|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | | | |  | | | | |  | | | | | | |  | | | | | | |  | | | | | | |  | | | | | | |  | | | | | | | | | | |
| {#r\_r\_1}{r} |  | | | | | {st} | | | | | {d\_b} | | | | | | | {c\_b} | | | | | | | {r\_b} | | | | | | | {a\_b} | | | | | | | {observation}{/r\_r\_1} | | | | | | | | | | |
| **版本** | **日期** | | | | | **状态** | | | | | **编写** | | | | | | | **校核** | | | | | | | **审核** | | | | | | | **批准** | | | | | | | **修改说明** | | | | | | | | | | |
| **GUANGDONG YANGJIANG**  **NUCLEAR POWER PROJECT UNIT 5&6**  **广东阳江核电站5,6号机组** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **文件编码** | | **{i0}** | | **{i1}** | | | **{i2}** | | **{i3}** | | | **{i4}** | | | **{i5}** | | **{i6}** | | | **{i7}** | | | **{i8}** | | | **{i9}** | | **{i10}** | | | **{i11}** | | **{i12}** | | **{i13}** | | | **{i14}** | | | **{i15}** | | **{i16}** | | **{i17}** | | **{i18}** | |  |
| **题目：**  **{t}** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 参考文件  编码  参考文件名称 | | |  |  |  | | |  | |  | | |  |  | |  | | |  | |  |  | |  | | |  | |  |  | |  | |  | |  |  | | | Rev | |  | | 文件类型 | | A类 | |  | |
|  | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |  | |  | |
| B类 | |  | |
| C类 | | X | |
| logo    核能 北京广利核系统工程有限公司  **Nuclear Power China Techenergy Co.,Ltd**    内部编码： {i\_s} | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| This document is the property of the issuer. It must not be used, reproduced transmitted or disclosed without the prior written permission of the issuer for other purpose than YJ Project Unit 5&6 DCS. 本文件的版权属于出版者，未获出版者的书面许可，任何人不得擅自在阳江5&6号机组DCS项目以外使用、复制、传递和泄露该文件。 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **北京广利核系统工程有限公司**  **技 术 文 件** | | | | | | | | | | | | |
| **文件名称**： {t}  **文件编号**： {i\_s}  **项目名称**： 阳江5&6号机组DCS项目的安全级DCS项目  **项目编号**： NPD1309002-1  **物料编码**：无  **受控标识**：受控  **第 1 册**  **共** {pages} **页**  **共**  1 **册** | | | | | | | | | | | | |
| **版本** | | **状态** | | **编写** | | **审核** | **审定** | | **批准** | | **批准日期** | |
| **{#r\_r\_3}{r}** | | **{st}** | | **{d\_b}** | | **{c\_b}** | **{r\_b}** | | **{a\_b}** | | **{/r\_r\_3}** | |
|  | |  | |  | |  |  | |  | |  | |
| **相关部门/人员会签：** | | | | | | | | | | | | |
| **发**  **布**  **范**  **围** | DCS项目 | | 项目管理组 | | 质量保证组 | | | 商务组 | | 结构件专项小组 | | |
| DCS项目  子项目1 | | 项目管理组 | | 工程组 | | | 生产组 | | 产品组 | | 系统组 |
| DCS项目  子项目2 | | 项目管理组 | | 工程设计组 | | | 工程成套组 | | 工程QC组 | | 硬件QC组 |
| 质量鉴定组 | | 非安平台组 | | | 应用开发组 | | 生产中心 | | BUP专项小组 |
| V&V项目 | | 项目管理组 | | 测试组 | | | 评估分析组 | |  | |  |

**修订页**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 编号 | 版本 | 状态 | 修订日期 | 修订章节 | 修订内容 |
| {#r\_r\_4}{no} | {r} | {st} | {date} |  | {observation}{/r\_r\_4} |

**目 录**

[1 概述 6](#_Toc460242849)

[1.1 目的 6](#_Toc460242850)

[1.2 参考文件 6](#_Toc460242851)

[1.3 文档位置 6](#_Toc460242852)

[2 缩略语和术语 7](#_Toc460242853)

[2.1 缩略语 7](#_Toc460242854)

[2.2 术语 8](#_Toc460242855)

[3 系统描述 8](#_Toc460242856)

[3.1 系统介绍 8](#_Toc460242857)

[3.2 各子系统结构要求 10](#_Toc460242858)

[3.2.1 反应堆停堆保护子系统 10](#_Toc460242859)

[3.2.2 专设安全设施驱动系统 13](#_Toc460242860)

[3.2.3 安全相关子系统 15](#_Toc460242861)

[3.2.4 设备接口子系统 16](#_Toc460242862)

[3.2.5 堆芯冷却监测系统 18](#_Toc460242863)

[3.2.6 报警处理系统 19](#_Toc460242864)

[3.2.7 网关系统 19](#_Toc460242865)

[3.2.8 安全控制显示系统 20](#_Toc460242866)

[3.3 接口要求 21](#_Toc460242867)

[4 设计要求 21](#_Toc460242868)

[4.1 可维护性 21](#_Toc460242869)

[4.2 可测试性 22](#_Toc460242870)

[4.3 隔离要求 22](#_Toc460242871)

[4.4 信号分配要求 22](#_Toc460242872)

[4.5 柜内布置要求 23](#_Toc460242873)

[5 产品规格 23](#_Toc460242874)

[5.1 平台产品 23](#_Toc460242875)

[5.2 机柜规格 23](#_Toc460242876)

[5.3 专用装置 23](#_Toc460242877)

[5.3.1 测试面板 23](#_Toc460242878)

[5.3.2 旁通面板 24](#_Toc460242879)

[5.4 线缆 24](#_Toc460242880)

[5.4.1 线缆材料 24](#_Toc460242881)

[5.4.2 线缆颜色 24](#_Toc460242882)

[5.4.3 线径 25](#_Toc460242883)

[5.4.4 布线要求 25](#_Toc460242884)

[5.4.5 线缆及装置排布要求 26](#_Toc460242885)

[5.5 COTS 26](#_Toc460242886)

[6 环境要求 26](#_Toc460242887)

[6.1 周围环境 26](#_Toc460242888)

[6.2 抗震要求 27](#_Toc460242889)

[6.3 噪声和浪涌防御 27](#_Toc460242890)

[7 性能要求 27](#_Toc460242891)

[7.1 响应时间 27](#_Toc460242892)

[7.2 精度 27](#_Toc460242893)

[7.3 可靠性 28](#_Toc460242894)

[7.3.1 MTBF 28](#_Toc460242895)

[7.3.2 MTTR 28](#_Toc460242896)

[7.3.3 可用性 28](#_Toc460242897)

[7.4 裕量要求 28](#_Toc460242898)

[8 供电接地要求 28](#_Toc460242899)

[8.1 系统供电规格 28](#_Toc460242900)

[8.2 系统接地规格 28](#_Toc460242901)

[9 标识要求 29](#_Toc460242902)

[9.1 机柜标识 29](#_Toc460242903)

[9.2 设备标识 30](#_Toc460242904)

[9.3 线缆标识 32](#_Toc460242905)

# 概述

本文档对阳江5、6号机组控制保护系统的硬件设计提供需求，规定了各子系统的硬件范围和结构、性能要求，以及硬件设计须完成的内容以及相关要求。

## 目的

本文档依据系统设计完成的各子系统设计说明书，设计专项方案，对保护系统硬件设备、装置需求进行归纳与整理，以指导后续的各子系统硬件设计工作。

本文档作为后续系统硬件设计的主要依据，阅读对象为工程设计、系统测试和产品V&V等人员。

## 参考文件

|  |  |
| --- | --- |
| 参考文件编号 | 参考文件名称 |
| PYZ57110001EIYK44DS | RPS System RequirementSpecification |
| PYZ17000029W00A45GN | UNIT5&6安全级DCS RPS总体设计说明书 |
| PYZ17000033W00A45GN | UNIT5&6安全级DCS RPS反应堆停堆保护系统设计说明书 |
| PYZ17000034W00A45GN | UNIT5&6安全级DCS RPS专设安全设施驱动系统设计说明书 |
| PYZ17000035W00A45GN | UNIT5&6安全级DCS RPS安全相关系统设计说明书 |
| PYZ17000036W00A45GN | UNIT5&6安全级DCS RPS设备接口系统设计说明书 |
| PYZ17000041W00A45GN | UNIT5&6安全级DCS RPS安全控制显示系统设计说明书 |
| PYZ17000043W00A45GN | UNIT5&6安全级DCS RPS定期试验方案设计说明书 |
| PYZ17000045W00A45GN | UNIT5&6安全级DCS RPS隔离设计说明书 |
| PYZ17000049W00A45GN | UNIT5&6安全级DCS RPS旁通方案设计说明书 |
| PYZ17000037W00A45GN | UNIT5&6安全级DCS RPS堆芯冷却监测系统设计说明书 |
| PYZ17000038W00A45GN | UNIT5&6安全级DCS RPS报警处理系统设计说明书 |
| PYZ17000039W00A45GN | UNIT5&6安全级DCS RPS网关系统设计说明书 |
| PY557110001W00A44DS | UNIT5 安全级DCS设计输入文件基线 |
| PY657110001W00A44DS | UNIT6 安全级DCS设计输入文件基线 |

## 文档位置

本文档在系统生命周期中的位置如下图所示，图中红框部分为本文档位置。



图1 在生命周期中的位置

# 缩略语和术语

## 缩略语

| 简称 | 英文名称 | 中文名称 |
| --- | --- | --- |
| AI | Analog Input | 模拟量输入模块 |
| AO | Analog Output | 模拟量输出模块 |
| CCMC | Core Cooling Monitoring Cabinet | 堆芯冷却监视机柜 |
| CCMS | Core Cooling Monitoring System | 堆芯冷却监视系统 |
| CIM | Component Interface Module | 设备接口模块 |
| COTS | Commercial Off The Shelf | 商品级物项 |
| DCS | Distributed Control System | 集散控制系统 |
| DI | Digital Input | 数字量输入模块 |
| DO | Digital Output | 数字量输出模块 |
| ECP | Emergency Control Panel | 紧急控制盘 |
| GW | Gateway | 网关 |
| ESFAS | Engineered Safety Feature Actuation System | 专用安全设施驱动系统 |
| HNU | High-Speed Net Communication Unit | 高速网络通信单元 |
| LNU | Low-Speed Net Communication Unit | 低速网络通信单元 |
| MPU | Main Processing Unit | 主处理单元 |
| MTBF | Mean Time Between Failures | 平均无故障时间 |
| MTTR | Mean Time To Repair | 平均修理时间 |
| NC | Not Classified | 非安全级 |
| OWP | Operator Work Place | 操作员工作站 |
| PDC | Power Distribution Cabinet | 电源分配机柜 |
| PSC | Power Supply Cabinet | 电源机柜 |
| RPS | Reactor Protection System | 反应堆保护系统 |
| RPC | Reactor Protection Cabinet | 反应堆保护机柜 |
| RTS | Reactor Trip System | 反应度停堆系统 |
| RTB | Reactor Trip Breaker | 反应堆停堆断路器 |
| SCID | Safety Control and Information Device | 安全控制显示设备 |
| SPC | Signal Preprocess Cabinet | 信号预处理机柜 |
| SICS | Safety Information and Control System | 安全信息与控制系统 |
| SR | Safety Related | 安全相关 |
| SRC | Safety Related Cabinet | 安全相关机柜 |
| SRS | Software Requirements Specification | 软件需求规格书 |
| VDU | Visual Display Unit | 显示单元 |
| 1E | Safety Class | 安全级 |

## 术语

硬件：实现应用功能的硬件设备，即构成保护系统的控制机柜，由产品单元，机械结构件，线缆，商品级物项等构成。

# 系统描述

## 系统介绍

基于FirmSys平台的控制保护系统划分为以下子系统：

* 反应堆停堆保护子系统RTS，实现1E级安全功能，由1E级设备实现；
* 专设安全设施驱动子系统ESFAS，实现专设安全设施及支持性系统的控制功能，1E级产品实现；
* 安全相关子系统SRS，执行上游逻辑功能中的SR功能，采用1E级产品实现；
* 设备接口子系统CIS，由采用多样化计算机技术的1E级产品实现；
* 堆芯冷却监视子系统CCMS，由1E级产品实现；
* 安全控制显示子系统SCIS，实现安全人机接口功能，采用1E级数字化设备实现；
* 网关子系统GWS，为NC功能，可以采用非安全级设备实现，需要满足抗震I类要求；
* 维护子系统MTS，完成产品的维护功能，为NC功能，采用非安全级设备实现；
* 事故后监视子系统PAMS，为NC功能，采用非安全级设备实现；
* 安全级报警子系统APS，实现安全逻辑部分的报警功能，为NC功能，采用1E 级产品实现。

控制保护系统的整体结构图如下：



图3.1-1 系统整体结构图

## 各子系统结构要求

### 反应堆停堆保护子系统

#### 系统配置要求

反应堆紧急停堆系统由四重冗余的保护通道构成，每个通道由两个功能完全独立的子组组成，每个子组内部又由两个热备冗余的主处理模块以及单一IO模块组成。四个保护通道的停堆指令分别控制各自的两个停堆断路器，四对停堆断路器以硬件方式连接成四取二表决逻辑结构,控制停堆线圈。系统结构描述如下：

* 外部信号通过信号预处理机柜（SPC）中的调理模块进行信号调理、隔离、分配，转换成4～20mA标准信号输出给IO模块，同时隔离分配给相关系统（如DAS和PAMS等）用于显示和控制；外部开关量信号同样通过SPC中的继电器进行信号隔离、分配输出给IO模块及其他系统；
* 调理后的信号经SPC传至反应堆保护机柜（RPC），通过AI或DI模块采集后进入通道CPU后通过运算阈值比较将模拟量信号转化为数字量信号：当用于停堆时，与来自其它通道的停堆信号进行表决逻辑的计算，同时该信号通过“点对点”通信方式输出给其它通道相应的子组完成同样的表决逻辑计算；当用于驱动安全专设时，该信号同样通过“点对点”通信方式单向传递给专设安全设施驱动系统完成驱动专设功能的相关表决逻辑计算；
* RPC分两个子组，两个子组输出的停堆信号通过硬接线连接成“或”逻辑的结构，硬接线输出给停堆断路器；
* 系统处理的指令通过DO或AO模块输出控制现场设备或至非安全系统参与控制逻辑；
* RPC与接口传输机柜（DTC）采用“点对点”通信方式，用以实现与SCID的操作或指示交互；由于DTC为并行冗余站，来自DTC的操作信号需要根据信号类型分别使用模拟量选择模块和数字量选择模块进行筛选。
* RPC通过“多节点”数据通信方式与安全系统总线连接，通过该总线将报警和显示信号传递到非安全级侧。



图3.2.1.1-1 反应堆停堆保护子系统结构

子组内硬件配置要求如下图所示，每个子组内部又由两个热备冗余的MPU及其外围的网络设备，以及单一IO模块组成。设备支持冗余供电功能，预设维护接口。



图3.2.1.1-2 单子组内硬件配置

蒸汽大气排放阀GCT131VV～133VV的控制功能分别在第II、III和IV通道的保护机柜中实现。其实现逻辑如下图3.2.1.1-3所示，具体描述如下。

* 正常情况下，当蒸汽大气排放阀处于自动控制模式，阀门根据主蒸汽管线压力测量值与压力整定值的偏差信号经调节器进行自动控制，压力整定值可由操纵员手动给定，也可以采用调节器内部设定值。当蒸汽大气排放阀处于手动控制模式，操纵员可以通过操纵员站（OWP）上的安全控制显示设备（SCID）手动控制阀门开度；
* 当操纵员站（OWP）故障时，可通过后备控制盘（BUP）上的安全级常规控制器通过硬接线连接来调整压力整定值或者手动控制阀门，作为操纵员站的后备；
* 此外来自DAS或SAS上的信号也可以直接硬接线至反应堆保护机柜对阀门进行操作，作为安全级DCS的后备；
* 当阀门处于DCS控制时，OWP上的SCID和BUP上的硬手操互相处于跟踪状态，保持双方压力手动设定值和手动操作指令一致，由未处于控制位置的设备跟踪当前处于控制位置的设备的值；
* 当未处于控制位置时，DAS、SAS开度指令需跟踪阀门当前的实际开度，以保证无扰切换。



图3.2.1.1-3 GCT-a多样性控制示意图

#### 系统机柜配置

反应堆紧急停堆系统的机柜分为如下三类：

信号预处理机柜（SPC）：安装调理模块，实现信号的调理、隔离和分配；

反应堆保护机柜（RPC）：安装MPU以及IO模块等数字化产品，采集并处理过程信号，并通过执行保护逻辑产生停堆指令；

电源机柜（PSC）：安装电源模块，提供SPC和RPC所需要的24V或48V直流电源。

各通道的机柜配置如下表格所示。

表格3.2.1.2-1 反应堆紧急停堆系统机柜配置表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 保护通道 | SPC（台） | RPC（台） | PSC（台） | 总计（台） |
| I | 2 | 2 | 1 | 5 |
| II | 2 | 2 | 1 | 5 |
| III | 2 | 2 | 1 | 5 |
| IV | 1 | 2 | 1 | 4 |

### 专设安全设施驱动系统

#### 系统配置要求

ESFAS由两重冗余的序列组成，分别布置在实体隔离的两个不同房间，两个序列功能一致。并且每个序列的专设安全设施驱动系统采用两个并行工作的控制站，采用1/2输出逻辑组合后驱动现场设备。

每个序列由专设安全设施驱动机柜(ESFAC)、数据传输机柜(DTC)、电源供电柜组成。数据传输机柜也采用两个并行工作的控制站。专设安全设施驱动机柜中包含试验接口装置，负责接收来自SRS的试验反馈信号。详细结构如图所示。

图3.2.2.1-1 安全专设系统结构

ESFAC采用基于数字化的DCS来实现，为了保证系统的可靠性，采用并行冗余控制站实现，控制站之间保持独立性。传感器、专用系统、ECP/BUP、SRC的开关量信号通过ESFAS继电器柜隔离分配后分别发送至两个ESFAC控制站进行数据处理。控制站结构如下图。



图3.2.2.1-2 ESFAC机柜设计示意图

DTC执行数据传输功能，采用1E级设备实现。

以A列为例，DTC采用基于数字化的DCS来实现，为1E级设备，为了保证系统的可靠性，采用并行冗余控制站实现，控制站之间保持独立性，控制站结构如图所示。



图3.2.2.1-3 DTC机柜设计示意图

试验接口装置设计接收来自SRC的定期试验反馈信号，传递给维护装置进行定期试验。

以A列为例，试验接口装置执行NC功能，采用1E级设备实现，放置在ESFAC的机柜中。试验接口装置为单CPU配置，为保证故障时不影响环网的正常运行，采用与ESFAC同样的供电方式。试验接口装置结构如图所示。



图3.2.2.1-4 试验接口装置设计示意图

#### 系统机柜配置

ESFAS的机柜分为如下三类：

专设安全设施驱动机柜（ESFAC）：安装主处理模块、通信模块、IO模块等数字化产品，采集和处理过程信号，并产生系统级专设指令；

数据传输机柜（DTC）：将系统状态、现场设备状态、中间计算结果等信息通过DTC传输至控制室或非安全级系统中，并且SCID调节GCT-A阀门指令通过DTC传输到RPC机柜中，同时RPC的状态反馈信号经DTC传递给SCID；

电源机柜（PDC）：安装电源模块，提供ESFAC、DTC及试验接口装置设备所需要的24V直流电源。

各通道的机柜配置如下表所示。

表 3.2.2.2‑1 ESFAS子系统机柜配置表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序列 | ESFAC（台） | DTC(台) | PDC(台) | 总计（台） |
| A | 5 | 1 | 1 | 7 |
| B | 5 | 1 | 1 | 7 |

### 安全相关子系统

#### 系统配置要求

SRS分为两重冗余的独立序列，A列和B列。每个SRC子组采用热备冗余的控制站和单一IO组成，热备冗余的控制站之间实现无扰切换。以A列为例，其结构示意图如下 ：



图 3.2.3.1‑1 A列SRC结构示意图

SRC通过安全总线和ESFAC、SCID、DTC、CCMS进行数据交换。

SRC-A1、SRC-A2、SRC-A3、SRC-B1、SRC-B2、SRC-B3各对应1组CIC机柜，SRC和其对应的CIC机柜之间通过IO总线进行通信。

#### 系统机柜配置

SRS系统机柜配置如下表所示：

| 序列 | 控制柜（台） | 电源柜（台） | 调理柜（台） | 总计（台） | 备注 |
| --- | --- | --- | --- | --- | --- |
| A1 | 1 | 2 | - | 3 | 和CIC-A1共用电源柜，小电源柜 |
| A2 | 1 | 2 | - | 3 | 和CIC-A2共用电源柜，小电源柜 |
| A3 | 1 | 2 | - | 3 | 和CIC-A3共用电源柜，小电源柜 |
| A4 | 1 | 1 | 1 | 3 | 和CCMS-A共用调理和电源柜 |
| B1 | 1 | 2 | - | 4 | 和CIC-B1共用电源柜，小电源柜 |
| B2 | 1 | 2 | - | 4 | 和CIC-B2共用电源柜，小电源柜 |
| B3 | 1 | 2 | - | 4 | 和CIC-B3共用电源柜，小电源柜 |

### 设备接口子系统

#### 系统配置要求

设备接口子系统包括两重冗余的独立序列。其主要组成部分是设备接口模块。

CIS分为两重冗余的独立序列，A列和B列。以A列为例，其结构示意图如下 ：



图 3.2.4.1‑1 A列CIS结构示意图

设备接口模块的质保等级为Q1，设备接口模块为1E级设备。设备接口模块接收来自ESFAC、SRC、DAC、SAC和NC-DCS的指令，这些指令通过优先级管理功能和驱动控制功能进行输出。

设备接口模块采集自诊断信息、试验反馈信息和驱动设备的反馈信息等，并通过通信的形式输出。CIS子系统的设备接口模块原理示意图如图表所示。



图 3.2.4.1‑2 设备接口模块原理示意图

#### 系统机柜配置

CIS系统机柜配置如下表格所示。

表格 3.2.4.2‑1 CIS系统机柜配置表

|  |  |  |
| --- | --- | --- |
| 序列 | 控制柜（台） | 电源柜（台） |
| A | 10 | 和SRC共用 |
| B | 9 | 和SRC共用 |

### 堆芯冷却监测系统

#### 系统配置要求

CCMS系统由冗余的A、B两个序列组成，每个序列的机柜CCMC分别布置在实体隔离的两个不同房间。CCMC采用主备冗余的控制器配置来完成其功能。

其详细的系统结构如下图3.2.5.1‑1所示。



图 3.2.5.1‑1 堆芯冷却监测系统结构

#### 系统机柜配置

CCMS系统各序列的机柜配置如下表格所示。

表格 3.2.5.2‑1 堆芯冷却监测机柜配置表

| 序列 | 控制柜（台） | 电源柜（台） | 调理柜（台） | 总计（台） | 备注 |
| --- | --- | --- | --- | --- | --- |
| A | 1 | - | - | 1 | 和SRC-A4共用调理和电源柜 |
| B | 1 | 1 | - | 2 |  |

### 报警处理系统

#### 系统配置要求

报警处理系统分为A、B两列，每列均采用热备冗余方式，热备CPU和单一IO，分别布置于独立的机柜中。报警处理系统采用FirmSys平台实现，其系统架构如下图3.2.6.1-1所示。



图 3.2.6.1‑1 报警处理系统架构示意图

#### 系统机柜配置

APS系统各序列的机柜配置如下表格所示。

表格 3.2.6.2-1 报警处理系统机柜配置表

|  |  |  |
| --- | --- | --- |
| 序列 | APC（台） | 总计（台） |
| A | 1 | 1 |
| B | 1 | 1 |

### 网关系统

#### 系统配置要求

网关系统包括GW-L1和GW-L2共2对网关，均由并行冗余的两个网关组成；通过环网模块连接入环网，实现与环网内设备之间的通信。冗余的两个网关相互独立，并分别布置于A列和B列的网关柜中。

#### 系统机柜配置

GW系统各序列的机柜配置如下表格所示。

表格 3.2.7.2-1网关系统机柜配置表

|  |  |  |
| --- | --- | --- |
| 序列 | GW（台） | 总计（台） |
| A | 1 | 1 |
| B | 1 | 1 |

### 安全控制显示系统

安全控制显示系统作为保护系统的人机接口，实现设备操作和监视功能。分为A、B两列，每列8个，共16个，分布在OWP、BUP和RSS盘台上，数量和布置如下表：

表格3.2.8-1 SCID位置及数量

|  |  |  |  |
| --- | --- | --- | --- |
| **安装位置** | | **Train A** | **Train B** |
| OWP | NI | 1 | 1 |
| CI | 1 | 1 |
| US | 1 | 1 |
| SE | 1 | 1 |
| BUP | | 2 | 2 |
| RSS | RSS-A | 1 | 1 |
| RSS-B | 1 | 1 |
| 共计 | | 8 | 8 |

SCID在盘台的分布位置如下图：



图3.2.8-1 SCID在OWP的布置示意图



图表3.2.8-2 SCID在BUP上的布置示意图



图3.2.8-3 SCID在RSS上的布置示意图

## 接口要求

保护系统通过IO板卡或通信模块以硬接线和通讯两种数据传输方式同外部系统以及不同子系统间进行接口。各子系统的具体接口要求参见“各子系统设计说明书”系统接口章节。

控制保护系统中应用到硬接线接口主要有：

（1） AI：接收来自现场传感器的模拟量信号；

（2） AO：输出控制调节阀或仪表显示；

（3） DI：接收现场设备的反馈或系统间传递的数字量信号；

（4） DO：输出到停堆断路器、或系统间传递的数字量信号；

（5） CIM：输出控制现场设备；

（6） 热电阻信号：热电阻(RTD)输入信号，含3线制、4线制两种规格；

（7） 热电偶信号：热电偶输入信号；

# 设计要求

## 可维护性

设备产品上提供电源、运行、故障、通信状态以及故障码等报警和显示信号，便于发现和解决故障。

系统应设计相应维护接口及维护设备，以实现对系统的维护功能。

## 可测试性

系统预留测试用接口，设计专用测试装置，实现对系统的定期测试。详见《UNIT5&6安全级DCS RPS定期试验方案设计说明书》。

## 隔离要求

隔离设计要求参见《UNIT5&6安全级DCS RPS隔离设计说明书》。

## 信号分配要求

* 不同安全等级的信号分散布置

根据不同安全等级或独立性要求，将信号分为几种必须隔离的类型（如1E和NC信号、PAMS信号等），不同类型的信号需尽量放在不同的机箱，至少应保证放在不同板卡上。

* 冗余信号分散布置

上游需求中互为冗余（包括逻辑表决）的信号尽量分配到不同的机箱, 至少应保证分配到不同的板卡上。

* 供电方式分散布置

根据信号不同的供电等级要求，设计独立的信号处理机箱。信号供电要求只可以升高，不可以降低，即当空间不够时，三路供电的信号可以放入四路供电的机箱，而不能放入两路供电的机箱。

* 功能分散原则

根据系统的设计要求及信号执行功能进行分析和合理分配布置，满足功能分散等要求，如三个环路对应的IO信号应分配到不同的卡件上，并尽量布置在不同的信号处理机箱；高压安注、中压安注和低压安注相关的设备尽量放在不同的机箱。

* 停堆信号分散原则

一块AI板卡一般分配两个停堆信号的采集，且一般是2/4表决和2/3表决的停堆信号放到一起，尽量避免两个2/3表决信号分配到同一板卡上。

* 互锁旁通信号分开

具有互锁或旁通的信号，应放置在不同的板卡，并尽量布置在不同的机箱，如停堆DO和旁通DO应放在不同的板卡上。

* 相同去向信号集中布置

根据信号的来源去向进行分类，将来源去向一致的信号尽量放在一起，利于走线和布线，如Local、BUP、ECP等。

* 相关信号统一分配

有计算关联的信号应放到同一块AI板卡上，如超温计算的多个AI变量。

* 板卡通道平均分配

与安全功能不直接相关的信号，尽量均布到各个板卡。

* 公共端信号集中布置

拥有公共端的信号应尽量放在同一板卡上，利于接线。

## 柜内布置要求

机柜内设备布置应遵循以下原则：

1）操作设备的布置高度应位于机柜中部，以便于维护人员操作；

2）大功耗电气设备应布置于机柜顶部以避免，由于设备散热量过大而影响相关设备；

3）应考虑设备日后的拆卸维护，设备之间应预留足够的维护空间；

4）柜内布置应充分考虑各设备的及线缆的布置位置，以保证机柜重心居中，不会产生倾斜；

# 产品规格

## 平台产品

各子系统硬件主要由以下几类平台产品构成：

* MPU：实现数据处理与逻辑计算功能，主要负责应用软件的执行；同时具备自身的故障诊断功能；
* IO模块：实现同外部传感器、驱动设备的信号接口；
* HNU、LNU：实现系统内部间或同外部系统间的数据传输功能；
* 信号隔离分配模块；
* 优先处理模块；
* 光电信号转换模块；
* 电源模块；
* 安全显示装置；

关于各类模块的具体规格需求详见相应产品用户手册。

## 机柜规格

系统需使用1E级机柜，抗震I类，质保A级，所选机柜的散热能力应满足柜内设备热功耗要求。

机柜具体规格与设计要求参见安全级机柜设计文件的相关要求。

## 专用装置

根据维护与试验的需求，设计相应的维护旁通面板和测试面板实现相应的功能。

### 测试面板

#### RTB测试面板

停堆断路器动作试验，由RTB试验面板通过RPC的DI接口往RPC注入停堆试验信号，使RPC输出停堆信号，从而使停堆断路器动作。RTB的反馈信号将其动作状态，送到RTB试验面板进行状态指示。

#### 输出控制试验面板

输出控制回路试验采用CIM试验面板进行触发，通过维护工具读取的方式进行。

CIM试验面板以硬接线的形式将试验信号发送到SRC，SRC用DI采集，并通过SN1总线发送给每一个CIM板卡。每个CIM板卡针对并行冗余的ESFAC，内部设计有2个相同的优先级输出逻辑和脉冲产生逻辑。

### 旁通面板

用于维修和试验的旁通包括反应堆紧急停堆系统的通道旁通、参数旁通、专设安全设施驱动系统的专设旁通和SRC旁通。

#### 保护通道旁通面板

旁通面板实现通道旁通和参数旁通的手动操作和显示功能，采用硬接线的接口方式。

旁通面板提供与用户的交互接口的操作面板，旁通面板上显示如下：

* 具有本通道的旁通开关，开关为手动控制，有两个状态，分别是正常状态和旁通状态；
* 具有本通道及其他通道的通道旁通状态指示灯显示，当通道旁通时，指示灯开启；
* 本通道的所有保护参数旁通状态在旁通面板上具有指示灯显示，每个子组分别用一个指示灯指示。

#### 专设旁通面板

为了完成ESFAC输出试验、控制回路试验等定期试验，需要对一个ESFAS序列的一个ESFAC控制器进行旁通，另一个并行冗余的ESFAC控制器以及另一个序列能够提供正常的保护功能，该旁通通过专设旁通面板实现。

#### SRC旁通面板

在维修时，需要将单个SRC控制器退出运行，通过SRC旁通面板实现。SRC旁通即对一个SRC子组旁通，每个SRC子组均设置一个旁通开关，用于旁通本子组SRC，旁通后该SRC退出运行，对应的设备驱动指令闭锁。

## 线缆

### 线缆材料

控制与电源线缆均应采用低烟无卤材料，具备高耐热，阻燃，低烟，无毒。

### 线缆颜色

为了明确识别线缆的功能与归属，区分相关通道与列，各通道或列内的线缆颜色定义如下：

|  |  |
| --- | --- |
| **通道和列** | **线缆颜色** |
| 保护通道 I | 黄色 |
| 保护通道 II | 蓝色 |
| 保护通道 III | 红色 |
| 保护通道 IV | 棕色 |
| A 列 | 橙色 |
| B列 | 绿色 |
| 列间耦合电路 | 黑色 |
| 非安全电路 | 白色 |
| 接地线缆 | 黄绿 |

### 线径

线缆选择应根据信号损耗及压降选择适当的线径，线缆的最大线径受所用设备接口端子压接规格限制。系统所需线缆的种类及线径要求如下：

|  |  |  |
| --- | --- | --- |
| **编号** | **类型** | **最小线径要求** |
| 1 | 交流动力电缆 | 2.5mm2 |
| 2 | 直流动力电缆 | 0.5mm2 |
| 3 | 仪表电缆 | 0.5mm2 |
| 4 | 控制电缆 | 0.5mm2 |
| 5 | 信号线缆 | 0.5mm2 |
| 6 | 接地线 | 2.5mm2 |

注：上表不包含特殊专用线缆。

### 布线要求

柜内线缆布线应参考以下原则：

1. 原则上柜内线缆采用线槽内敷设，特定情况下无法采用槽内敷设的可采用绑扎走线；
2. 绑扎材料应采用玻璃纤维，以具备高耐热，高电阻，阻燃，低烟，耐腐蚀以及低吸水性；
3. 通过设备的端子接口，端子台或连接器进行线缆连接；
4. 线缆应进行合理的固定，并保证不可将金属固件直接压接在电缆上；此外还应考虑未固定部分的保护；
5. 对于并柜间的线缆，原则上在相同的分区单元内可直接连接；在不同的分区单元间线缆应通过端子台连接；
6. 一个端子上不超出两个接线端，此外对于外部电缆的连接原则上一个端子对应一个接线；
7. 外部线缆通过端子台或连接器同柜内线缆连接（配电盘除外）；
8. 热电偶补偿导线直接连至柜内监测仪表不经端子。
9. 线缆分离：

* 动力电缆、控制电缆、仪表电缆应相互分离，对相同类型电缆方可进行绑扎；
* 对反应堆安全保护机柜内的信号线缆，应根据信号的不同安全等级，不同序列进行线缆分离；

1. 对于柜内光纤，应考虑以下方面：弯曲半径应大于允许值；光纤的固定不直接增加连接器的重量；
2. 为了提高EMI性能，线缆外包裹高耐热PVC膜和铝箔层进行屏蔽

### 线缆及装置排布要求

对线缆及装置的排布要求如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 左右布置 | 上下布置 | 前后布置 |
| 三相交流 | 从左起1，2，3相 | 从上起1，2，3相 | 从前起1，2，3相 |
| 单相交流 | 从左起L，N相 | 从上起L，N相 | 从前起L，N相 |
| 直流电路 | 左为负极，右为正极 | 上为正极，下为负极 | 前为正极，后为负极 |

## COTS

系统中使用到的其他模块，例如断路器、继电器、滤波器、端子排等属于外购商品级物项，由相关设计人员根据实际项目需要进行选型。见各相关设备规格书。

# 环境要求

## 周围环境

系统在安装、运输、存储和运行前环境条件：

* 极限环境温度：-31.6℃~55℃；
* 相对湿度：0~100%，无凝结；
* 空气：盐、尘；
* 大气压力：86~106kPa。
* 满足RCC-E D2220震动要求。

在运行期间环境条件：

* 正常运行条件：
  1. 温度：5℃~35℃；
  2. 相对湿度：10%~95%，无凝结；
  3. 空气：无盐
* 事故条件：
  1. 温度达到40℃时同时通风系统失效期间，系统能够正常运行；
  2. 温度达到45℃时同时通风系统失效期间（一天时间），系统能够运行，设备不应造成永久损坏。

## 抗震要求

所有的系统设备应满足抗震I类的要求。

## 噪声和浪涌防御

进入机柜的220V交流电源需安装交流滤波器，同时需安装浪涌保护器。通过走桥架进入机柜的24V供电回路需考虑增加直流滤波设计。

所有柜内设备金属壳体必须接保护地；所有柜内电源负端需接信号地；所有进入机柜的电缆需接屏蔽地。通过良好的接地来提高防电磁干扰能力。

机柜、机箱和板卡在设计时需保证良好的屏蔽效能，提高抗电磁干扰能力，减少噪声和浪涌干扰。

# 性能要求

## 响应时间

* 反应堆停堆响应时间：≤150 ms，对于超功ΔT和超温ΔT，响应时间不超过700 ms。
* 专设安全设施驱动响应时间：≤400ms（由P4信号引起的汽轮机动作响应时间≤350ms）；
* 简单页面切换时间：≤1S；
* 复杂页面切换时间：≤2S；
* 点击屏幕到向操作员反馈时间不超过400mS；
* 画面视图显示刷新时间不超过1S；
* RPC\ESFAC\SRC到安全控制显示时间不超过1.5S，DCS接收信号到安全级网关时间不超过1S；
* 从操作员发出控制指令到DCS输出时间不超过1S；
* 控制站处理器冷启动时间不超过5分钟；
* 应用软件单设备全部下装完成时间不大于30分钟；

## 精度

采集精度包括从隔离分配、采集的全部采集路径，输出通道精度包括现场设备前端的所有输出设备精度。

* 模拟量输入通道（高电平，如1~5V、4~20mA）：优于±0.2%；
* 模拟量输入通道（毫伏信号）：优于±0.25%；
* 模拟量输出通道：优于± 0.25%；
* 热电阻采集精度：优于± 0.25%；
* 热电偶采集精度：优于±4.66℃；

## 可靠性

### MTBF

* 由于DCS设备故障引起停机事件的MTBF：≥50堆年；
* DCS设备故障造成电厂可用性降低的MTBF：≥5年。

### MTTR

除电源模块外的所有模块MTTR不大于4小时，电源模块MTTR不大于2小时。

### 可用性

反应堆紧急停堆系统的可用性要求如下：

* 总体可用率 ≥99.99%；
* 系统拒动率<10-7/指令；
* 误停堆率 0.1次/年；

## 裕量要求

为考虑安全级系统将来的可扩展性，硬件和软件需保留了一定的裕量。

* 雪崩条件下的CPU负荷
* 每个处理器模块的CPU负荷不大于70%；
* SCID设备的CPU负荷不大于70%；
* IO裕量：≥ 15%；
* 内存裕量：≥50%；
* 电源负荷：＜70%；
* 标准画面和设备图符的裕量：＞10%；
* 网络负荷：＜40%。

# 供电接地要求

## 系统供电规格

系统供电电源由电厂提供，规格如下：

* 电压：AC 220V +10%/-15%
* 类型：交流单相系统2线制
* 频率：50Hz±5%

## 系统接地规格

系统接地分为保护地、屏蔽地和数字地，机柜内存在数字地、屏蔽地和保护地3种接地汇流排，数字地和屏蔽地接地螺钉与机柜柜体绝缘，各个机柜的接地汇流排分别与接地主母线相连接，最后通过一点接入现场地。

保护地的接地设计如下：

* 每个模块上的保护地接线柱需连接到保护接地汇流排上；
* 直流电源、滤波模块及其他外购设备的保护地连接到机柜的保护接地汇流排上；
* 所有金属外壳设备保证良好的保护接地。

屏蔽地的接地要求：

* 进出机柜的屏蔽线的屏蔽层在出柜口将屏蔽层接到屏蔽接地汇流排上；
* 屏蔽层需保证一端接地，在信号的供电侧进行屏蔽接地；
* 柜内屏蔽电缆可以就近将屏蔽层接到机柜上；
* 预制电缆可通过预制头将屏蔽层接到模块或设备上。

数字地的接地要求：

* 所有模块上的数字地接地柱需连接到数字地汇流排上；

# 标识要求

柜内各设备均应设计有清晰的标识铭牌，以便于后期维护。各类设备的标识编码要求如下：

## 机柜标识

机柜标识采用“编码”+“标牌”的标识方式。

机柜编码具体规则如下图9.1‑1所示：



图9.1‑1 机柜编码规则

其中：

1. 机组号：

5：5号机组；

6：6号机组。

1. 系统标识：

KCS：安全级系统；

KCP：非安全级系统；

KSC：OWP，ECP，ACP，RSS。

1. 功能组号：各功能组编号，

0：反应堆紧急停堆部分；

1：专设安全设施驱动部分；

2：安全信息和控制部分

3：其他部分。

1. 子组号：表示每个功能子组在该功能组中的编号，例如紧急停堆部分RPC I~IV通道分别为1~4；专设安全设施驱动部分ESFAC为1、2，SRC 1~4分别为3~6，以此类推；
2. 机柜号：该字符为子组内机柜流水号，范围为1~9；
3. 设备类型：

AR：机柜；

RK: 继电器架；

PP：控制台；

TB：配电柜。

机柜标牌的颜色要求如下表格 9.1‑1所示，其他规格参数，包括尺寸，材质，安装方式，字体等，由相关设计人员在项目实施中进行选择确认。

表格 9.1‑1 机柜标牌颜色说明

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 内容 | CH.I | CH.II | CH.III | CH.IV | Train A | Train B | NC |
| 标牌颜色 | 黄 | 蓝 | 红 | 棕 | 橙 | 绿 | 白 |
| 字体颜色 | 黑 | 白 | 白 | 白 | 白 | 白 | 黑 |

## 设备标识

设备标识采用“编码”+“标牌”的标识方式。设备包括机箱，电源，模块，卡件，端子排及其他设备等。

机箱，电源及模块的编码规则如下图9.2‑1所示：



图9.2‑1 设备编码规则

其中：

1. 设备类型：

CF：机箱；

PS：电源，特指独立安装的电源模块；

UN：模块，特指有独立功能的模块。

1. 机柜号：功能组内机柜排号；
2. 流水号：机柜内设备排号，流水号1~Z。

卡件（包括电源板卡）的编码规则如下图9.2‑2所示：



图9.2‑2 卡件槽号编码规则

其中：

1. 卡件位置：

S：单板卡；

F：前板卡；

R：后板卡；

1. 子组号：表示每个功能子组在该功能组中的编号；
2. 机柜号：功能组内机柜流水号；
3. 机箱号：机柜内机箱流水号；
4. 卡槽号：机箱内卡槽号，范围为1~E。

端子排的编码规则如下图9.2‑3所示：



图9.2‑3 端子排编码规则

其中：

1. 机组号：

5：5号机组；

6：6号机组。

1. 系统标识：

KCS：安全级系统；

KCP：非安全级系统；

KSC：OWP，ECP，BCP，RSS；

1. 机柜号码：功能组内机柜排号；
2. 位置码：从机柜正面看，

当端子排位于机柜左前侧时，编号为1，3（初始为1，当端子排号超过9时，则为3，其他侧规则相同）；

当端子排位于机柜右前侧时，编号为2，4；

当端子排位于机柜左后侧时，编号为5，7；

当端子排位于机柜右后侧时，编号为6，8；

1. 端子排号：为端子排流水号0~9；
2. 设备类型：BN为端子排。

其他设备的编码规则如下图9.2‑4所示：



图9.2‑4 其他设备编码规则

其中：

1. 设备类型：包括浪涌，空开，滤波器，继电器等，为设备的缩写，例如，浪涌为Z，空开为CP，滤波器为LF，继电器为RL等；
2. 流水号：该类设备依次排号，流水号01~99。

## 线缆标识

线缆标识采用“编码”+“标牌”+“色标”的标识方式。

柜内电缆（包括预制电缆和半预制电缆）不区分颜色；柜内导线颜色如下表格 9.3‑1所示：

表格 9.3‑1 导线颜色说明

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 电路名称 | 导线颜色 | | | | | |
| CH.I | CH.II | CH.III | CH.IV | Train A | Train B |
| 控制线路（DC） | 黄 | 蓝 | 红 | 棕 | 橙 | 绿 |
| AC电源回路 | L线 : 红色 N 线：蓝色 | | | | | |
| DC电源回路 | 正极性 :红色  负极性 :蓝色 | | | | | |
| 接地回路 | 黄绿 | | | | | |
| 非安全级系统 | 白 | | | | | |