ICS 27.120.99
CCS F 81

团　　体　　标　　准

T/CNS 39—2020

高温气冷堆核动力厂反应堆保护系统设计准则

Design criteria for the reactor protection system of high temperature gas-cooled reactor nuclear power plant

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：李铎、张良驹。

高温气冷堆核动力厂反应堆保护系统设计准则

1 范围

本文件规定了高温气冷堆核动力厂反应堆保护系统的设计准则和基本要求。

本文件适用于高温气冷堆核动力厂反应堆保护系统的设计。

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 12727 核电厂安全级电气设备鉴定

IEEE std 1012—2014 IEEE Standard for Software Verification and Validation

3 术语和定义

下列术语和定义适用于本文件。

3.1

反应堆保护系统 reactor protection system

监测反应堆的运行，并根据接收到的异常工况信号，自动触发动作以防止发生不安全或潜在的不安全工况的系统。

3.2

专设安全设施 engineered safety features

为限制或缓解反应堆事故后果而专门设置的安全系统，高温气冷堆核电厂专设安全设施包括一回路系统隔离、蒸汽发生器事故排放等。

3.3

单一故障 single failure

导致某一部件不能执行其预定安全功能的一种故障，以及由此引起的各种继发故障。

3.4

冗余 redundancy

除本身外，设置另外一个或多个（相同的或不相同的）构筑物、系统或部件，以便其中一个能执行所要求的功能，不管任何其他的是处于运行状态还是故障状态。

3.5

多样性 diversity

为执行某一确定功能设置两个或多个多重部件或系统，这些多重部件或系统具有不同属性，从而减少了共因故障的可能性。

3.6

独立性 independence

设备的一种状态，在该状态下，冗余的设备不会因任何单一设计基准事件（如水淹）而同时失效。

4 系统设计

4.1 系统范围

反应堆保护系统包括从敏感元件到安全驱动器输入端的所有设备和线路，以及设备中运行的软件。参考附录 A，其构成分为：安全监测装置、安全逻辑装置和安全驱动装置。

安全监测装置包括检测单元（含敏感元件和变送器）、信号甄别和处理部件、输出电路。检测单元的信号类型包括核测量信号和工艺过程信号。

安全逻辑装置接收安全监测装置的输出信号，完成预定的逻辑功能，并将其输出信号送给一个或多个安全驱动装置。

安全驱动装置根据一个或多个安全逻辑装置的指令，控制执行机构动作。

4.2 系统功能

4.2.1 概述

反应堆保护系统连续监测反应堆保护变量，在监测的保护变量达到或超过停堆整定值时，自动产生紧急停堆触发信号，停闭反应堆，以保证在发生预计运行事件时反应堆状态不超出规定的设计限值，从而保证反应堆的安全；在发生设计基准事故时，在紧急停堆的同时，启动专设安全设施，以减轻事故的后果。

4.2.2 紧急停堆功能

在监测的保护变量达到停堆整定值时，保护系统输出紧急停堆触发信号，从而使反应堆达到安全停堆状态。紧急停堆动作包括：

——产生紧急停堆触发信号，触发停堆断路器脱扣，断开控制棒驱动电源，控制棒依靠自身重力紧急下落实现停堆；

——产生停一回路主氦风机触发信号，触发主氦风机断路器脱扣，停主氦风机；关闭主氦风机挡板（在电气控制回路内延迟后执行关闭动作）；

——二回路系统隔离触发信号，关闭主给水隔离阀，联锁停给水泵；关闭主蒸汽隔离阀（在隔离阀电气控制回路内延迟后执行关闭动作）。

4.2.3 专设安全设施触发功能

根据高温气冷堆核电厂事故分析的结果，需要启动专设安全设施的设计基准事故包括一回路系统失压事故和蒸汽发生器破管事故。相应的专设安全设施包括：

——一回路系统隔离，在发生一回路系统失压事故时，关闭与一回路系统隔离相关的阀门；

——蒸汽发生器事故排放，在发生蒸汽发生器破管事故时，打开蒸汽发器事故排放阀，执行事故泄压排放；当二回路与一回路压差低于整定值时关闭事故排放阀，蒸汽发生器事故排放结束。

4.3 安全分级与抗震类别

保护系统安全等级为安全级（1E 级），质保等级为 QA1 级，抗震类别为抗震Ⅰ类。

5 设计总则

每座反应堆设置单独保护系统，提供安全保护措施。多堆单机组核动力厂允许多堆之间共用构筑

物、动力源和辅助支持设施，但应保证所有反应堆单独或同时执行所需安全功能的能力不受影响。

预计运行事件和设计基准事故下的所有安全动作均应自动触发完成，在预计运行事件或设计基准事故开始的 30 min 内，不需要操纵员的干预。在不需要立即动作的情况下，可允许根据操纵员判断手动启动安全动作。应把对操纵员在短时间内进行干预的要求降至最低。

安全功能应设置系统级手动触发动作，作为自动触发的后备。设计应确保自动触发电路中的故障不妨碍手动触发保护功能的执行。

保护系统应能实现反应堆安全分析提出的保护功能并满足相关性能要求，包括需要保护的反应堆状态、保护动作、监测变量、安全限值、监测量程、精度及响应时间等。

为了保证保护功能的有效性，对于事故分析中的每一种假设始发事件，宜采用不同的物理效应或不同的变量来监测，可用不同类型的设备来测量同一物理变量，以便克服共因故障。

在设计基准事故工况下，保护系统设备应能满足功能及性能要求。

保护系统应为主控制室提供足够的信息，使操作员可以连续监视保护变量、保护系统的工作状态及触发动作的执行效果，相关信息显示设备可以不是安全级。

保护系统应同时满足高温气冷堆核动力厂的安全目标和可用性目标。应最大限度降低拒动概率（拒动概率$<10^{-5}$）和误动概率（误动概率<1 次 / 堆年），保证高温气冷堆核动力厂的连续运行。

6 详细设计准则

6.1 单一故障准则

保护系统内单一故障或单次事件及其继发故障不应有损于系统的保护功能。

6.2 冗余

为满足单一故障准则要求，保护系统设计应采用冗余技术。它包括安全监测装置的冗余、安全逻辑装置的冗余及安全驱动装置的冗余。

6.3 符合

为了提高保护系统触发动作的可靠性，应采用符合技术，以减少因信号波动、仪表漂移、系统内元器件故障等因素使保护系统产生误动作的可能性。

6.4 独立性

6.4.1 总体要求

为了克服冗余部件相互间的有害作用，保护系统各冗余监测通道之间，以及冗余逻辑列之间，均应按独立性原则设计，防止一个通道（或逻辑列）故障导致其他通道（或逻辑列）同时失效的可能性。还应在保护系统中采取措施保证自身对其他系统的独立性，防止其他系统故障导致保护系统失效的可能性。通常采用电气隔离、通信隔离和实体分隔来满足独立性的要求。

6.4.2 电气隔离

在保护系统的冗余通道之间及保护系统与其他系统之间在需要有信号联系时应采用隔离装置（如光电隔离器件、隔离放大器、继电器接点等）实现电气隔离。隔离装置输出端（或输入端）的任何可能故障（出现开路、短路、接地、最大可能电压等）不应影响输出端（或输入端）所连设备的正常工作。隔离装置应作为保护系统的一部分来设计。

冗余监测通道或冗余逻辑列应采用独立的安全级电源供电。

6.4.3 实体分隔

保护系统的冗余部件之间应采用距离、屏障或两者结合的方法来实现实体隔离，以便减少某些假设始发事件和故障引起不利后果的可能性。应该对设计基准中考虑到的所有假设始发事件，例如火灾、爆炸物、高能管道甩击和飞射物的影响提供保护的必要性。

冗余监测通道的现场设备（传感器、变送器等）应采用距离、屏障物（如墙、大型设备）作实体隔离。

冗余监测通道的仪表机柜、冗余逻辑列的机柜以及冗余的电源系统应分别放在彼此独立的、按抗震要求和独立防火区设计的仪器间内。

保护系统冗余部分的电缆之间、保护系统电缆与其他系统的电缆之间，通过屏障或留有足够的间距来保证实体隔离。

6.4.4 通信隔离

在保护系统的冗余通道之间或保护系统与非安全系统之间在需要采用数据通信时，应采取通信隔离措施，以避免影响安全功能的执行。

6.5 故障安全设计

保护系统的设计应当尽量保证当部件故障或失去动力源时都趋向于产生保护动作。

保护系统在失去动力源和出现监测通道或逻辑列内电路开断、短路等故障时，均导致系统安全动作，即触发紧急停堆。

专设安全设施的执行一般需要动力源支持，对专设安全设施驱动系统可设计成通电动作，但专设安全设施触发电路应设计成失电安全。

6.6 多样性与抗共因故障

6.6.1 应该采取措施避免某些共因故障造成安全功能失效的可能性，对数字化保护系统应特别考虑软件共因故障导致冗余部件同时失效的可能性。可以考虑采用的多样性措施有。

——功能多样性：对每个要求保护动作的假设始发事件采用不同的变量或用不同的物理效应来监测，对需要执行的安全功能采用不同的保护动作来实现。

——设备多样性：在系统中使用不同工作原理的设备，或者使用不同制造厂家的类似设备来实现同一个或类似功能。设备多样性可以是系统级的，如保护系统和第二停堆系统采用多样性设备实现；也可以是系统内部件级的，如保护系统内的冗余逻辑部件可以采用多样性设备实现。

6.6.2 对数字化保护系统应进行分析，以保证采取了必要的多样化措施，防止软件共因故障导致安全功能失效的可能性。数字化保护系统应满足如下多样性要求。

——对数字化保护系统执行的安全功能，如果同时有其他安全的或非安全的设施可以执行同样的功能或提供类似的保护，且这种功能多样性不受数字化保护系统假想软件故障的影响，则在数字化保护系统冗余通道中采用相同软件是可以接受的。

——如果不存在上述的功能多样性，则可以分析在纵深防御的不同层次（如紧急停堆、专设安全设施、控制监测系统）之间是否存在多样性。作这种分析时可以包括手动操作功能和非安全的控制监测功能，但它们在所需要的时间内应该可以执行预期的功能。如果纵深防御的不同层次不受数字化保护系统假想软件故障的影响，则在数字化保护系统冗余通道中采用相同软件是可以接受的。

——如果既不存在功能多样性，也不存在纵深防御层次间的多样性，则应在保护系统内采用多样化设计。保护系统内的多样化设计可以采用计算机通道与非计算机通道的结合；也可以采用多样性的计算机。多样性的计算机可以通过采用不同的计算机功能规格书、不同的计算机硬件、

不同的计算机语言等来实现，以尽可能减小发生共因故障的可能性。

6.7 安全联锁与旁通

保护系统与其他有关系统之间应设置必要的安全联锁，以确保保护系统能够恰当地执行安全功能，仅当设计中预定的条件满足时，才能改变安全系统运行状态。系统保护动作信号仅作有条件的旁通，旁通操作应设有明显的状态显示。旁通有以下两种：

——运行旁通：为了满足不同运行工况的需要，可在一定条件下旁通部分功能。但只有在设计允许的条件满足时，才能实现要求的旁通。在执行旁通后，如果旁通条件失去，则旁通应自动失效或使系统进入安全状态。

——维修旁通：使用维修旁通时，应能确保保护系统不丧失自动保护功能。

6.8 保护动作的手动触发

安全功能都应设置手动触发动作作为自动触发的备份。手动触发电路与自动触发电路共用的部件应尽可能少，以保证自动触发电路中的故障不会阻碍手动触发功能的执行。

6.9 保护动作的完成

保护动作一旦被触发就应完成到底，仅当保护变量恢复到允许的整定值范围内时，系统才能手动复原。

6.10 与控制系统关系

应在保护系统内采取以下措施保证保护系统对于控制系统的独立性，防止控制系统对保护系统的不利影响。

——应尽量避免两者之间的相互连接，必须连接时应在保护系统内采取适当的隔离措施；

——安全级系统的测量仪表应尽可能独立设置，信号必须同时用于非安全级系统时，应在保护系统内可靠地隔离；

——数字化保护系统与数字化控制系统之间采用通信方式交换数据时，应在保护系统内采用通信隔离技术，且应保证数据只从保护系统向控制系统单向发送。

6.11 可试验性

6.11.1 总体要求

保护系统应设计成具有充分的自检功能，并具有可以进行在役试验的条件。检验的范围应包括从冗余通道的敏感元件到逻辑处理装置以及安全驱动器输出端的所有电路和设备。

6.11.2 在线自检

保护系统应设计成尽可能实现在线自检。在线自检是在保护系统工作的同时自动循环执行或通过内部的附加电路执行的对内部电路进行的检验。在电路模块的前面板上应有模块工作状况和诊断结果的指示。在控制室应有系统工作状况和诊断结果的指示。

6.11.3 在役试验

保护系统应设计成具有在役试验功能，允许运行人员在反应堆运行过程中对保护系统的部分电路进行功能试验。需要执行试验时，由操作员手动启动，试验过程自动完成。试验时间间隔的选择应满足系统可靠性目标的要求，试验的持续时间应尽量短。

在役试验只能逐个通道或逐“列”进行。一个通道或“列”在试验时，其余通道或“列”的试验功能应被闭锁(不允许投入试验)。

在役试验可分段进行，各段试验间应相互衔接并有覆盖。

对安全监测通道的在役试验可以通过冗余通道的读数互相校验进行。

在役试验时，如需将被试验部分旁通，则剩余部分仍应满足单一故障准则。

在役试验过程中，不得影响系统执行保护功能，也不得产生错误的保护触发信号。

试验时在主控制室内应有试验指示。

为试验目的在保护系统中附加的装置或线路，如与保护系统无可靠隔离措施，应满足安全级要求。

6.11.4 定期试验

少数试验项目(如测量通道的校验)允许在计划停堆期间进行。

6.12 质量保证和质量鉴定

保护系统的设备应按规定的质保大纲进行设计、制造、质量鉴定、安装、试验、运行和维修。质量保证文件需建立档案，并在整个反应堆寿期内妥善保存。

质量鉴定应符合 GB/T 12727 的要求。

数字化保护系统的安全软件验证与确认活动按照 IEEE Std 1012—2014 进行(软件完整性等级为 Level 4)。

6.13 对外部灾害的防护

保护系统设备及其安装场所应采取措施，防止火灾、地震、水淹和飞射物等外部事件对保护系统功能造成不利影响。冗余设备之间进行实体分隔，以防止外部事件引起系统保护功能共因失效。

6.14 电缆

保护系统的电缆应是低烟、无卤、阻燃的安全级电缆。

6.15 标识

保护系统的部件、设备及连接电缆应加鲜明的标识，以便清楚地与其他系统区别。保护系统内的冗余通道也应采用不同颜色的标识，以易于识别。

6.16 信息显示

应在主控制室提供保护系统有关的信息，包括：

——保护变量的状态，如动作整定值、当前值、事故状态；

——保护系统自身的状态，如投入、旁通、闭锁、故障等；

——触发动作及执行结果反馈；

——紧急停堆时应对导致停堆的保护变量有报警信号，并应有保护动作前 10 min 内重要参数的打印或记录；

——保护系统机柜门被打开也应在主控制室中有报警信号。

显示应置于运行人员便于观察的位置。这些信号的显示器可以是非安全级，但必须与保护系统可靠隔离。

6.17 电源

保护系统的冗余监测通道、冗余逻辑装置及驱动装置应由具有相同冗余度的、独立的安全级电源分

别供电。对供电状况应有状态指示，供电不正常时应有报警信号。

6.18 环境条件

保护系统装置应安装于按抗地震要求设计的设备间内。在各种设计基准事故下，设备间的环境条件（湿度、温度、压力及辐射等）应满足保护系统功能及性能有效性的要求。

7 基于计算机系统的补充要求

7.1 系统安全生存周期活动

为保证所有反应堆安全要求的获取、执行和维持，与保护系统研制、实现和运行有关的所有活动均应置于系统安全生存周期的框架中来完成。安全生存周期中一个阶段可再划分成若干个基本任务，每个任务均规定有明确的活动，一个阶段可在前一阶段活动完成之前开始，但该阶段只有在前面的各阶段已经完成并且它的输出与这些阶段活动所提供的输入相一致时才能结束。

7.2 系统确定性特征

基于计算机的系统设计应保证系统内部具有与执行功能要求相一致的预先确定性行为特征，具有承受某些不能预料运行情况的能力。如保证激励和响应之间的时间延迟存在最大和最小值，满足所有预期电厂瞬态数据负荷下的性能要求。

7.3 系统完整性

基于计算机的保护系统应设计成在所有可能造成保护功能失效的内外部条件下完成其保护功能，试验和校准功能不得对计算机完成其保护功能的能力产生不利影响。

7.4 安全性

只有经批准的人和系统才能访问保护系统计算机。对信息和数据未经许可的访问、修改、泄露以及恶意破坏，要求有安全性措施保护。

附 录 A
（资料性）
高温气冷堆反应堆保护系统结构框图

高温气冷堆反应堆保护系统包括从敏感元件到安全驱动器输入端的所有设备和线路，其构成分为：安全监测装置、安全逻辑装置和安全驱动装置，系统结构图见图 A.1。

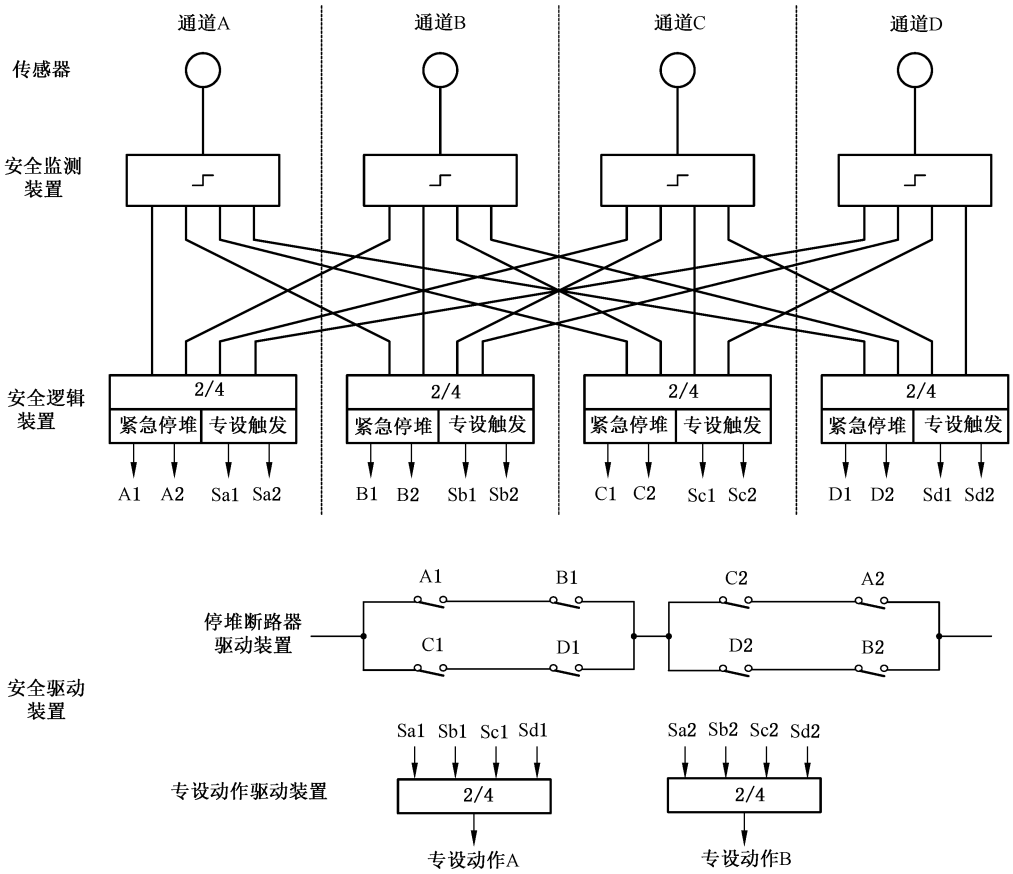

图 A.1 高温气冷堆反应堆保护系统结构框图

参 考 文 献

[1] GB/T 2423.2 系列电工电子产品环境试验 第2部分:试验方法 试验B:高温
[2] GB/T 4083—2005 核反应堆保护系统安全准则
[3] GB/T 5204—2008 核电厂安全系统定期试验与监测
[4] GB/T 12727—2017 核电厂安全级电气设备鉴定
[5] GB/T 12790—2008 核电厂安全级电气设备和系统文件标识方法
[6] GB/T 13284.1—2008 核电厂安全系统 第1部分:准则
[7] GB/T 13286—2008 核电厂安全级电气设备和电路独立性准则
[8] GB/T 13625—2018 核电厂安全系统电气设备抗震鉴定
[9] GB/T 13626—2008 单一故障准则应用于核电厂安全系统
[10] GB/T 13627—2010 核电厂事故监测仪表准则
[11] GB/T 13629—2008 核电厂安全系统中数字计算机的适用准则
[12] GB/T 17626(所有部分) 系列电磁兼容 试验和测量技术
[13] HAD 102/10—1988 核电厂保护系统及有关设施
[14] HAD 102/16—2004 核电厂基于计算机的安全重要系统软件
[15] HAF 102—2016 核动力厂设计安全规定
[16] EJ/T 1058—1998 核电厂安全系统计算机软件
[17] EJ/T 1060—1998 数字计算机在核电厂仪表和控制中的应用
[18] IEC 60880:2006 Nuclear power plants—Instrumentation and control systems important for safety—Software aspects for computer-based systems performing category A functions

中 国 核 学 会
团 体 标 准
高温气冷堆核动力厂反应堆保护系统设计准则
T/CNS 39—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:155066·5-3454　定价 18.00 元

T/CNS 39-2020