ICS 27.120.99
CCS F 81

# 团　　体　　标　　准

T/CNS 40—2020

# 高温气冷堆核动力厂控制系统设计准则

**Design criteria for control system of high temperature gas cooled reactor nuclear power plants**

2020-12-31 发布　　2021-04-01 实施

中 国 核 学 会　　发 布

# 目　　次

# 前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国核学会提出。

本文件由核工业标准化研究所归口。

本文件起草单位：清华大学核能与新能源技术研究院。

本文件主要起草人：于晖、张良驹、黄晓津、周树桥、李江海、姚启欣。

# 高温气冷堆核动力厂控制系统设计准则

## 1 范围

本文件规定了球床模块式高温气冷堆核动力厂控制系统的功能要求和设计准则。

本文件适用于球床模块式高温气冷堆核动力厂控制系统(简称“控制系统”)和设备的设计。

本文件不适用于工艺设备配套的控制装置。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 2423.1 电工电子产品环境试验 第2部分:试验方法 试验A:低温

GB/T 2423.2 电工电子产品环境试验 第2部分:试验方法 试验B:高温

GB/T 2423.3 电工电子产品环境试验 第2部分:试验方法 试验Cab:恒定湿热试验

GB/T 2423.4 电工电子产品环境试验 第2部分:试验方法 试验Db:交变湿热(12 h+12 h循环)

GB/T 2423.10 电工电子产品环境试验 第2部分:试验方法 试验Fc:振动(正弦)

GB/T 2423.22 电工电子产品环境试验 第2部分:试验方法 试验N:温度变化

GB/T 17626.2 电磁兼容 试验和测量技术 静电放电抗扰度试验

GB/T 17626.3 电磁兼容 试验和测量技术 射频电磁场辐射抗扰度试验

GB/T 17626.4 电磁兼容 试验和测量技术 电快速瞬变脉冲群抗扰度试验

GB/T 17626.5 电磁兼容 试验和测量技术 浪涌(冲击)抗扰度试验

GB/T 17626.6 电磁兼容 试验和测量技术 射频场感应的传导骚扰抗扰度

GB/T 17626.8 电磁兼容 试验和测量技术 工频磁场抗扰度试验

GB/T 17626.9 电磁兼容 试验和测量技术 脉冲磁场抗扰度试验

GB/T 17626.11 电磁兼容 试验和测量技术 电压暂降、短时中断和电压变化的抗扰度试验

GB/T 17626.12 电磁兼容 试验和测量技术 振铃波抗扰度试验

GB/T 17626.13 电磁兼容 试验和测量技术 交流电源端口谐波、谐间波及电网信号的低频抗扰度试验

GB 17799.4 电磁兼容 通用标准 工业环境中的发射

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

## 3 术语和定义

本文件没有需要界定的术语和定义。

## 4 系统功能和系统组成

### 4.1 系统功能

执行高温气冷堆核动力厂的运行监测、显示、控制和报警功能，以维持高温气冷堆核动力厂系统和参数在正常运行范围内，防止或纠正偏离正常运行工况，从而保证高温气冷堆核动力厂连续稳定运行，减少不必要的停堆。

提供丰富的监测手段，监测高温气冷堆核动力厂在正常运行、预期运行事件时的运行参数和设备状态。

提供可靠的控制手段，可以自动或手动维持运行参数在规定的范围内，或自动跟踪负荷变化，保证反应堆及其辅助系统的连续运行。

提供报警逻辑处理和画面报警显示手段，在反应堆及其重要系统异常或设备故障时，采用控制系统设备给出声光报警的触发信号以及人机界面报警显示，提请操纵员及时注意并采取必要的动作。

控制系统不执行安全功能。

### 4.2 系统组成

#### 4.2.1 概述

控制系统主要包括反应堆功率控制系统、工艺控制系统和协调控制系统。其中工艺控制系统包括核岛工艺控制系统、常规岛控制系统和辅助设施控制系统。

工艺设备自带的控制装置，不属于控制系统设备。

#### 4.2.2 反应堆功率控制系统

##### 4.2.2.1 控制棒手动控制

应通过手动操作控制棒，实现反应堆的启动、功率运行、功率转换及正常停堆等操作。为保证控制棒操作的安全性，应考虑下列措施：

——设置安全联锁，只有在规定的条件满足的情况下，才能操作控制棒；

——棒控操作应按照规定的逻辑次序；

——应对反应性添加速度加以限制。

##### 4.2.2.2 反应堆功率自动调节

应实现规定功率范围内的自动功率调节，克服反应堆功率的瞬变，限制对正常运行工况的偏离，满足设计要求的稳态和动态特性；在规定功率范围内，自动完成不同功率水平的转换。

#### 4.2.3 工艺控制系统

##### 4.2.3.1 核岛工艺控制系统

核岛工艺控制系统应实现高温气冷堆核动力厂工艺系统运行参数及设备状态的监测，并实现对设备的手动或自动操作控制，对某些重要参数进行自动调节，还应实现对重要电气设备的电气保护。核岛工艺控制系统主要执行以下控制功能：

——主氦风机监测控制；

——吸收球系统监测控制；

——一回路压力泄放系统监测控制；

——燃料装卸系统监测控制；
——乏燃料贮存系统监测控制；
——氦净化及氦辅助系统监测控制；
——负压通风系统监测系统；
——厂房通风系统监测控制；
——设冷水系统和厂用水系统监测控制；
——厂用电系统监测控制；
——工艺辐射系统监测控制。

#### 4.2.3.2 常规岛控制系统

常规岛控制系统完成汽轮机、发电机-变压器组、厂用电源系统及其辅机生产过程的控制，执行以下监测控制功能：

——数据采集(DAS)；
——模拟量控制(MCS)；
——顺序控制(SCS)；
——汽轮机数字电液控制系统(DEH)；
——汽轮机跳闸和保护；
——电气监测控制。

#### 4.2.3.3 辅助设施控制系统

辅助设施控制系统应执行除核岛工艺和常规岛之外的辅助设施的监测控制功能。

### 4.2.4 协调控制系统

协调控制系统在反应堆功率控制系统和工艺控制系统自动调节的基础上，进行整个两模块或多模块高温气冷堆核动力厂的协调优化控制，应由协调控制器根据负荷要求，确定每个反应堆模块的当前运行功率，自动调节每个模块的反应堆功率、热氦温度、氦气流量、蒸汽发生器出口蒸汽温度、蒸汽发生器给水流量、模块输出热功率以及汽轮机进口压力等参数到控制回路给定值，从而使整个多模块高温气冷堆核动力厂安全、平稳、经济运行。

## 5 安全分级与抗震类别

### 5.1 安全等级

控制系统设备的安全等级为非安全级。

### 5.2 质保等级

控制系统设备的质保等级为 QA3 或 QNC。

### 5.3 抗震类别

控制系统设备的抗震类别为非核抗震类。

## 6 设计原则

### 6.1 安全原则

控制系统不执行安全功能，且与安全系统相互独立，使得在任何情况下不会妨碍安全系统执行其安

全功能。对可能影响安全的重要操作应在设计中采取必要的安全联锁措施。

### 6.2 高度自动化原则

宜提高高温气冷堆核动力厂自动化运行水平，简化各种操作。单个模块50%功率以上功率运行过程中的功率维持、功率转换及主要工艺参数的维持均可自动执行，同时应保持操纵员的最高决策权和干预权。

### 6.3 集成一体化原则

控制系统设计宜采用统一的硬件和软件平台，并集成到整个控制网络中，在主控制室采用统一显示和操作的人机界面，最大限度地改善运行人员与高温气冷堆核动力厂之间的人机接口，同时可以通过网关协议转换将非标准控制设备接入，从而可以方便系统集成、减少备品备件、方便运行维护。

### 6.4 独立性控制原则

执行控制及自动调节功能的过程控制站宜直接采集监测变量，不依赖网络通信和其他过程控制站即可以执行控制或联锁功能，从而保证控制及调节功能的独立性和更好的实时性能。

### 6.5 可用性原则

控制系统应具有高可用性，设备应采用高度冗余配置，系统内任一组件发生故障，均不应影响整个系统工作。

### 6.6 可维护性原则

控制系统设计应具有高的可维护性。宜采用工业标准设备，以减少备品备件种类。设备应易于进行故障诊断和故障定位，故障部件可以在线更换，从而提高可维护性。

## 7 设备和软件设计准则

### 7.1 总则

控制系统采用统一的、集成一体化的分布式控制系统(Distributed Control System，简称DCS)作为基础平台设备，实现反应堆功率控制、工艺控制以及协调控制功能。

### 7.2 系统架构

DCS系统由过程控制层设备、人机界面层设备通过工业以太网连接而成。DCS系统网络是高温气冷堆核动力厂控制系统的专用网络，外部公共网络不应通过有线或无线的方式接入DCS系统网络。

### 7.3 过程控制层设备

#### 7.3.1 控制器

控制器应满足以下要求：

——控制器应具有冗余控制器支持能力，以主从方式工作时，应具有数据热备份和同步运算能力。

——控制器应有两个独立的网络接口，可以同时与互为冗余的两个系统网络连接。一个过程控制站可以通过冗余通信总线连接若干个扩展I/O站。

——控制器模件应采用无风扇设计。

——控制器应可以热插拔，具有即插即用能力。应具有掉电保护功能，失电时控制器模件中的逻辑

不会失去，输出应保持在预先设定的安全状态，一旦重新受电，控制器应能自动恢复正常工作而无需运行人员的任何干预。

#### 7.3.2 过程控制站

过程控制应满足以下要求：

——过程控制站应可以根据需要配置不同的通信模件，提供串行通信接口，以实现 DCS 与其他数字化子系统的数据通信。

——过程控制站应能够至少输入以下信号类型：

- 无源 4 mA～20 mA 模拟量输入信号；
- 有源 4 mA～20 mA 模拟量输入信号；
- IEC K 型、E 型热电偶(TC)信号；
- Pt100 类型热电阻信号；
- 无源触点型开关量信号；
- 脉冲输入信号；
- 通信信号。

——过程控制站应能够对采集的开关量信号进行 SOE 处理。

——DCS 系统需要设置通信网关，接受反应堆保护系统、核测量系统等系统通过通信方式发送来的监测数据。

——过程控制站应能够至少输出以下信号类型：

- 有源 4 mA～20 mA 模拟量输出信号；
- 24 V DC 无源触点；
- 24 V DC 固态开关；
- 220 V AC 无源触点；
- 脉冲输出信号。

### 7.4 人机界面层设备

人机界面层设备由系统工程师站、系统操作员站、服务器、监视器等组成。

——系统工程师站应能对整个 DCS 系统进行配置组态、系统功能编程、系统状态诊断及监视。

——系统操作员站应能够为主控制室运行人员提供具有足够信息的人机界面，包括但不限于：主控制室的信息显示、设备操作、报警处理、模拟显示盘显示控制、数据记录和报表打印功能。

——DCS 屏幕显示信息及报表应能实现全部汉字化，显示内容及形式如下：

- 以图形方式显示的系统流程图、条杆图、趋势曲线图；
- 以数据表格形式显示的参数实时值；
- 以事件序列显示的报警事件、泵和阀等工艺设备的状态变化事件、设备故障事件等。

DCS 系统应具有历史数据存储和数据回溯功能，应能对重要数据进行备份，以便长期保存。

### 7.5 通信网络层

通信网络层的设备宜包括网络交换机、服务器和网关。DCS 系统网络层实现过程控制站、操作员站、工程师站、通信网关及服务器之间的网络通信。系统网络应采用符合 ISO 标准的开放式协议(如工业以太网)，不得采用 DCS 平台供货商的专有协议。

### 7.6 时钟同步

应采用一个“数字主时钟”作为统一的 DCS 系统时钟基准，使挂在系统网络总线上的各个节点设备

时钟同步。

### 7.7 冗余设计

#### 7.7.1 过程控制站冗余

应按照以下要求进行过程控制站的冗余配置：

——过程控制站内部应配置冗余的控制器、冗余的电源，采用冗余的外电源供电；

——控制器与 I/O 模件及扩展 I/O 站之间应采用冗余的 I/O 总线通信。

#### 7.7.2 系统网络冗余

系统主干网络应采用高速、冗余的环形网络，环上任一网段均是其他网段的冗余，两个环形光纤以太网互为冗余。每个网络节点（过程控制站、操作员站、工程师站、服务器及网关）都应具有或配置不少于两个独立的通信网络端口，并通过冗余通信电缆分别与两个主干环网相连。

#### 7.7.3 重要设备冗余

每种服务器都应采用冗余配置，主控制台上的各个操作员站都应具有完全相同的显示和操作能力，互为冗余备份。

#### 7.7.4 供电冗余

控制机柜应接受两路 220 V AC 电源供电。控制机柜内应设两对独立的直流电源装置，每对中的两个电源装置分别采用冗余外电源中的一路供电。其中一对直流电源装置给机柜内的控制器和 I/O 模件等电路冗余供电，另一对直流电源装置给输入机柜的现场信号冗余供电。

网络交换机或协议转换器应采用冗余的外电源供电，其他所有设备（服务器、操作员站、工程师站、打印机、网关等）宜采用冗余外电源供电。不能直接接受两路供电的设备，可采用能够将两路供电输入切换为一路电源输出的电源切换装置为其供电，切换时间应不影响受电设备的正常工作。

### 7.8 软件要求

DCS 系统的软件应满足以下要求：

——应具有构成 DCS 系统平台、完成应用开发和进行诊断维护所需要的各种软件，包括但不限于各类计算机操作系统、过程控制站实时操作系统及控制执行软件、操作员站人机界面平台软件、工程师站组态工具软件、DCS 系统诊断监督软件、服务器平台软件、各部分的网络通信软件等。

——操作员站、工程师站和服务器应选用稳定的并且广泛应用于工业领域的操作系统。

——工程师站组态软件应保证采用统一的方式进行组态。至少应包括下列组态功能：

- 设备配置组态；
- 数据库组态；
- 控制算法组态；
- 数据处理计算组态；
- 报表组态；
- 人机界面组态；
- 下装工具。

——DCS 系统应用控制程序的编程语言应至少有功能块图（FBD）、梯形图（LD）、顺序功能图（SFC）、指令表（IL）和结构化文本（ST）五种方式。

——应选用通用的编程语言开发特殊要求的功能软件/子程序，无缝嵌入到DCS系统的软件中，以实现复杂的控制算法（如反应堆功率调节）、特殊格式的显示画面、特定格式的报表打印等功能。

——应能通过各类逻辑块联接模拟控制回路的组态，并用易于识别的工程名称加以标明。应能在工程师站根据指令打印出已完成的所有系统组态。

——应能在工程师站调出系统内任一过程控制站或操作员站的组态信息，还可将组态数据下载到各过程控制站或操作员站。组态应可在任一台工程师站上进行，通过登陆权限控制组态或修改的范围。在线修改一般限于在核电站的系统调试阶段，在核电站进入启动或运行阶段后，可以通过某种手段封锁在线修改功能。

——工程师站应能设置软件保护密码，以防非授权人员擅自改变控制策略、应用程序和系统数据库。

### 7.9 可维护性要求

DCS系统设备应满足以下可维护性要求：

——DCS平台应具备自诊断功能，在运行过程中，工程师站应能对整个系统的状态进行监视和诊断，可以集中监视整个系统、某个过程控制站直至过程控制站中某个模件的工作状态。

——DCS模件应具有在线自检的功能，在运行过程中可自动连续进行功能检查，面板上应具有指示灯指示模件的工作状态及检查结果。

——DCS模件应可以在线更换并具有即插即用能力，而不影响DCS运行。

——DCS硬件应易于扩充，软件应允许并易于修改。

### 7.10 环境适应性和电磁兼容性

DCS设备应具有环境适应性和电磁兼容性，以保证DCS设备长期可靠运行。

DCS设备应按照下述标准进行试验或提供试验报告，以证明DCS设备具有要求的环境适应性和电磁兼容性：

——DCS设备环境适应性试验，按照GB/T 2423.1～GB/T 2423.4、GB/T 2423.10和GB/T 2423.22；

——DCS设备电磁兼容性试验，按照GB/T 17626.2～GB/T 17626.6、GB/T 17626.8～GB/T 17626.9、GB/T 17626.11～GB/T 17626.13和GB 17799.4。

### 7.11 设备内部电缆

DCS系统设备内部电缆应满足低烟、无卤、阻燃要求。

## 8 DCS系统工程设计准则

### 8.1 概述

DCS系统工程设计包括DCS系统设备安装、与其他系统硬件和软件接口、DCS系统硬件配置、DCS系统软件工程组态、DCS网络安全等内容。

### 8.2 环境条件要求

DCS设备所在房间的实际环境条件应优于DCS设备允许长期可靠运行的环境条件。

### 8.3 独立性控制设计

相同反应堆模块的同一系统I/O信号测点宜分配到同一过程控制站，常规岛及公用系统中的同一

系统 I/O 信号测点宜分配到同一过程控制站。

属于同一控制回路和调节回路的 I/O 测点，应分配到同一过程控制站；若某 I/O 信号同时工作在不同控制站内的控制回路或调节回路，则需要采用硬接线方式实现该信号在两个控制站之间的传输。

### 8.4 与其他系统接口

过程控制站设备应避免直接接入现场设备高电压或电流等级的主供电回路或控制电源回路，以减少现场工频电源对过程控制站设备带来的电磁干扰。

过程控制站设备宜通过具有大容量输出触点的中间继电器隔离后输出控制信号，满足现场设备控制回路中较高等级的电压和电流要求。

保护系统及核测量系统与 DCS 系统之间通过通信网关传输数据时，要考虑 DCS 系统网络安全问题。应在控制系统一侧设置单向接收装置，接收通信数据。

DCS 系统的“数字主时钟”应能够与核动力厂全厂统一时钟信号对接并实现同步。

### 8.5 网络安全

DCS 系统设计时应考虑网络安全，除非 DCS 自身具备网络安全风险防护能力，否则应为 DCS 提供网络安全风险防护措施。

因 DCS 具有很高的可用性要求，根据 GB/T 22239—2019，在进行 DCS 网络安全设计时，要充分考虑到实现等级保护要求的一些约束条件，原则上安全措施不应对 DCS 的基本功能产生不利影响。

第三方设备与 DCS 系统设备的通信接口处，应采取直接连接、逻辑隔离、设置专用的横向单向隔离装置等措施。

# 参 考 文 献

[1] HAF 003 核电厂质量保证安全规定

中 国 核 学 会
团 体 标 准
**高温气冷堆核动力厂控制系统设计准则**
T/CNS 40—2020
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址 www.spc.net.cn
总编室:(010)68533533　发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1　字数 25 千字
2021 年 8 月第一版　2021 年 8 月第一次印刷
*
书号:155066·5-3452　定价 18.00 元



T/CNS 40-2020