ICS 27.120.99
CCS F 81

# 中华人民共和国国家标准

GB/T 41142—2021

# 核电厂安全重要数字仪表和控制系统硬件设计要求

**Hardware design requirements of computer-based instrumentation and control systems important to safety for nuclear power plants**

**（IEC 60987:2007，Nuclear power plants—Instrumentation and control important to safety—Hardware design requirements for computer-based systems，MOD）**

2021-12-31 发布　　2022-07-01 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。

本文件使用重新起草法修改采用IEC 60987：2007《核电厂　安全重要仪表和控制　基于计算机系统的硬件设计要求》。

本文件与IEC 60987：2007相比，在结构上有较多调整，附录A列出了本文件与IEC 60987：2007章条编号变化对照一览表。

本文件与IEC 60987：2007的技术性差异及其原因如下：

——关于规范性引用文件，本文件做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第2章“规范性引用文件”中，具体调整如下：

- 用GB/T 12727和GB/T 36044代替IEC 60780（见第8章）；
- 用修改采用国际标准的NB/T 20026—2014代替IEC 61513（见7.9、10.4、12.2）；
- 用修改采用国际标准的NB/T 20054代替IEC 60880（见4.4、5.2.3、7.9）；
- 用修改采用国际标准的NB/T 20055代替IEC 62138（见4.4、5.2.3、7.9）；
- 用GB/T 13626代替IAEA NS-G-1.3（见5.3.2）。

——删除了IEC 60987：2007中的部分术语和定义，以适应标准的需要；

——增加了术语“基于计算机的系统”“基于计算机的安全重要系统”（见3.1和3.2），以适应标准的需要；

——更改系统安全分级，由1级和2级更改为安全级系统和其他系统（见4.4、5.2.1、5.3.5、7.3.1、7.3.2、10.7），以适应我国技术现状；

——删除了4.3中“符合ISO 9001是满足这些需求的一种可接受的方法”，该内容与我国核电厂质量保证要求不符（见IEC 60987：2007的4.3）；

——删除了9.1.9中“国际”（见IEC 60987：2007/Amd 1：2013的9.1.9），以适用于我国认证的国情；

——更改了9.5.4.5中对尺寸控制和抽样检查计划的要求（见IEC 60987：2007/Amd 1：2013的9.5.4.5），以适应我国的技术条件，增加可操作性。

本文件做了下列编辑性改动：

——纳入了IEC 60987：2007/Amd1：2013的修正内容，所涉及的条款的外侧页边空白位置用垂直双线（‖）进行了标识；

——对第1章范围进行了编辑性的修改；

——删除了系统寿期总貌、鉴定示意图和维护程序举例（见IEC 60987：2007的附录A、附录B和附录C）；

——修改了参考文献。

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：中核控制系统工程有限公司、中国核动力研究设计院、北京广利核系统工程有限公司、国核自仪系统工程有限公司。

本文件主要起草人：王怀敬、刘瑞、梁嘉琳、孙武、景阳、刘艳阳、吴志强、江国进、郭春。

# 核电厂安全重要数字仪表和控制系统硬件设计要求

## 1 范围

本文件规定了核电厂基于计算机的安全重要系统硬件设计要求，包括硬件需求、设计和开发、验证和确认、鉴定、制造、安装和调试、运行、维护等相关内容。

本文件适用于核电厂基于计算机的安全重要系统硬件的设计，及对预开发硬件（包括固件）的评估；也适用于可编程逻辑器件的设计过程和设计验证。

本文件不适用于用于软件下载和检查的计算机硬件设施。

## 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

GB/T 13626 单一故障准则应用于核电厂安全系统

GB/T 36044 核电厂安全重要电气设备鉴定规程

NB/T 20026—2014 核电厂安全重要仪表和控制系统总体要求（IEC 61513:2011，MOD）

NB/T 20054 核电厂安全重要仪表和控制系统执行A类功能的计算机软件（NB/T 20054—2011，IEC 60880:2006，MOD）

NB/T 20055 核电厂安全重要仪表和控制系统执行B类和C类功能的计算机软件（NB/T 20055—2011，IEC 62138:2004，MOD）

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**基于计算机的系统 computer-based system**

其功能主要依靠或完全由使用微处理器、可编程电子设备或计算机来实现的仪表和控制（I&C）系统。

注：基于计算机的系统等同于数字系统、基于软件的系统、可编程系统。

[来源：NB/T 20026—2014，3.11]

3.2

**基于计算机的安全重要系统 computer-based system important to safety**

系统安全功能通过内置计算机系统实现的核动力厂安全重要系统。

[来源：HAD 102/16—2004，名词解释]

3.3

**固件 firmware**

硬件装置和以只读软件方式驻留在该装置中的计算机指令和数据的组合。