ICS 27.120.20
CCS F 83

# 中华人民共和国国家标准

GB/T 13629—2023
代替 GB/T 13629—2008

# 核电厂安全系统中可编程数字设备的适用准则

**Criteria for programmable digital devices in safety systems of nuclear power generating stations**

2023-12-28 发布　　2024-04-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件代替GB/T 13629—2008《核电厂安全系统中数字计算机的适用准则》，与GB/T 13629—2008相比，除结构调整和编辑性改动外，主要技术变化如下：

——更改了文件的适用范围，将“数字计算机”更改为“可编程数字设备”（见第1章，2008年版的第1章）；

——更改了术语“商品级物项”“固件”“危害”“危害分析”的定义（见第3章，2008年版的第3章）；

——删除了术语和定义“验收测试”“应用软件”“结构”“复杂性”“部件”“计算机”“计算机指令”“计算机程序”“计算机系统”“配置”“配置控制”“配置项”“配置管理”“正确性”“数据”“数据结构”“设计”“文件”“文档”“差错”“执行”“失效”“故障”“功能”“功能单元”“硬件”“实现”“接口”“模块”“规程”“鉴定试验”“需求”“需求规格书”“软件”“软件维护”“软件质量度量”“软件工具”“规格书”“系统”“系统软件”“系统试验”“试验”“试验大纲”“确认”“验证”“验证与确认”（见2008年版的第3章）；

——增加了术语和定义“安全状态”“功能状态”“关键特性”“基本部件”“可编程数字设备”“数字安全系统”（见第3章）；

——增加了缩略语（见3.2）；

——增加了针对单一故障的相关准则要求（见5.1）；

——更改了应用于数字装置、软硬件开发、固件和可编程逻辑设备开发所用到的软件工具内容（见5.3.3，2008年版的5.3.2）；

——增加了功能优先级的相关要求（见5.5.5）；

——增加了安全系统内部各冗余部分以及安全系统和其他系统之间独立性方面的详细规定（见5.6.5）；

——增加了3项试验和校准准则（见5.7）；

——增加了多序列控制和显示的相关要求（见5.8）；

——增加了安全系统在计算机安全防范方面的要求，特别给出了安全开发和运行环境的相关准则（见5.9）；

——增加了安全系统中与计算机相关的共因失效（CCF）的要求（见5.16）；

——增加了可编程设备和软件的商品级适用性确认要求（见5.17）；

——增加了安全系统简单性方面的要求（见5.18）。

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。

本文件由全国核仪器仪表标准化技术委员会（SAC/TC 30）提出并归口。

本文件起草单位：核工业标准化研究所、北京广利核系统工程有限公司、生态环境部核与辐射安全中心、国核自仪系统工程有限公司、中核控制系统工程有限公司。

本文件主要起草人：焦丽玲、程建明、张亚栋、杜乔瑞、王晓燕、杜建、邓瑞源、吴飞飞、裴红伟、武方杰、黄君龙、石秦、刘春明、王忠秋、耿文行、刘景宾、乔宁、任春香、刘志凯、王海峰。

本文件及其所代替文件的历次版本发布情况为：

——1998年首次发布为GB/T 13629—1998，2008年第一次修订；

——本次为第二次修订。

# 核电厂安全系统中可编程数字设备的适用准则

## 1 范围

本文件规定了可编程数字设备用于核电厂安全系统的设计准则，包括安全系统准则、监测指令设备的功能和设计要求、执行装置的功能和设计要求、对动力源的要求。

本文件适用于核电厂安全系统中的可编程数字设备。

## 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—2017 核电厂安全级电气设备鉴定

GB/T 13284.1—2008 核电厂安全系统 第1部分：设计准则

GB/T 13625—2018 核电厂安全级电气设备抗震鉴定

GB/T 22032—2021 系统与软件工程 系统生存周期过程

NB/T 20448—2017 核电厂系统和软件的验证和确认

ISO/IEC 12207:2017 系统和软件工程 软件生命周期过程（Systems and software engineering—Software life cycle processes）

## 3 术语和定义、缩略语

### 3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

**安全状态 safe state**

在其应用场景中被认为是安全的系统状态或符合核电厂安全分析的系统工况。

3.1.2

**功能状态 functional state**

由可编程数字设备（PDD）设计规定的部件或系统的运行状态。

注：包括运行模式、容错模式，以及测试/诊断/故障检测模式。

3.1.3

**固件 firmware**

硬件设备和驻留在此设备上的作为只读软件的计算机指令和数据的组合。

注：为与本文件一致，固件被当作可编程设备中的软件。

3.1.4

**关键特性 critical characteristic**

为了保证商品级物项可执行其预定安全功能，需验证物项重要的设计、材料和性能（包括设计过程）