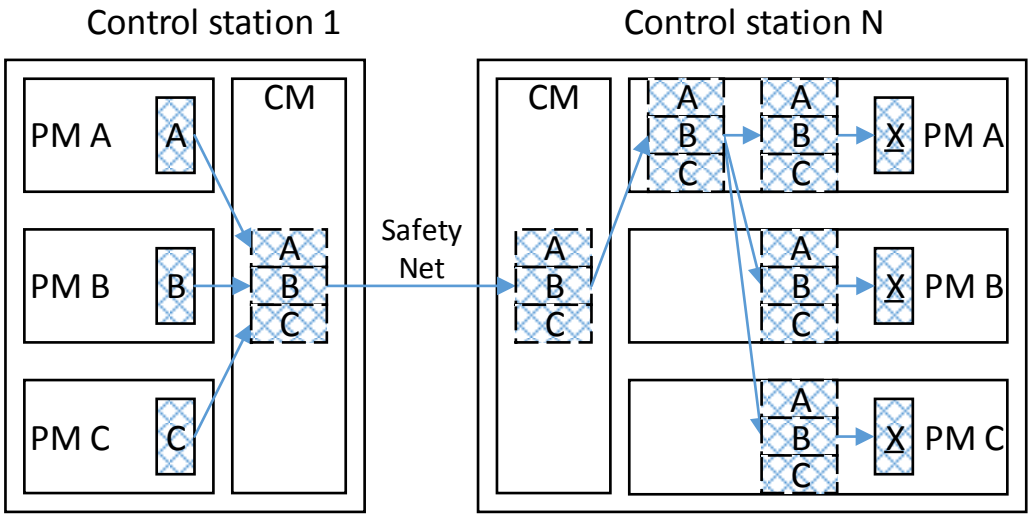

Figure 4-3 Data flow of Peer to Peer safety communication

图 4-3 安全站间通讯数据流示意图

As show in Figure 4-3, the data flow includes the following steps:

如上图所示，整个发送数据流分为以下几步：

- Each PM sends the message to CM. The send period can be configured in the configuration software. When the period is less than the actual interval (the actual interval is the time between send requests and receive the response), the actual interval will replace the set cycle.
- The CM packs the messages of all PMs into one packet, and sends it through the Safety Net.
- The CM in destination control station receives the packet and transmits it to one PM that works normally.
- The PM send the packet to other PMs.
- Each PM handles the safety layer synchronously, and then gets the final results by voting.
- 各个 PM 将数据帧发送给 CM。发送周期可配置，当配置的发送周期小于实际间隔（从数据发送到接收到对方控制器的应答）时，按实际间隔发送数据。
- CM 将本站所有 PM 的安全帧打包，并通过 Safety Net 发送。
- 目的控制站的 CM 收到数据包后，发给其中一个正常工作的 PM。
- 该 PM 处理安全层将数据包同步给其他 PM。
- 三系 PM 同步处理数据包，各自通过表决得到最后结果。

4.3.1 Safety layer function 安全层功能

The measures including Sequence number, Time expectation - Watchdog, Connection authentication, Data integrity assurance – CRC, Feedback message are implemented to avoid communication errors.

使用序列号、时间预期、连接验证、CRC、应答包等技术防御通讯威胁。

The fault control matrix is shown in the table 4-9:

安全层提供的保护如表 4-9 所示：

Table 4-9 Fault Control Matrix

表 4-9 威胁/防御矩阵

Communication failure 通信错误	Safety measure 安全措施				
	Sequence number 序号	Watchdog 看门狗	CRC	Feedback message 应答包	Connection authentication 连接验证
Data Corruption 数据损坏			X		
Repetition 重复	X				
Incorrect sequence 不正确的序列	X				
Loss 丢失	X			X	
Unacceptable delay 不可接受的延迟		X		X	
Insertion 插入	X			X	X
Masquerade 伪装					X
Addressing 寻址异常					X

4.3.2 Protocol message structure 协议消息结构

Table 4-10 Frame structure in CM

表 4-10 CM 帧结构

Additional Info	PMA Safety Frame	PMB Safety Frame	PMC Safety Frame	FCS
4 bytes	variable	variable	variable	4 bytes

Table 4-11 Additional Info structure

表 4-11 附加信息结构

	Data Type	Length	Desc
Total Length	unsigned short	2 bytes	Number of bytes in data frame with Additional Info 打包后的数据帧的总长度（字节），包括附加信息
PM Info.	unsigned char	1 byte	Bit 0->PMA; Bit 1->PM B; Bit 2->PM C. Set corresponding bit to '1' when the data frame contains the safety frame from corresponding PM. Bit 0->PMA；Bit 1->PMB；Bit 2->PMC，当此数据帧包含相应 PM 的安全帧时，相应的位置 1。
Reserved	unsigned char	1 byte	

Table 4-12 REQ safety frame structure of one PM

表 4-12 单个 PM 请求帧结构

~~Header 1~~	~~Header 2~~	~~Safety data 1~~	~~Safety data 2~~	~~CRC 1~~	~~CRC 2~~
~~8 bytes~~	~~8 bytes~~	~~Variable~~	~~variable~~	~~4 bytes~~	~~4 bytes~~

Header 1	Safety IO data 1	CRC 1	Header 2	Safety IO data 2	CRC 2
8 bytes	variable	4 bytes	8 bytes	variable	4 bytes

As show in Table 4-12, 'Header 2' is the bit-reversed data of 'Header 1', 'Safety data 2' is the bit-reversed data of 'Safety data 1', and 'CRC 2' is the bit-reversed data of 'CRC 1'.

上述结构中，第二份数据是第一份数据的反转。

Table 4-13 REQ safety frame header structure

表 4-13 请求帧头结构

	Data Type	Length	Value	Desc
Sequence Number	unsigned short	2 bytes		Increment after each REQ in source PM 递增序号
SrcAddr	unsigned char	1 byte		(ID of source PM (0, 1, 2) << 6) | ID of control station (0~63) 源地址：PM 编号+控制站节点号
DstAddr	unsigned char	1 byte		ID of destination control station (0~63) 目的控制站节点号（0~63）
Block Number	unsigned char	1 byte	n	Number of safety relevant data blocks 数据块的个数
Control Byte	unsigned char	1 byte		
Frame Length	unsigned short	2 bytes		Number of total bytes in safety frame with Header

				安全层数据帧的总长度（字节），包括帧头

Table 4-14 Control Byte

表 4-14 控制字节

Bit	Value	Description
0	Failure flag	Set to ‘1’ when using fail-safe value 倒向安全状态标志位
1-7	Reserved	

Table 4-15 ACK safety frame structure of one PM

表 4-15 单个 PM 应答帧结构

~~Header 1~~	~~Header 2~~	~~CRC 1~~	~~CRC 2~~
~~8 bytes~~	~~8 bytes~~	~~4 bytes~~	~~4 bytes~~

Header 1	CRC 1	Header 2	CRC 2
8 bytes	4 bytes	8 bytes	4 bytes

As show in Table 4-16, ‘Header 2’ is the bit-reversed data of ‘Header 1’ and ‘CRC 2’ is the bit-reversed data of ‘CRC 1’.

上述结构中，第二份数据是第一份数据的反转。

Table 4-16 ACK safety frame header structure

表 4-16 应答帧头结构

	Data Type	Length	Value	Desc
Sequence Number	unsigned short	2 bytes		Increment after each REQ in source PM 序号，同请求包
SrcAddr	unsigned char	1 byte		(ID of source PM (0, 1, 2) << 6) | ID of control station (0~63) 源地址：PM 编号+控制站节点号
DstAddr	unsigned char	1 byte		ID of destination control station (0~63) 目的控制站节点号（0~63）
Status Byte	unsigned char	2 byte		
Reserved	unsigned char	1 byte		
Frame Length	unsigned short	1 bytes		Number of total bytes in safety frame with Header 安全层数据帧的总长度（字节），包括帧头

Table 4-17 Status Byte

表 4-17 状态字节

Bit	Value	Description
0	Communication failure: WD-timeout	Set to '1' when Watchdog timeout 通信错误：看门狗超时时，置 1
1	Communication failure: PMA CRC	Set to '1' when CRC of PM A failure PM A 的 CRC 错误时，置 1
2	Communication failure: PMB CRC	Set to '1' when CRC of PM B failure PM B 的 CRC 错误时，置 1
3	Communication failure: PMC CRC	Set to '1' when CRC of PM V failure PM C 的 CRC 错误时，置 1
4	Communication failure: PMA Addr	Set to '1' when SrcAddr or DesAddr of PM A failure PM A 源地址或目的地址出错时，置 1
5	Communication failure: PMB Addr	Set to '1' when SrcAddr or DesAddr of PM B failure PM B 源地址或目的地址出错时，置 1
6	Communication failure: PMC Addr	Set to '1' when SrcAddr or DesAddr of PM C failure PM C 源地址或目的地址出错时，置 1
7	Communication failure: PMA SQ	Set to '1' when Sequence number of PM A failure PM A 序号错误时，置 1
8	Communication failure: PMB SQ	Set to '1' when Sequence number of PM B failure PM B 序号错误时，置 1
9	Communication failure: PMC SQ	Set to '1' when Sequence number of PM C failure PM C 序号错误时，置 1
10	Alarm	PM Info in Additional Info not matched with safety data frame. 附加信息中的 PM Info，与安全帧中的 PM 信息不一致。
11~13	Reserved	
14, 15	Data Source	Source PM ID of adopted data, 1: PMA; 2: PMB; 3: PMC 源 PM ID，1：PMA；2：PMB；3：PMC

5 Functional security design 信息安全设计

5.1 Identification and Authentication Control 识别和身份验证控制

SWSC_NSafR_SecR_B_001

The user can set a control station password for the control station in configuration software, and the PC software must use this password to connect the controller. Each PC software has a unique ID and operating range. When the control station received a command from PC software, the embedded software will check it. If the ID is invalid or the command is out of the operating range, an alarm will be provided to the user. The project version will be verified when the control station received a

debugging operation from PC software.

组态软件可配置控制站密码，所有上位机软件和控制站通讯时都需要输入此密码。每个上位机软件均具备唯一的 ID 和服务码范围。嵌入式软件验证 ID 有效性，并且根据 ID 及其服务码范围，检查上位机软件下发的操作是否有效，如果无效，则拒绝服务并且报错。调试操作时需验证工程版本信息。

For identification and authentication control between control stations, the embedded software will check the validation of the stations ID.

其他控制站识别（站间通信）：嵌入式软件负责验证源控制站 ID 和目的控制站 ID 是否有效。

For device (Modbus or IO module) identification and authentication, the embedded software will check the ID and the actual use port to ensure that they are accord with the project configuration.

对于设备（Modbus 设备或者 IO 模块）的识别和身份验证，嵌入式软件检查实际使用的端口或 ID 号和工程中的配置是否一致。

Support IP access control, and user can configure read/write authority and communication protocol for each IP address.

支持 IP 访问控制，可以为每个 IP 配置读写权限及可使用的通讯协议。

Remote access is not supported.

不支持远程访问。

5.2 Use control 使用控制

SWSC_NSafR_SecR_B_002

Control station must be accessed with a control station password, and the read/ write authority of communication between control stations as well as communication to the third party devices must be explicitly configured when editing the project in PC software.

控制站必须使用控制站密码才能够访问，控制站站间通信的读写权限由工程唯一确定，Modbus 设备的读写权限由工程唯一确定。

SWSC_NSafR_SecR_A_004

Option is provided to support session locking after an administrator specified period of time of inactivity for the session until re-established by authorized user.

一段时间无任何通讯操作后，上位机软件需要重新登录。该非活动时间的大小用户可配。

SWSC_NSafR_SecR_A_005

Records which are relevant to security with timestamp, source, category, type, event ID & results are generated and stored in control station, including: access control, power on, error event, backup &

restore event, download and other debug operation event, and audit log events.

嵌入式软件保存与信息安全相关的日志记录。日志类型包括：访问控制、上电记录、故障记录、备份与恢复、组态下装和调试记录，以及审计日志。日志内容包含：时间戳、故障源、日志类型、日志 ID 和事件结果。

SWSC_NSafR_SecR_A_006

Each PM, CM can save the latest 10000 log records. When the space which is used for storing log is less than the threshold value, an alarm will be provided to the user. The threshold is 5%.

PM、CM 各自保存最近的 10000 条日志记录。当有未被读取的日志将要被最新日志覆盖时，产生报警，该预警门限为 5%。

SWSC_NSafR_SecR_A_007

Failure of audit processing will not influence the safety critical functions, and an alarm will be provided to the user.

日志记录失败不会影响到安全功能，但会提供一个警告给用户。

SWSC_NSafR_SecR_A_008

Timestamp is synchronized with system-wide time source. Detection of unauthorized alteration of time source and discrepancy of time is implemented, and it will cause an audit event upon alteration or discrepancy.

时间戳所用的时间在系统内部同步，当检测非法的时间源或者校时偏差超限时会产生日志记录。

SWSC_NSafR_SecR_A_009

Debug operation of PC software or abnormal access of the device will be recorded in the SRAM with a time stamp. The battery on chassis provides power for SRAM to ensure the records can be maintained after power-off.

上位机软件的调试操作以及接入设备的异常访问会作为记录保存在 SRAM 中，有带时间戳。机架上的电池保证 SRAM 中的记录掉电不丢失。

5.3 System Integrity 系统完整性

SWSC_NSafR_SecR_A_010

Safety measures are applied for all the safety communications. Measures such as CRC and odd-even check is used to protect other non-safety related communications.

安全相关的通讯采用安全协议来保证通讯完整性，非安全的通讯采用 CRC 或者奇偶校验来保证通讯完整性。

SWSC_NSafR_SecR_A_028

Separation of data and executable code in control station, and measures are in place to prevent execution of code located in data space. For CM, MMU is used for memory separation. For PM, the separation is implemented by software design.

Only specified functionalities in CM OS (Linux) are used in dedicated way, while other functionalities are not used to avoid the opportunity of attacking from malicious code.

控制站中数据和代码分离，用于防止代码在数据区中执行。CM 中使用 MMU 来进行内存分配，PM 通过软件设计来进行内存分配。

在 CM 中的 OS（Linux）已经裁剪为实际需要的最小功能，用于减少来自恶意代码攻击的机会。

SWSC_NSafR_SecR_A_012

Protection measures such as CRC are used to detect modifications to firmware, libraries and project. If an unauthorized change occurs, the embedded software will record it and provide an alarm to the user.

固件、库和工程等均带有 CRC 信息，嵌入式软件可通过计算 CRC，然后与其自带的 CRC 进行比较，从而判断得知上述内容是否被意外损坏。当损坏发生时，嵌入式软件记录日志并报警。

SWSC_NSafR_SecR_A_013

The control station is responsible for judging whether the data is valid, such as whether the data address is out of the range, whether the data value is overrun, and so on.

控制站判断数据是否有效，如数据地址范围是否正确、数据值是否超限等等。

PM and CM are responsible for judging whether the CM_BUS data is valid, such as whether the data address is out of the range, whether the data value is overrun, and so on.

PM、CM 各自判断 CM_BUS 数据是否有效，如数据地址范围是否正确、数据值是否超限等等。

The software checks the value of the key switch whether it is in the allowed range。

软件检查钥匙开关的值是否在允许范围内。

SWSC_NSafR_SecR_A_015

Error messages are handled by dedicated diagnostic software with account and password IAC which is in an expeditious manner without providing information that could be exploited.

错误记录只能被诊断软件获取，诊断软件带有 IAC 和 UC 控制，保证信息不被非法利用。

SWSC_NSafR_SecR_A_016

It does not support the modification of the log with diagnostic software, and support the clear of

the log.

不支持对日志的修改，支持诊断软件清除日志。

5.4 Data Confidentiality 数据保密性

SWSC_NSafR_SecR_C_017

Control station password is protected by private hash algorithm when it is stored and transmitted.

控制站密码在存储和传输时，都采用私有 hash 算法进行保护。

~~Control station password is encrypted, neither stored internally nor sent over shared network in clear text format~~

~~控制站密码为加密传输和加密保存。~~

SWSC_NSafR_SecR_A_018

The log file and the source project can be cleared by diagnostic software. If the key switch is in 'Init' when power on, the project will be cleared.

日志和源工程文件支持内部诊断软件通过相应的服务清除。如果上电时钥匙开关在 init 档位，上电后工程无效。

5.5 Restricted Data Flow 受约束的数据流

SWSC_NSafR_SecR_A_019

User configuration of network parameters (IP, masks, etc.) is supported.

网络参数，如 IP 地址，子网掩码等，用户可配。

5.6 Timely Response to Events 事件的及时响应

SWSC_NSafR_SecR_A_020

Diagnostic software can be configured to read the log automatically.

诊断软件可配置为自动读取日志。

5.7 Resource Availability 资源可用性

SWSC_NSafR_SecR_A_021

Operation under degradation mode during flooding type attack with IP_BUS or IO module.

IP_BUS 通讯或 I/O 模块故障后，控制站降级模式下运行。

When network storm occurs, all the functions of the PM and CM except system net communication shall be remain normal. System net communication shall be recovered after the network storm.

当网络风暴发生时，除系统网通讯功能外，PM、CM 的其他功能不受影响。网络风暴结

束后系统网通讯功能恢复工作。

Communication and safety functions independent of each other, communication failure does not affect the safety function.

通讯功能和安全功能相互独立，通讯故障不影响安全功能。

SWSC_NSafR_SecR_A_022

All resources are statically allocated.

所有资源都是静态分配。

SWSC_NSafR_SecR_A_023

The CM support to store the source project in FLASH, and does not affect normal operation.

嵌入式固件支持备份源工程文件在 CM 中，备份过程不影响其他功能。

SWSC_NSafR_SecR_A_024

After power on, the system will be running according to the project configuration. If the project is missing, the configuration software can read the source project from CM, and then download the project again.

上电后，系统按照工程配置运行。如果工程丢失，组态软件可读取 CM 中备份的源工程文件，然后重新下装工程。

SWSC_NSafR_SecR_B_026

The properties of physical port (such as Ethernet port and serial port) can be configured by user though configuration software. Some functions of the protocol can be prohibited by the configuration software, such as writing function of Modbus protocol.

物理端口（网口和串口）的相关属性用户可配，如协议类型、是否使能，可通过上位机软件进行设置。协议的某些功能可通过上位机软件禁止，如可禁止通过 Modbus 协议写变量。

Only specified functionalities in CM OS (Linux) are used in dedicated way, while other functionalities are not used to avoid the opportunity of attacking from malicious code. TCP/IP is only used for private communication protocol、Modbus TCP and SNTP, and unused ports will be disabled.

CM 的 linux 操作系统中，不用的功能都会被裁剪，用于保护受到恶意代码的攻击。TCP/IP 协议只用于私有通讯协议、Modbus TCP、SNTP，不用的端口会被禁用。

SWSC_NSafR_SecR_A_027

The embedded software collects information of installed component including ID, revision & configuration, etc. The information will be send to diagnostic software.

嵌入式软件负责收集已安装模块的信息：ID、版本和配置信息等，此信息可被诊断软件读取。

——以下无正文

The last requirement number is SWSC_SafR_NSecR_A_060

本文档最后一个需求编号为 SWSC_SafR_NSecR_A_060