ICS 27.120.20
CCS F 83

中华人民共和国国家标准

GB/T 40444—2021

核电厂安全重要仪表和控制系统总体要求

General requirements for instrumentation and control systems important to safety in nuclear power plants

（IEC 61513:2011，Nuclear power plants—Instrumentation and control important to safety—General requirements for systems，MOD）

2021-10-11 发布　　2022-02-01 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 61513：2011《核电厂　安全重要仪表和控制　系统总体要求》。

本文件与IEC 61513：2011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，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：

- 用修改采用国际标准的GB/T 13630—2015代替IEC 60964(见5.2.2、5.2.4、5.4.2.3)；
- 用修改采用国际标准的GB/T 15474—2010代替IEC 61226(见5.2.3.1、5.4.2.6、6.2.1、6.5.3.3、附录B)；
- 用修改采用国际标准的GB/T 13631代替IEC 60965(见5.4.2.3)；
- 用修改采用国际标准的NB/T 20060代替IEC 60709(见5.4.2.4、6.2.2.3.2、6.2.3.3.3)；
- 用修改采用国际标准的NB/T 20342代替IEC 61500(见5.4.2.4)；
- 用修改采用国际标准的NB/T 20054—2011代替IEC 60880(见5.4.2.5、5.4.4.2、5.6.2、6.1、6.2.2.3.3、6.2.2.3.4、6.2.2.7、6.2.3.2、6.2.3.3.4、6.2.3.4、6.2.4.1、6.2.6、6.2.8、6.3.2.1、6.3.2.2、6.3.5、6.4.2.2、6.4.4.1、6.5.3.3、8.2)；
- 用修改采用国际标准的NB/T 20055—2011代替IEC 62138(见5.4.2.5、5.6.2、6.1、6.2.2.3.3、6.2.2.7、6.2.3.2、6.2.3.4、6.2.4.1、6.2.8、6.3.2.1、6.4.4.1、6.5.3.3、8.2)；
- 用修改采用国际标准的NB/T 20068代替IEC 62340(见5.4.2.6、6.2.2.3.2、6.2.3.3)；
- 用等同采用国际标准的GB/T 17626.1代替IEC 61000-4-1(见5.5.4.2、6.5.3.2)；
- 用等同采用国际标准的GB/T 17626.2代替IEC 61000-4-2(见5.5.4.2、6.5.3.2)；
- 用等同采用国际标准的GB/T 17626.3代替IEC 61000-4-3(见5.5.4.2、6.5.3.2)；
- 用等同采用国际标准的GB/T 17626.4代替IEC 61000-4-4(见5.5.4.2、6.5.3.2)；
- 用等同采用国际标准的GB/T 17626.5代替IEC 61000-4-5(见5.5.4.2、6.5.3.2)；
- 用等同采用国际标准的GB/T 17626.6代替IEC 61000-4-6(见5.5.4.2、6.5.3.2)；
- 用修改采用国际标准的NB/T 20298—2014代替IEC 60987(见6.1、6.2.1、6.2.2.3.4、6.2.2.3.6、6.2.3.2、6.2.4.1、6.2.8、6.3.6、6.4.4.1、6.5.3.3、8.2)；
- 用等同采用国际标准的GB/T 19001代替ISO 9001(见6.3.2.1)；
- 增加引用了GB/T 12727(见6.5.3.2)和GB/T 13625(见6.5.3.2)；
- 删除了IEC 60780和IEC 60980。

——为适应我国的技术条件，本文件对第3章的“术语和定义”内容做了部分调整，具体调整如下：

- 修改了共因故障、多样性、安全重要物项、假设始发事件、安全系统、单一故障的定义，采用HAF 102(2016)中的定义(见3.8、3.15、3.33、3.35、3.44、3.46)；
- 修改了调试、质量保证的定义，采用HAF 003(1991)中的定义(见3.7、3.39)；
- 修改了安全组的定义，采用GB/T 13284.1—2008中的定义(见3.43)；
- 修改了部件、配置管理的定义，采用GB/T 13629—2008中的定义(见3.10、3.12)；
- 修改了通道、冗余、单一故障准则、型式试验的定义，采用GB/T 4960.6—2008中的定义(见3.5、3.40、3.47、3.56)；

- 修改了(系统特性的)评价的定义,采用 GB/T 18272.1—2000 中的定义(见 3.19);
- 修改了质量的定义,采用 GB/T 19000—2016 中的定义(见 3.38);
- 修改了可靠性的定义,采用 GB/T 7163—2008 中的定义(见 3.41);
- 修改了差错、失效、故障的定义,采用 GB/T 11457—2006 中的定义(见 3.18、3.20、3.21);
- 修改了要求的定义,采用 GB/T 1.1—2020 中的定义(见 3.42)。

——删除了第 4 章中部分正文中未使用的缩略语。

本文件做了下列编辑性修改:

——按照 GB/T 1.1—2020 的要求,规范了第 1 章的编写;

——删除了第 3 章“术语和定义”的部分注释;

——将 5.2.3.1 注 2 中“不同国家对功能分类的规范性引用文件可能不同,并可能与本文件的引用文件(IEC 61226)不同”修改为“不同实践的功能分类方法可能不同”;

——将 A.4 中纵深防御描述修改为和 HAF 102(2016)一致;

——删除附录 B 中“IAEA NS-G-1.3 将这种分级理念扩展到仪表和控制系统。将 I&C 系统分为安全重要系统和非安全重要系统。然后,又将安全重要系统细分为‘安全系统’和‘安全有关系统’,并提出了设计要求。”及“IAEA 规定的级别数目与 IEC 61226:2009 不同(安全系统和安全有关系统对应 A、B 和 C 类)。并且 IAEA 和 IEC 使用的定义和概念也不同(IAEA 的系统分级对应 IEC 的功能分类/系统分级),而这些差异可能导致不同的解释。”

——删除了附录 D 和附录 E。

——根据本文件实际参考内容,对参考文献进行了调整。

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:中广核工程有限公司、中国核电工程有限公司、上海核工程研究设计院有限公司。

本文件主要起草人:黄伟军、张龙强、傅涛、周亮、彭华清、张黎明、张睿琼、谭珂、江辉、刘光明、李公杰、孙伟、赵岩峰、田勇、谢红云、杜德君、郑伟、张玉峰、张淑慧。

引　言

安全重要仪表和控制(I&C)系统可采用传统的基于模拟技术的设备、基于计算机技术的设备或这两类设备的组合实现。本文件对安全重要I&C系统的总体架构提出要求和建议，适用于包含上述任一项技术的I&C系统。

本文件强调了根据核电厂安全目标导出安全重要I&C系统完整和准确要求的必要性，这是制定I&C总体架构的总体要求、并进而制定单个安全重要I&C系统要求的前提。

本文件提出了I&C总体架构的安全生命周期以及单个系统安全生命周期的概念。它着重说明核电厂安全目标与安全重要I&C系统总体架构要求之间的关系，以及I&C总体架构与单个安全重要I&C系统要求之间的关系。

本文件描述并遵循的生命周期并不是唯一可行的生命周期，只要本文件中规定的目标得到满足，也可以遵循其他生命周期。

本文件主要核心技术要素包括以下4个章节(图1给出了整体框架结构)：

——第5章叙述安全重要I&C系统总体架构：

- 根据核电厂安全分析确定I&C的功能需求以及有关的系统和设备，并确定I&C功能分类、电厂布置和运行环境；
- 建立I&C的总体架构，将其划分为多个系统并将I&C功能分配给系统。确定设计准则，包括提供纵深防御和最大限度降低共因故障(CCF)可能性的准则；
- 设计I&C系统的总体架构。

——第6章叙述单个安全重要I&C系统的要求，特别是基于计算机系统的要求。其中，对单个安全重要I&C系统的要求依据其所执行功能的安全类别而有所区别。

——第7章和第8章叙述安全重要I&C系统的总的集成、调试、运行和维护。

本文件包括3个资料性附录：

——附录A给出了核电厂安全重要I&C系统设计考虑的主要安全概念；

——附录B提供关于功能分类和系统分级原则的说明；

——附录C列举了安全重要I&C系统对CCF敏感的例子，并给出了防御CCF的定性方法。

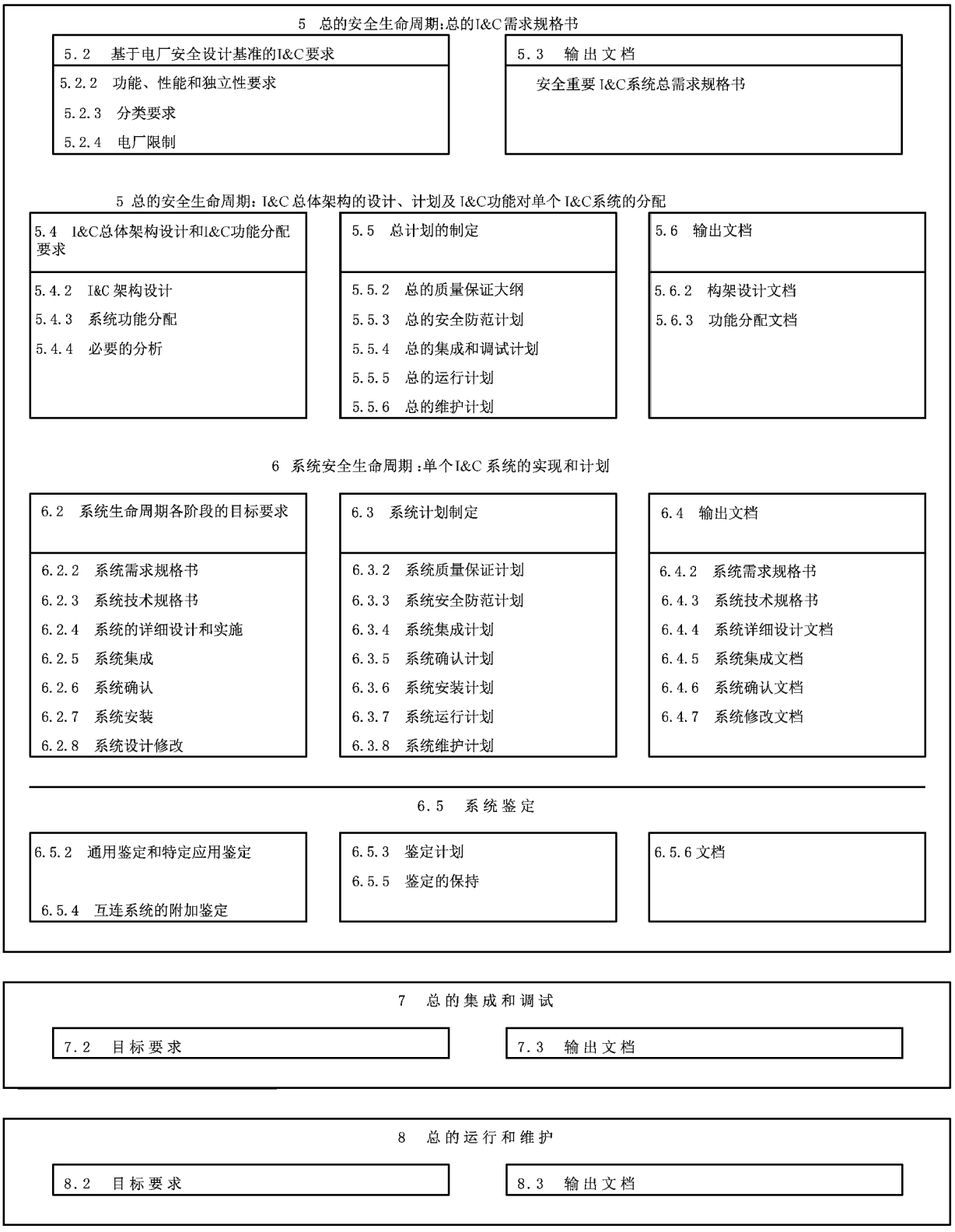
5 总的安全生命周期:总的I&C需求规格书
5.2 基于电厂安全设计基准的I&C要求
5.2.2 功能、性能和独立性要求
5.2.3 分类要求
5.2.4 电厂限制
5.3 输出文档
安全重要I&C系统总需求规格书
5 总的安全生命周期:I&C总体架构的设计、计划及I&C功能对单个I&C系统的分配
5.4 I&C总体架构设计和I&C功能分配要求
5.4.2 I&C架构设计
5.4.3 系统功能分配
5.4.4 必要的分析
5.5 总计划的制定
5.5.2 总的质量保证大纲
5.5.3 总的安全防范计划
5.5.4 总的集成和调试计划
5.5.5 总的运行计划
5.5.6 总的维护计划
5.6 输出文档
5.6.2 构架设计文档
5.6.3 功能分配文档
6 系统安全生命周期:单个I&C系统的实现和计划
6.2 系统生命周期各阶段的目标要求
6.2.2 系统需求规格书
6.2.3 系统技术规格书
6.2.4 系统的详细设计和实施
6.2.5 系统集成
6.2.6 系统确认
6.2.7 系统安装
6.2.8 系统设计修改
6.3 系统计划制定
6.3.2 系统质量保证计划
6.3.3 系统安全防范计划
6.3.4 系统集成计划
6.3.5 系统确认计划
6.3.6 系统安装计划
6.3.7 系统运行计划
6.3.8 系统维护计划
6.4 输出文档
6.4.2 系统需求规格书
6.4.3 系统技术规格书
6.4.4 系统详细设计文档
6.4.5 系统集成文档
6.4.6 系统确认文档
6.4.7 系统修改文档
6.5 系统鉴定
6.5.2 通用鉴定和特定应用鉴定
6.5.4 互连系统的附加鉴定
6.5.3 鉴定计划
6.5.5 鉴定的保持
6.5.6 文档
7 总的集成和调试
7.2 目标要求
7.3 输出文档
8 总的运行和维护
8.2 目标要求
8.3 输出文档

图 1 本文件的整体结构

核电厂安全重要仪表和控制系统总体要求

1 范围

本文件确立了核电厂安全重要仪表和控制(I&C)系统的总体要求,规定了总的I&C安全生命周期、系统安全生命周期、总的集成和调试、总的运行和维护。

本文件适用于新建核电厂安全重要I&C系统。对于现有核电厂安全重要I&C系统的升级或改造可参照使用,适用的要求宜在项目的开始阶段予以确定。

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 13625 核电厂安全级电气设备抗震鉴定

GB/T 13630—2015 核电厂控制室设计(IEC 60964:2009,MOD)

GB/T 13631 核电厂辅助控制点设计准则(GB/T 13631—2015,IEC 60965:2009,MOD)

GB/T 15474—2010 核电厂安全重要仪表和控制功能分类(IEC 61226:2005,MOD)

GB/T 17626.1 电磁兼容 试验和测量技术 抗扰度试验总论(GB/T 17626.1—2006,IEC 61000-4-1:2000,IDT)

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 17626.2—2018,IEC 61000-4-2:2008,IDT)

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 17626.3—2016,IEC 61000-4-3:2010,IDT)

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 17626.4—2018,IEC 61000-4-4:2012,IDT)

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 17626.5—2019,IEC 61000-4-5:2014,IDT)

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 17626.6—2017,IEC 61000-4-6:2013,IDT)

GB/T 19001 质量管理体系 要求(GB/T 19001—2016,ISO 9001:2015, IDT)

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

NB/T 20055—2011 核电厂安全重要仪表和控制系统 执行B类或C类功能计算机系统的软件(IEC 62138:2004, MOD)

NB/T 20060 核电厂安全重要仪表和控制系统隔离(NB/T 20060—2012,IEC 60709:2004,MOD)

NB/T 20068 核电厂安全重要仪表和控制系统应对共因故障的要求(NB/T 20068—2012,IEC 62340:2007,MOD)