Document Title: Embedded Software Safety Requirements Specification of Safety Control System

Document Number: 15-Q01-000058

Project Number: SF-RD-1501

Project Number: First phase of Safety Control System Development Project

Material Number: N/A

Document Version: A.4

Classification Level: Highly secret

Document Status: CFC

Controlled Status: Under control

|  |  |
| --- | --- |
| Prepared by: Zhu Genghua | 2017-4-17 |
| Checked by: Wen Yiming | 2017-4-17 |
| Countersigned by: Wang Dong, Li Qi, | 2017-4-17 |
| Liu Yang, Liu Yue |  |
| Approved by: Ji Jun | 2017-4-17 |

**Revision History**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| No. | Relevant Chapter | Change Description | Date | Version Before Change | Version After Change | Prepared by | Checked by | Approved by |
|  |  | Document created | 2015-5-22 |  | A | Zhu Genghua | Wen Yiming | Ji Jun |
|  | 3.8  3.11  3.16  3.18 | 3.8: Modify the description of PeerToPeer.  3.11: Add this chapter.  3.16: Delete GPS Timing.  3.18: Add the chapter 3.18.4, 3.18.5. | 2015-9-16 | A | A.1 | Zhu Genghua | Wen Yiming | Ji Jun |
|  | 2.2  3.1  3.2  3.3  3.4  3.5  3.6  3.7  3.9  3.10  3.12  3.15  3.16  3.18  3.19  3.21  全部 | 2.2: Modify the description of Communication data flow.  3.1: Modify the description of software state transition.  3.2: Modify the description of PM degradation.  3.3: Add PI points  3.4: The maximum control cycle is 500ms.  3.5: Add conditions for data power lost retention  3.6: Add synchronization of project  3.7: Add HMI write variable  3.9: Add this chapter.  3.10: Add this chapter.  3.12: Modify the description of hard SOE.  3.15: Add IP access control  3.16: Add GPS Timing; Add NTP/SNTP Master.  3.18: Add Modbus ASCII.  3.19: Modify the description of indicator.  3.21: Modify the description of log.  ALL: Add requirement number. | 2015-10-09 |
|  | 2.1  2.2  3.1  3.2  3.15 | 2.1: Modify Figure 2-1 and scope of PC software  2.2: Modify Figure 2-2 and scope of PC software  3.1: Modify the PM operation to DO and AO modules when it is in “Stop state”  3.2: Modify the description of operation time for single PM  3.15: Move the “IP access control” to 3.14 chapter. | 2016-2-15 | A.1 | A.2 | Zhu Genghua | Wen Yiming | Ji Jun |
|  | 3.7  3.12  3.14  3.18  3.20  3.21  3.23 | 3.7: Delete 3.7.4 Chapter.  3.12: Modify the SOE capacity.  3.14: Modify the description of IP address setting.  3.18: Modify the description of 3.18.3. Delete 3.18.5 Chapter.  3.20: Delete the function that the system can scan the module information before the module is configured.  Delete 3.20.14 Chapter  3.21: Modify the description.  3.23: Modify the description. | 2016-12-26 | A.2 | A.3 | Zhu Genghua | Wen Yiming | Ji Jun |
|  | 3.9.2  3.14.1 | 3.9.2:  Modify the task timeout reaction to be not related to the Control/Safety property of a task.  3.14.1：  Modify the default IP address of NET1. | 2017-4-17 | A.3 | A.4 | Zhu Genghua | Wen Yiming | Ji Jun |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

**Relationship between this version and old version:**

文件名称：安全控制系统嵌入式软件安全需求规格书

文件编号：15-Q01-000058

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.4

文件密级：机密

文件状态：CFC

受控标识：受控

|  |  |
| --- | --- |
| 拟制：朱耿华 | 2017年4月17日 |
| 审核：温宜明 | 2017年4月17日 |
| 会签：王东、李琦、刘阳、刘跃 | 2017年4月17日 |
|  |  |
| 批准：季俊 | 2017年4月17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 |
|  |  | 首次创建 | 2015-5-22 |  | A | 朱耿华 | 温宜明 | 季俊 |
|  | 3.8  3.11  3.16  3.18 | 3.8：修改站间安全通讯描述。  3.11：增加该章节。  3.16：删去GPS直接校时章节。  3.18：增加数据类型章节和端口权限控制章节。 | 2015-9-16 | A | A.1 | 朱耿华 | 温宜明 | 季俊 |
|  | 2.2  3.1  3.2  3.3  3.4  3.5  3.6  3.7  3.9  3.10  3.12  3.13  3.16  3.18  3.19  3.21  全部 | 2.2：修改通讯示意图及其描述。  3.1：修改软件状态转换图及描述。  3.2：修改降级模式的描述。  3.3：增加PI点。  3.4：最大控制周期改为500ms。  3.5：增加数据掉电保护条件。  3.6：增加同步工程描述。  3.7：增加HMI写变量  3.9：插入3.9异常处理章节  3.10：增加PM算法章节  3.12：增加从OSP模块读取SOE。  3.15：增加IP访问控制  3.16：恢复GPS直接校时章节；增加支持NTP/SNTP主站功能。  3.18：Modbus增加ASCII方式。  3.19：修改状态灯描述  3.21：修改日志的描述  全部：增加条目编号 | 2015-10-09 |
|  | 2.1  2.2  3.1  3.2  3.15 | 2.1:修改图2-1和上位机软件范围  2.2:修改图2-2和上位机软件范围  3.1：修改”Stop state”时PM对DO和AO模块的操作  3.2：修改单个PM时关于运行时间的描述  3.15：将IP访问控制移动到3.14章节 | 2016-2-15 | A.1 | A.2 | 朱耿华 | 温宜明 | 季俊 |
|  | 3.7  3.12  3.14  3.18  3.20  3.21  3.23 | 3.7：删去3.7.4章节  3.12：修改SOE容量  3.14：修改IP地址设置的描述  3.18：修改3.18.3modbus启停的描述，删去3.18.5章节  3.20：删去3.20.12章节中未配置时支持扫描IO从站的功能；删去3.20.14章节  3.21：修改描述  3.23.2：修改描述 | 2016-12-26 | A.2 | A.3 | 朱耿华 | 温宜明 | 季俊 |
|  | 3.9.2  3.14.1 | 3.9.2:  修订任务超时时的响应，与任务的Control/Safety属性无关  3.14.1:  修改NET1的默认IP地址 | 2017-4-17 | A.3 | A.4 | 朱耿华 | 温宜明 | 季俊 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

**本版本与旧文件（版本）的关系：**

**Content 目录**

[1 Document overview 文档概述 1](#_Toc482611655)

[1.1 Introduction 综述 1](#_Toc482611656)

[1.2 Reference 参考文档 1](#_Toc482611657)

[1.2.1 Project documents 内部参考文档 1](#_Toc482611658)

[1.3 Terms and abbreviations 术语和缩略语 1](#_Toc482611659)

[1.3.1 Terms 术语 1](#_Toc482611660)

[1.3.2 Abbreviations 缩略语 3](#_Toc482611661)

[2 Software general description 软件总体描述 3](#_Toc482611662)

[2.1 Function overview 功能概述 3](#_Toc482611663)

[2.2 Communication data flow 通讯数据流 4](#_Toc482611664)

[3 Software requirement specification 软件需求规格 5](#_Toc482611665)

[3.1 Software state transition 软件状态转换 5](#_Toc482611666)

[3.2 PM degradation mode PM降级模式 7](#_Toc482611667)

[3.3 Scale of single control station 单站规模 9](#_Toc482611668)

[3.4 Control cycle configuration 控制周期设置 9](#_Toc482611669)

[3.4.1 Control cycle 控制周期 9](#_Toc482611670)

[3.4.2 Multitasking 多用户程序 9](#_Toc482611671)

[3.4.3 Control cycle ladder 控制周期设置阶梯 9](#_Toc482611672)

[3.5 Power lost retention 掉电保持 9](#_Toc482611673)

[3.5.1 Data retention 数据掉电保持 9](#_Toc482611674)

[3.5.2 Project retention 工程掉电保持 10](#_Toc482611675)

[3.6 PM online replacement PM在线更换 10](#_Toc482611676)

[3.7 Configuration and debug operation组态及调试 10](#_Toc482611677)

[3.7.1 Download 下装 10](#_Toc482611678)

[3.7.2 Write variables 写变量 11](#_Toc482611679)

[3.7.3 Enable/disable 使能/释放使能 11](#_Toc482611680)

[3.7.4 Parameters read-back 参数回读 11](#_Toc482611681)

[3.7.5 Pause 暂停 11](#_Toc482611682)

[3.7.6 Single step 单步运行 12](#_Toc482611683)

[3.8 Safety communication 安全通讯 12](#_Toc482611684)

[3.8.1 Safety communicaton between control stations 安全站间通讯 12](#_Toc482611685)

[3.8.2 Safety IO protocol 安全IO协议 12](#_Toc482611686)

[3.9 Exception handling 异常处理 12](#_Toc482611687)

[3.9.1 IP\_BUS failure recovery IP\_BUS故障恢复 12](#_Toc482611688)

[3.9.2 User program execution timeout 执行用户程序超时 13](#_Toc482611689)

[3.9.3 Calculation exception 运算异常 13](#_Toc482611690)

[3.10 PM Algorithm PM算法 13](#_Toc482611691)

[3.11 Communication protocol type 通讯协议类型 14](#_Toc482611692)

[3.12 SOE function SOE功能 15](#_Toc482611693)

[3.12.1 Hard SOE record 硬SOE记录 15](#_Toc482611694)

[3.12.2 Soft SOE record 软SOE记录 15](#_Toc482611695)

[3.12.3 The capacity of SOE SOE容量 15](#_Toc482611696)

[3.12.4 SOE group SOE分组 15](#_Toc482611697)

[3.12.5 SOE read SOE读取 16](#_Toc482611698)

[3.13 Source project backup 源文件备份 16](#_Toc482611699)

[3.14 IP configuration IP配置 16](#_Toc482611700)

[3.14.1 IP address setting IP地址配置 16](#_Toc482611701)

[3.14.2 IP Access Control IP访问控制 17](#_Toc482611702)

[3.15 Network Storm Protect 防网络风暴 17](#_Toc482611703)

[3.16 Timing 校时 17](#_Toc482611704)

[3.16.1 Timing Function Block 功能块校时 17](#_Toc482611705)

[3.16.2 NTP/SNTP Timing NTP/SNTP校时 17](#_Toc482611706)

[3.16.3 GPS Timing GPS直接校时 17](#_Toc482611707)

[3.17 Variables On-line Monitor 变量在线监视 18](#_Toc482611708)

[3.17.1 Variables Monitor by Configuration Software 组态软件变量监视 18](#_Toc482611709)

[3.17.2 Oscilloscope 示波器 18](#_Toc482611710)

[3.17.3 Variables Monitor by OPC Software OPC软件变量监视 18](#_Toc482611711)

[3.18 Modbus 18](#_Toc482611712)

[3.18.1 Modbus Protocol Modbus协议 18](#_Toc482611713)

[3.18.2 Modbus Application Modbus应用 19](#_Toc482611714)

[3.18.3 Modbus Start/Stop Modbus启停 19](#_Toc482611715)

[3.18.4 Data Type 数据类型 19](#_Toc482611716)

[3.18.5 Port access control 端口权限控制 19](#_Toc482611717)

[3.19 Indicators指示灯 19](#_Toc482611718)

[3.19.1 CM Indicators CM指示灯 19](#_Toc482611719)

[3.19.2 PM Indicators PM指示灯 22](#_Toc482611720)

[3.20 Diagnostic function 诊断功能 24](#_Toc482611721)

[3.20.1 Debug interface 调试接口 24](#_Toc482611722)

[3.20.2 Memory usage diagnostic 内存使用率诊断 24](#_Toc482611723)

[3.20.3 CPU load diagnostic CPU负荷诊断 25](#_Toc482611724)

[3.20.4 System Net load diagnostic System Net网络负荷诊断 25](#_Toc482611725)

[3.20.5 CM\_BUS status diagnostic CM\_BUS故障诊断 25](#_Toc482611726)

[3.20.6 PM\_BUS status diagnostic PM\_BUS故障诊断 25](#_Toc482611727)

[3.20.7 Safety Net status diagnostic Safety Net故障诊断 25](#_Toc482611728)

[3.20.8 IP\_BUS status diagnostic IP\_BUS故障诊断 25](#_Toc482611729)

[3.20.9 CM status diagnostic CM状况诊断 26](#_Toc482611730)

[3.20.10 PM status diagnostic PM状况诊断 26](#_Toc482611731)

[3.20.11 PW status diagnostic PW状况诊断 26](#_Toc482611732)

[3.20.12 IO module status diagnostic IO状况诊断 26](#_Toc482611733)

[3.20.13 Diagnostic information clear 诊断清除 26](#_Toc482611734)

[3.20.14 Safety parameters information 安全参数信息 26](#_Toc482611735)

[3.21 Log 日志 27](#_Toc482611736)

[3.21.1 Log capacity 日志容量 27](#_Toc482611737)

[3.21.2 Log content 日志内容 27](#_Toc482611738)

[3.21.3 Power lost retention 日志掉电保持 27](#_Toc482611739)

[3.21.4 Log read 日志读取 27](#_Toc482611740)

[3.22 Performance 性能 28](#_Toc482611741)

[3.22.1 The scale of control station 控制站规模 28](#_Toc482611742)

[3.22.2 System network load 系统网负荷 28](#_Toc482611743)

[3.22.3 Power-on time 上电时间 28](#_Toc482611744)

[3.23 Upgrade via network 现场升级 28](#_Toc482611745)

[3.23.1 Upgrade software via network 软件网络升级 28](#_Toc482611746)

[3.23.2 Version record 版本记录 29](#_Toc482611747)

# Document overview 文档概述

## Introduction 综述

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

本文档依据《安全控制系统安全需求规格书》和《安全控制系统总体设计说明书》，描述了安全控制系统中PM和CM嵌入式软件的需求规格，是后续PM和CM软件设计的输入。

## Reference 参考文档

### 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 |
| 4 | 15-O05-0049 | Safety requirement specification of Safety Control System  安全控制系统安全需求规格说明书 |
| 5 | 15-O06-0051 | System safety concept of Safety Control System  安全安全控制系统总体设计说明书 |

## Terms and abbreviations 术语和缩略语

### 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  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。 |

### 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 | AI | Analog Input Module | 模拟量输入模块 |
| 4 | AO | Analog Output Module | 模拟量输出模块 |
| 5 | DI | Digital Input Module | 数字量输入模块 |
| 6 | DO | Digital Output Module | 数字量输出模块 |
| 7 | OSP | Over Speed Protect Module | 超速保护模块 |
| 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 |

# Software general description 软件总体描述

## Function overview 功能概述

SWSRS\_SafR\_NSecR\_B\_067



Figure 2-1 System logical architecture diagram

图2-1 系统逻辑架构图

System logical architecture is shown in Figure 2-1, the part in the red dashed box is PM and CM. Embedded software includes the firmware in the PM, the firmware in the CM and the OS in the CM.

系统逻辑架构如图2-1所示，其中红色虚线框内部分为本文涉及的PM、CM。嵌入式软件指的是PM中的固件以及CM中的固件和OS。

## Communication data flow 通讯数据流

SWSRS\_SafR\_NSecR\_B\_068

The system data flow are illustrated in Figure 2-2. IP\_BUS is the communication link between the PM and the IO modules; System Net is used for communication between the control station and PC software; Modbus RTU/TCP is used for communication between the control station and the t[hird](http://cn.bing.com/dict/search?q=Third&FORM=BDVSP6&mkt=zh-cn)[-](http://cn.bing.com/dict/search?q=-&FORM=BDVSP6&mkt=zh-cn)[party](http://cn.bing.com/dict/search?q=party&FORM=BDVSP6&mkt=zh-cn) device; Safety Net is used for the safety data exchange between control stations.

数据流如图2-2所示，其中IP\_BUS用于PM与IO模块进行通讯；System Net用于控制站与各个上位机软件进行通讯；Modbus RTU/TCP用于控制站和第三方设备进行通讯；Safety Net用于控制站与其他控制站进行通讯。

CM\_BUS is used for communication between CM and PM; PM\_BUS is used for data exchange between PMs.

PM和CM之间通过CM\_BUS通讯，PM与PM之间通过PM\_BUS进行通讯。



Figure 2-2 Control station communication data flow

图2-2 控制站通讯示意图

# Software requirement specification 软件需求规格

## Software state transition 软件状态转换

SWSRS\_SafR\_NSecR\_C\_001

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 3-1 Transition of software states

图3-1 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 in the ‘Prog’ position, the software enters into Debug run state.

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.

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.

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.

PM中无用户工程。

* Program state：In this state, PM has a project and supports user debug operation.

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.

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.

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.

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。

System shall support start-up to normal operation when only one PM or two PMs exist.

系统支持仅存在一系PM或两系PM时上电启动。

## PM degradation mode PM降级模式

SWSRS\_SafR\_NSecR\_C\_002

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 3-2 PM degradation mode

图3-2 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。

## Scale of single control station 单站规模

SWSRS\_SafR\_NSecR\_B\_003

The system shall support a maximum scale of 3680 digital points or 1248 analog points (including PI point) in a single control station.

单控制站硬件测点规模：开关量点最大支持3680点，模拟量点(含PI点)最大支持1248点。

## Control cycle configuration 控制周期设置

### Control cycle 控制周期

SWSRS\_SafR\_NSecR\_A\_004

For a typical 300 point configuration case, the control cycle is 10ms. If the number of IO [point](http://cn.bing.com/dict/search?q=point&FORM=BDVSP6&mkt=zh-cn)s is [1000](http://cn.bing.com/dict/search?q=300&FORM=BDVSP6&mkt=zh-cn), i.e. 500 digital points and 500 analogue points (16 pairs of DI/DO, 10 pairs of AI, 12 pairs of AO), the minimum [control](http://cn.bing.com/dict/search?q=control&FORM=BDVSP6&mkt=zh-cn) [cycle](http://cn.bing.com/dict/search?q=cycle&FORM=BDVSP6&mkt=zh-cn) can be [less than](http://cn.bing.com/dict/search?q=less%20than&FORM=BDVSP6&mkt=zh-cn) 100ms.

单用户程序情况下，如系统规模中硬件测点小于300点，控制周期至少可设置为10ms；如系统规模中硬件测点小于1000点，其中开关量500点，模拟量500点，控制周期至少可设置为100ms。

### Multitasking 多用户程序

SWSRS\_SafR\_NSecR\_A\_005

It allows users to configure two user programs (tasks), and set to different control cycles separately.

支持用户组态两个用户程序（任务），并设置为不同的控制周期。

### Control cycle ladder 控制周期设置阶梯

SWSRS\_SafR\_NSecR\_B\_006

The control cycle can be set by configuration software, and the range is 5ms~500ms, the ladder is 5ms.

控制周期最小为5ms，最大为500ms，设置阶梯为5ms。

## Power lost retention 掉电保持

### Data retention 数据掉电保持

SWSRS\_SafR\_NSecR\_B\_007

When module re-power on after power off, a part of data can be resumed to the result of the last normal calculation. These variables will be defined by the user in configuration software, and its total size is 1kByte. If the key switch is in ‘Init’ when power on, the retained data will be cleared. If the module has been pulled out, the retained data is lost.

模块掉电后再次上电，部分数据能够恢复成最后一次正常运算后的结果。变量由使用者通过组态软件指定，总大小为1kByte。如果上电时钥匙开关在init档位，上电后保持的数据无效。模块拔插后掉电保护数据无效。

### Project retention 工程掉电保持

SWSRS\_SafR\_NSecR\_A\_008

When module re-power on after power off, the project retain valid. If the key switch is in ‘Init’ when power on, the project will be cleared.

模块掉电后再次上电，工程保持有效。如果上电时钥匙开关在init档位，上电后工程无效。

## PM online replacement PM在线更换

SWSRS\_SafR\_NSecR\_B\_009

Online replacement of PM shall be supported, 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, the delayed time is related to the number of real time data, but the maxmum delayed time is no more than 3 control cycles.

支持在线更换PM，更换后的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。同步实时数据会使得用户程序执行有一次延后，延后时间和实时数据量有关，不大于3个控制周期。

It is not allowed to install two or more PMs at the same time during the system running. It is not allowed to install the next PM module until the current PM module is running normally.

系统运行过程中不允许同时安装两个或多个PM，需等待前一个被安装的模块正常运行后方可安装下一个模块。

## Configuration and debug operation组态及调试

### Download 下装

SWSRS\_NSafR\_NSecR\_A\_010

Downloading and online downloading to the control station shall be supported in Program state by configuration software.

Online downloading supports the following operations: add variables; modification logic; add or remove IO modules; modification IO parameters; add or remove chasises.

在Program状态下，支持组态软件对控制站进行全下装操作、在线下装操作。

在线下装包括在线增减变量；在线修改逻辑；在线增减IO模块或修改IO模块参数；在线增减机架。

### Write variables 写变量

SWSRS\_NSafR\_NSecR\_B\_011

Writing variables to the control station shall be supported in Program state by configuration software, OPC software and HMI software.

在Program状态下，支持组态软件对控制站进行写变量操作支持OPC软件或HMI软件对控制站进行写变量操作。

### Enable/disable 使能/释放使能

SWSRS\_NSafR\_NSecR\_A\_012

Enable or disable variables operation of the control station shall be supported in Program state by configuration software. If the key switch has been switched from ‘Prog’ to the other positions, there shall be no effect on enabled/disabled status of the variables.

在调试模式下，支持组态软件对控制站进行使能变量/释放使能操作。钥匙开关从PROG档位切换到其他档位不会影响使能状态。

### Parameters read-back 参数回读

SWSRS\_NSafR\_NSecR\_A\_013

Parameters read-back operation shall be supported in Program state by configuration software, the parameters which want to be readed back shall be assigned by user using configuration software.

在调试模式下，支持组态软件对控制站进行持参数回读，需要回读的参数变量由使用者通过组态软件指定。

### Pause 暂停

SWSRS\_NSafR\_NSecR\_A\_014

Pause operation shall be supported in Program state by configuration software. User program is not executed when pause operation happened, and the output hold the last calculation result. This operation can be used by single user program.在调试模式下，支持组态软件对控制站进行暂停操作。暂停时，控制站不执行用户程序，输出保持暂停前最后一次运算的结果。该操作可以针对单个用户程序。

### Single step 单步运行

SWSRS\_NSafR\_NSecR\_A\_015

Single step operation shall be supported in Program state by configuration software. The user program is executed only once in this condition, and the output hold the current calculation result. This operation can be used by single user program.

在调试模式下，支持组态软件对控制站进行单步运行操作。此时，控制站只执行一次用户程序，后续输出保持该次运算的结果。该操作可以针对单个用户程序。

## Safety communication 安全通讯

### Safety communicaton between control stations 安全站间通讯

SWSRS\_NSafR\_NSecR\_B\_016

Safty communication between control stations (Peer to Peer) can be used between several control stations, the communication start or stop of each control station can be controlled independently. The cycle of the communication between control stations can be configured. When the cycle is less than the actual interval (the actual interval is the time between send requests and receive the responsed), the actural interval will replace the set cycle.

There is an independent ID for each control station, which is configured by the configuration software.

支持多个控制站之间的安全数据通讯（Peer to Peer），可单独控制每一个控制站的通讯启停。站间通讯周期可配置，当配置的通讯周期小于实际的数据发送间隔（从数据发送到接收到对方控制器的应答）时，按实际的数据发送间隔发送数据。

每个控制站有各自的站号，通过组态软件配置。

### Safety IO protocol 安全IO协议

SWSRS\_NSafR\_NSecR\_A\_017

The safety IO communication protocol will be used betwwen PM and IO modules, the safety layer which belonged to the master of IP\_BUS is implemented by PM software.

PM和IO模块之间采用安全通讯协议，IP\_BUS主站端的安全层由PM软件实现。

## Exception handling 异常处理

### IP\_BUS failure recovery IP\_BUS故障恢复

SWSRS\_NSafR\_NSecR\_A\_018

The communication re-connection between PM and IO can be configured to require confirmation by user, when the communication failure has happened. This property is configured by the user via the configuration software, if the choice is not need to be confirmed, the re-connection will be established automatically after the [failure](javascript:void(0);) [recovery](javascript:void(0);). Otherwise, the re-connection will not be established until the user confirmed.

PM和IO通讯中断后，再次建立连接是否需要用户确认为可配的。该属性由使用者通过组态软件配置，如配置为不需确认，PM和IO之间故障排除后，会自动建立连接；如配置为需确认，在用户确认前，PM和IO之间保持通讯中断。

### User program execution timeout 执行用户程序超时

SWSRS\_SafR\_NSecR\_B\_019

The user program can be configured as both stopped and alarmed or just alarmed when executing timeout. This property is configured by the user via 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。

When timeout occurs in task, the system only generates alarm on PCSW, which is independent of Control/Safety property of a task.

执行用户任务超时时，系统仅在上位机软件上产生报警。此特性与任务的Control/Safety属性无关。

### Calculation exception 运算异常

SWSRS\_SafR\_NSecR\_A\_020

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, when user selects the safty application mode; the property can be configured to enabled or disabled, when user selects the control application mode.

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。

## PM Algorithm PM算法

SWSRS\_SafR\_NSecR\_B\_069

PM provides standard functions such as ABS, provides standard function blocks such as TON, and provides system function blocks such as UP\_STATUS which is used for reading UP status.

PM提供ABS等标准函数；提供TON等标准功能块；以及提供读取UP状态等系统库。

## Communication protocol type 通讯协议类型

SWSRS\_NSafR\_SecR\_B\_023

The communication protocol and the corresponding Ethernet port or serial port which CM supported is shown in Table 4-1, and the "-" means not supported. CM can identify different PC software, and can be configured as a redundant network interface.

CM支持的通讯协议类型及相应的以太网口或串口如下表所示，其中“—”表示不支持。CM能够识别不同的上位机软件，并可配置为冗余网口。

Table 4-1 CM communication protocal type

表4-1 CM通讯协议类型

|  |  |  |  |
| --- | --- | --- | --- |
| No.  序号 | Protocl or device  协议或设备 | Ethernet port  支持的以太网口 | serial port  支持的串口 |
| 1 | CS1131 | NET1，NET2 | — |
| 2 | OPC Server | NET1，NET2 | — |
| 3 | HMI | NET1，NET2 | — |
| 4 | diagnostic software  诊断软件 | NET1，NET2 | Port 5（USB转串口） |
| 5 | SOE software  SOE软件 | NET1，NET2 | — |
| 6 | AMS | NET1，NET2 | — |
| 7 | Peer-to-Peer | NET1，NET2 | — |
| 8 | Modbus Slave (RTU/ASCII) | — | Port 1-4 |
| 9 | Modbus Master (RTU/ASCII) | — | Port 1-4 |
| 10 | Modbus Master or Slave | NET1，NET2 | — |
| 11 | NTP/SNTP timing  NTP/SNTP 校时 | NET2 | — |
| 12 | GPS timing  GPS校时 | — | Port 4 |

## SOE function SOE功能

### Hard SOE record 硬SOE记录

SWSRS\_NSafR\_SecR\_A\_024

Support to collect SOE records from DI module、AI module、OSP module，and provide SOE record to SOE software.

支持从DI模块、AI模块、OSP模块收集SOE记录，并能将SOE记录提供给上位机SOE软件。

### Soft SOE record 软SOE记录

SWSRS\_NSafR\_SecR\_A\_025

Support to record SOE from the change of the BOOL variables，and provide SOE record to SOE software.

The BOOL type variable is labeled as ‘SOE variable’ in the configuration software by user. PM records SOE of the states change of these variables, and the accuracy of soft [SOE](http://cn.bing.com/dict/search?q=SOE&FORM=BDVSP6&mkt=zh-cn) is 1 control cycle.

支持对内部BOOL类型变量做SOE记录，并能将SOE记录提供给上位机SOE软件。

使用者在组态软件上配置BOOL类型变量是否为SOE点，PM将这些变量的跳变信息记录为SOE，精度为一个控制周期。

### The capacity of SOE SOE容量

SWSRS\_NSafR\_SecR\_B\_026

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

三系各自保存SOE记录，每系的记录总数为612万条，其中，掉电保持的条数为500020000条。

### SOE group SOE分组

SWSRS\_NSafR\_SecR\_A\_027

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.

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；硬SOE和软SOE不能设置在一个组内。

### SOE read SOE读取

SWSRS\_NSafR\_SecR\_A\_028

SOE software can read SOE records from one PM or three PMs.

上位机SOE软件可读取一系或者三系的SOE记录。

## Source project backup 源文件备份

SWSRS\_NSafR\_SecR\_A\_029

The configuration software can download, upload and clear the source project.

The CM stores the source project in FLASH, to ensure that the source project is maintained after power-off.

This function is independent of the key switch position, it means the source project files will not be cleared if the key switch is in the ‘Init’ position when the system power on.

组态软件可下载、上传、清除源工程文件。

CM中的FLASH保存组态软件下载的源工程文件，不会因为模块掉电丢失。

钥匙开关的init档位和源文件备份功能无关，即上电时钥匙开关在init档位不会导致源工程文件丢失。

## IP configuration IP配置

### IP address setting IP地址配置

SWSRS\_NSafR\_SecR\_C\_030

The default IP address of Ethernet port 1 in CM is 192.168.1.0192.168.0.1, and the default IP address of Ethernet 2 is 192.168.1.1. These address can be configured with the configuration software or diagnostic software by user, and can be read with the configuration software.

The default IP address will be recovered after power on if the key switch is in the ‘Init’ position.

CM上以太网口1的IP地址默认为192.168.1.0192.168.0.1，以太网口2的IP地址默认为192.168.1.1，工程人员可通过组态软件或者诊断软件对IP地址进行配置，可通过诊断软件读取目前的IP地址。

如果上电时钥匙开关在init档位，上电后恢复默认IP地址。

### IP Access Control IP访问控制

SWSRS\_NSafR\_SecR\_B\_032

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。

## Network Storm Protect 防网络风暴

SWSRS\_NSafR\_SecR\_A\_031

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。

## Timing 校时

### Timing Function Block 功能块校时

SWSRS\_NSafR\_SecR\_A\_033

Support timing function block, and source of the block can be DI, Modbus input or user debug command.

提供校时功能块，校时使能源可以来自于DI输入、Modbus输入或者用户的调试命令。

### NTP/SNTP Timing NTP/SNTP校时

SWSRS\_NSafR\_SecR\_B\_034

CM can be slave station of the NTP/SNTP, so it can accept timing command of the NTP/SNTP timing master.

CM can be master station of the NTP/SNTP, so it can send timing command to other control stations as a timing source.

CM可作为NTP/SNTP的从站，接受NTP/SNTP校时源的校时命令。

CM可作为NTP/SNTP的主站，作为校时源给其他控制站校时。

### GPS Timing GPS直接校时

SWSRS\_NSafR\_SecR\_A\_035

CM support GPS timing through serial port.

CM支持GPS通过串口校时。

## Variables On-line Monitor 变量在线监视

### Variables Monitor by Configuration Software 组态软件变量监视

SWSRS\_NSafR\_NSecR\_A\_036

Control station will upload variables value cyclicly, which was assigned by the configuration software.

控制站根据组态软件指定需求监视的变量，周期性上传监视数据。

### Oscilloscope 示波器

SWSRS\_NSafR\_NSecR\_A\_037

PM record variables value in every control cycle or in several control cycles, and the user can assign variables which need to be recorded and its record interval. The recorded information can be displayed by the configuration software.

PM按单个控制周期间隔或者多个控制周期间隔记录部分变量的值，变量的指定、记录间隔的设置由使用者通过组态软件配置，记录信息可提供给组态软件显示。

### Variables Monitor by OPC Software OPC软件变量监视

SWSRS\_NSafR\_NSecR\_A\_038

Control station will upload variables value cyclicly, which was assigned by the OPC software.

控制站根据OPC软件指定需求监视的变量，周期性上传监视数据。

## Modbus

### Modbus Protocol Modbus协议

SWSRS\_NSafR\_NSecR\_B\_039

Modbus protocol will be used to realize the communication between the control station and the third party systems.

* Support Modbus RTU Master and Slave.
* Support Modbus ASCII Master and Slave.
* Support Modbus TCP Client/Server.

Modbus协议用于实现控制站与第三方系统间的通讯。

* 支持Modbus RTU主从。
* 支持Modbus ASCII主从。
* 支持Modbus TCP Client/Server。

### Modbus Application Modbus应用

SWSRS\_NSafR\_NSecR\_A\_040

Modbus input variable can be used to calculate in the PM user program or only displayed by the PC software.

Modbus输入变量可参与PM用户程序运算，或者只用于上位机显示。

### Modbus Start/Stop Modbus启停

SWSRS\_NSafR\_SecR\_B\_041

As a Modbus master/Modbus TCP Server, the access of every slave station can be started or stopped independently. As a Modbus slaveModbus TCP Client, whether it can be accessed by the masterServer can be controlled.

作为Modbus主站或者Modbus TCP Server时，对每个从站的访问可单独控制启停。作为Modbus从站Modbus TCP Client时，可控制能否被主站Server访问。

### Data Type 数据类型

SWSRS\_NSafR\_NSecR\_A\_042

The protocal support Bool, Word, Real and Long Real type, and the byte order of Real and Long Real type can be set using configuration software. As a Modbus master, the total communication data size for all its modbus slave stations is 4k.

支持Bool、Word、Real、Long Real、DWORD类型，其中Real、Long Real、DWORD类型的字节顺序可通过组态软件配置。作为Modbus主站时，和从站通讯的变量总大小为4k。

### Port access control 端口权限控制

SWSRS\_NSafR\_SecR\_A\_043

As a Modbus slave, the port authority (read-only or read/write) can be configured using the Configuration software.

作为Modbus从站时，可通过组态软件配置为只读或者读写。

## Indicators指示灯

### CM Indicators CM指示灯

SWSRS\_NSafR\_NSecR\_B\_044

CM's indicators are described as below, and the indicators as PASS, FAULT, ACTIVE, CM\_BUS are controlled by the embedded software.

CM的状态灯描述如下，其中PASS、FAULT、ACTIVE、CM\_BUS由嵌入式软件控制灯的状态：

Table 4-2 Communication Module indicators

表4-2 通讯模块指示灯定义

|  |  |  |  |
| --- | --- | --- | --- |
| Name  名称 | Color  颜色 | Status  状态 | Meaning  含义 |
| POWER | Green  绿色 | On  亮 | The module is powered on.  模块上电 |
| Off  灭 | The module is powered off.  模块掉电 |
| Flash  闪 | Undefined.  未定义 |
| PASS | Green  绿色 | On  亮 | The module self-test passed.  模块自检通过 |
| Off  灭 | The module self-test failed.  模块自检失败 |
| Flash  闪 | Undefined.  未定义 |
| FAULT | Red  红色 | On  亮 | The module has detected faults.  模块故障 |
| Off  灭 | The module has not detected faults.  模块无故障 |
| Flash  闪 | Network upgrade.  在线升级 |
| ACTIVE | Yellow  黄色 | On  亮 | The module has a project.  有工程，正常运行 |
| Off  灭 | The module does not have a project.无工程 |
| Flash  闪 | Undefined.  未定义 |
| CM\_BUS | Yellow  黄色 | On  亮 | Undefined.  未定义 |
| Off  灭 | No communication on CM\_BUS.  无通讯 |
| Flash  闪 | CM\_BUS communication in processing.  通讯过程中 |
| PULSE | Yellow  黄色 | On  亮 | Timing pulse is normal.  校时脉冲正常 |
| Off  灭 | No timing pulse or timing pulse is abnormal.  无校时脉冲或校时脉冲不正常 |
| Flash  闪 | Undefined.  未定义 |
| NET1  TX RX | Yellow  黄色 | On  亮 | Link is normal, and no data exchange.  链接正常，无数据交换 |
| Off  灭 | No link.  无链接 |
| Flash  闪 | Data exchange in processing.  有数据交换 |
| NET2  TX RX | Yellow  黄色 | On  亮 | Link is normal, and no data exchange.  链接正常，无数据交换 |
| Off  灭 | No link.  无链接 |
| Flash  闪 | Data exchange in processing.  有数据交换 |
| COM1  TX RX | Yellow  黄色 | On  亮 | Undefined.  未定义 |
| Off  灭 | No communication.  无通讯 |
| Flash  闪 | TX1：Send data；RX1：Receive data  TX1：发送数据；RX1：接收数据 |
| COM2  TX RX | Yellow  黄色 | On  亮 | Undefined.  未定义 |
| Off  灭 | No communication.  无通讯 |
| Flash  闪 | TX2：Send data；RX2：Receive data  TX2：发送数据；RX2：接收数据 |
| COM3  TX RX | Yellow  黄色 | On  亮 | Undefined.  未定义 |
| Off  灭 | No communication.  无通讯 |
| Flash  闪 | TX3：Send data；RX3：Receive data  TX3：发送数据；RX3：接收数据 |
| COM4  TX RX | Yellow  黄色 | On  亮 | Undefined.  未定义 |
| Off  灭 | No communication.  无通讯 |
| Flash  闪 | TX4：Send data；RX4：Receive data  TX4：发送数据；RX4：接收数据 |
| DEBUG  TX，RX  5 | Yellow  黄色 | On  亮 | Undefined.  未定义 |
| Off  灭 | No communication.  无通讯 |
| Flash  闪 | TX5：Send data；RX5：Receive data  TX5：发送数据；RX5：接收数据 |

### PM Indicators PM指示灯

SWSRS\_NSafR\_NSecR\_B\_045

PM's indicators are described as below, and the indicators as PASS、FAULT、ACTIVE、SYNC、FORCE、INIT、RUN、PROG、STOP、CM\_BUS、PM\_BUS are controlled by the embedded software.

PM的状态灯描述如下，其中PASS、FAULT、ACTIVE、SYNC、FORCE、INIT、RUN、PROG、STOP、CM\_BUS、PM\_BUS由嵌入式软件控制灯的状态：

Table 4-3 PM indicators

表4-3 主处理器指示灯

|  |  |  |  |
| --- | --- | --- | --- |
| Name  名称 | Color  颜色 | Status  状态 | Meaning  含义 |
| POWER | Green  绿色 | On  亮 | The module is powered on.  模块上电 |
|  |  | Off  灭 | The module is powered off.  模块掉电 |
|  |  | Flash  闪 | Undefined.  未定义 |
| PASS | Green  绿色 | On  亮 | The module self-test passed.  模块自检通过 |
|  |  | Off  灭 | The module self-test failed.  模块自检失败 |
|  |  | Flash  闪 | Undefined.  未定义 |
| FAULT | Red  红色 | On  亮 | The module has detected faults.  模块故障 |
|  |  | Off  灭 | The module has not detected faults.  模块无故障 |
|  |  | Flash  闪 | Network upgrade  在线升级 |
| ACTIVE | Yellow  黄色 | On  亮 | The module has a project, and is executing user program.  有工程，正常运行 |
|  |  | Off  灭 | The module does not have a project.  无工程 |
|  |  | Flash  闪 | The module has a project, but has stopped executing user program.  有工程，停止运行 |
| SYNC | Yellow  黄色 | On  亮 | [Synchronization](http://cn.bing.com/dict/search?q=Synchronization&FORM=BDVSP6&mkt=zh-cn) is [complete](http://cn.bing.com/dict/search?q=complete&FORM=BDVSP6&mkt=zh-cn)d.  同步完成 |
|  |  | Off  灭 | [Synchronization](http://cn.bing.com/dict/search?q=Synchronization&FORM=BDVSP6&mkt=zh-cn) [has](http://cn.bing.com/dict/search?q=has&FORM=BDVSP6&mkt=zh-cn) [not](http://cn.bing.com/dict/search?q=not&FORM=BDVSP6&mkt=zh-cn) started.  同步尚未开始 |
|  |  | Flash  闪 | [Synchronization](http://cn.bing.com/dict/search?q=synchronization&FORM=BDVSP6&mkt=zh-cn) is [in](http://cn.bing.com/dict/search?q=in&FORM=BDVSP6&mkt=zh-cn) [progress](http://cn.bing.com/dict/search?q=progress&FORM=BDVSP6&mkt=zh-cn).  同步进行中 |
| FORCE | Yellow  黄色 | On  亮 | A variable has been disabled.  有变量被强制 |
|  |  | Off  灭 | No variable has been disabled.  无变量被强制 |
|  |  | Flash  闪 | Undefined.  未定义 |
| INIT | Yellow  黄色 | On  亮 | The keyswitch is in the ‘Init’ position.  钥匙开关在Init状态 |
|  |  | Off  灭 | The keyswitch is not in the ‘Init’ position.  钥匙开关未在Init状态 |
|  |  | Flash  闪 | Undefined.  无定义 |
| RUN | Yellow  黄色 | On  亮 | The keyswitch is in the ‘Run’ position.  钥匙开关在Run状态 |
|  |  | Off  灭 | The keyswitch is not in the ‘Run’ position.  钥匙开关未在Run状态 |
|  |  | Flash  闪 | Undefined.  无定义 |
| PROG | Yellow  黄色 | On  亮 | The keyswitch is in the ‘Prog’ position.  钥匙开关在Prog状态 |
|  |  | Off  灭 | The keyswitch is not in the ‘Prog’ position.  钥匙开关未在Prog状态 |
|  |  | Flash  闪 | Undefined.  无定义 |
| STOP | Yellow  黄色 | On  亮 | The keyswitch is in the ‘Stop’ position.  钥匙开关在Stop状态 |
|  |  | Off  灭 | The keyswitch is not in the ‘Stop’ position.  钥匙开关未在Stop状态 |
|  |  | Flash  闪 | Undefined.  无定义 |
| IP\_BUS | Yellow  黄色 | On  亮 | Undefined.  未定义 |
|  |  | Off  灭 | No communication on IP\_BUS.  无通讯 |
|  |  | Flash  闪 | IP\_BUS communication is in processing.  通讯过程中 |
| CM\_BUS | Yellow  黄色 | On  亮 | Undefined.  未定义 |
|  |  | Off  灭 | No communication on CM\_BUS.  无通讯 |
|  |  | Flash  闪 | CM\_BUS communication is in processing.  通讯过程中 |
| PM\_BUS | Yellow  黄色 | On  亮 | Undefined.  未定义 |
|  |  | Off  灭 | No communication on PM\_BUS, or the bus has detected a fault.  无通讯，或存在PM\_BUS故障 |
|  |  | Flash  闪 | PM\_BUS has not detected a fault in communication process.  通讯过程中，两条PM\_BUS正常 |
| TX1，RX1 | Yellow  黄色 | On  亮 | Undefined.  未定义 |
|  |  | Off  灭 | No communication.  无通讯 |
|  |  | Flash  闪 | TX1：Send data；RX1：Receive data  TX1：发送数据；RX1：接收数据 |

## Diagnostic function 诊断功能

### Debug interface 调试接口

SWSRS\_NSafR\_SecR\_A\_046

The debug interface is mainly used for reading internal fault information and internal log information of CM and PM. This debug interface only can be used by developers.

The interface uses serial port as a medium.

私有调试接口主要用于对CM、PM的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。

### Memory usage diagnostic 内存使用率诊断

SWSRS\_NSafR\_SecR\_A\_047

The control station monitors memory usage in real-time, and this information can be provided to the diagnostic software.

实时检测内存使用率，该信息能够提供给诊断软件。

### CPU load diagnostic CPU负荷诊断

SWSRS\_NSafR\_SecR\_A\_048

The control station monitors CPU load in real-time, and this information can be provided to the diagnostic software.

实时检测CPU负荷，该信息能够提供给诊断软件。

### System Net load diagnostic System Net网络负荷诊断

SWSRS\_NSafR\_SecR\_A\_049

The control station monitors the load of System Net in real-time, and this information can be provided to the diagnostic software.

实时检测System Net网络负荷，该信息能够提供给诊断软件。

### CM\_BUS status diagnostic CM\_BUS故障诊断

SWSRS\_NSafR\_SecR\_A\_050

The control station monitors the status of CM\_BUS in real-time, and this information can be provided to the diagnostic software.

实时检测CM\_BUS网络状况，该信息能够提供给诊断软件。

### PM\_BUS status diagnostic PM\_BUS故障诊断

SWSRS\_NSafR\_SecR\_A\_051

The control station monitors the status of PM\_BUS in real-time, and this information can be provided to the diagnostic software.

实时检测PM\_BUS网络状况，该信息能够提供给诊断软件。

### Safety Net status diagnostic Safety Net故障诊断

SWSRS\_NSafR\_SecR\_A\_052

The control station monitors the status of Safety Net in real-time, and this information can be provided to the diagnostic software.

实时检测Safety Net网络状况，该信息能够提供给诊断软件。

### IP\_BUS status diagnostic IP\_BUS故障诊断

SWSRS\_NSafR\_SecR\_A\_053

The control station monitors the status of IP\_BUS in real-time, and this information can be provided to the diagnostic software.

实时收集IP\_BUS网络状况，该信息能够提供给诊断软件。

### CM status diagnostic CM状况诊断

SWSRS\_NSafR\_SecR\_A\_054

The control station monitors the status of CM in real-time, and this information can be provided to the diagnostic software.

实时检测CM运行状况，该信息能够提供给诊断软件。

### PM status diagnostic PM状况诊断

SWSRS\_NSafR\_SecR\_A\_055

The control station monitors the status of PM in real-time, and this information can be provided to the diagnostic software.

实时检测PM运行状况，该信息能够提供给诊断软件。

### PW status diagnostic PW状况诊断

SWSRS\_NSafR\_SecR\_A\_056

The control station monitors the status of PW in real-time, and this information can be provided to the diagnostic software.

实时读取PW的运行状况，该信息能够提供给诊断软件。

### IO module status diagnostic IO状况诊断

SWSRS\_NSafR\_SecR\_B\_057

The control station can scan the module information before the module is configured, and monitors the status of IO module in real-time after the module is configured, and this information can be provided to the diagnostic software.

上电后系统未做硬件配置时支持对本系统内所安装模块的扫描识别，系统完成硬件配置后实时收集IO模块运行状况，该信息能够提供给诊断软件。

### Diagnostic information clear 诊断清除

SWSRS\_NSafR\_NSecR\_A\_021

The system supports the user to clear the diagnostic information using diagnostic software.

支持用户对部分诊断信息进行清除处理。

### Safety parameters information 安全参数信息

SWSRS\_NSafR\_NSecR\_A\_022

The information as IO module status, IO module fault record (with time stamp), UP running information (with time stamp) which is related with safety parameters can be provided to the configuration software.

This information can be used by configuration software to calculate the safety parameters.

上报PM及IO模块的状态及故障信息（带时间戳）、UP的运行状态及变化信息（带时间戳）给组态软件，可用于组态软件进行安全参数计算。

## Log 日志

### Log capacity 日志容量

SWSRS\_NSafR\_SecR\_B\_058

Each PM, CM can save the lateset 10000 log records.

PM、CM各自保存最近的10000条日志记录。

PM can save the lateset 30000 log records. CM can save the lateset 10000 log records.

PM保存最近的30000条日志记录，CM保存最近的10000条日志记录。

### Log content 日志内容

SWSRS\_NSafR\_SecR\_A\_059

The important operation information and all kinds of exception information need to be recorded in the log, include: power on records, fault records, download records and debug records, etc.

日志中需要记录关键运行信息和各种异常信息，主要包括：上电记录、故障记录、组态下装及调试记录等。

### Power lost retention 日志掉电保持

SWSRS\_NSafR\_SecR\_C\_060

The latest 1000 important log will not be lost after PM power off. The important log include power on records, fault records, access control (entry and exit), download and debugging records, etc. If the module has been pulled out, the retained log is lost.

日志记录中最近的1000条关键日志具有掉电保持功能，不会因为模块掉电而丢失。上电记录、故障记录、访问控制（登录和退出）、组态下装和调试记录等为关键日志。模块拔插后日志不保持。

### Log read 日志读取

SWSRS\_NSafR\_SecR\_B\_061

User can read log from each PM or CM by diagnostic software. 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%.

The log can not be modify by diagnostic software, but can be cleared by diagnostic software.

使用上位机诊断软件，可读取指定PM或CM的日志记录。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%。

不支持诊断软件对日志的修改；支持诊断软件清除日志。

## Performance 性能

### The scale of control station 控制站规模

SWSRS\_SafR\_NSecR\_A\_062

One control station supports a maximum of 16 PCs (includes engineer station, operator station, SOE station and diagnostic station). System supports a maximum of 64 control station.

系统中最多支持16个上位机（包括工程师站、操作员站、SOE站、诊断站、AMS站），最多支持64个控制站。

### System network load 系统网负荷

SWSRS\_NSafR\_NSecR\_A\_063

In the case of 100Mbps Ethernet, the load of system network is less than 40% when system is in normal running. System normal running does not include the status as download process, system restart process, etc.

在采用100Mbps以太网情况下，系统正常运行过程中，系统网负荷小于40%。系统正常运行过程不包括组态软件下装、系统重启过程等。

### Power-on time 上电时间

SWSRS\_NSafR\_NSecR\_A\_064

The power on time of PM is less than 2 minutes, and the power on time of CM is less than 2 minutes. Power-on time is the interval between the module power-on completed to the module self-check completed.

CM、PM的上电时间应不大于32min。上电时间是指从模块电源端口上电完成到模块自检完成之间的时间。

## Upgrade via network 现场升级

### Upgrade software via network 软件网络升级

SWSRS\_NSafR\_NSecR\_A\_065

Firmware, OS, FPGA of CM/PM can be upgraded by diagnostic software via System Net. The new firmware will be checked while upgrading. The new firmware will not take effect immediately until the system power-on again. Before this, the system keeps using the original firmware.

PM can receive the upgrade data of IO module from diagnostic software and send it to IO modules.

上位机诊断软件通过System Net升级CM、PM中的FW、OS、FPGA，升级时需进行数据校验。升级后的版本在系统重新上电后才会加载生效，在此之前，系统继续使用原来的软件运行。

PM将上位机诊断软件下发的IO模块升级数据发送给对应IO模块，用于该模块的网络升级。

### Version record 版本记录

SWSRS\_NSafR\_SecR\_B\_066

CM and PM record the version of firmware, OS, FPGA, CPLD and hardware and Power\_MCU information. These information can be provided to the configuration software and diagnostic software.

PM can get the version of firmware, FPGA, CPLD and hardware information from IO modules, and provided it to the configuration software and diagnostic software.

CM、PM记录本模块上的FW、OS、FPGA、CPLD和Power\_MCU的版本号，该信息能够提供给组态软件及诊断软件。

支持从IO模块读取模块固件、FPGA、CPLD、硬件的版本号，并提供给组态软件及诊断软件。

——以下无正文

The last requirement number is SWSRS\_NSafR\_NSecR\_A\_069

本文档最后一个需求编号为SWSRS\_NSafR\_NSecR\_A\_069