ICS 27.120.20
F 83

中华人民共和国国家标准

GB/T 13629—1998

核电厂安全系统中数字计算机的适用准则

Applicable criteria for digital computers in safety systems of nuclear power plants

1998-11-17 发布　　1999-07-01 实施

国家质量技术监督局 发布

目　　次

前言 …… I
IEEE 前言 …… II
1 范围 …… 1
2 引用标准 …… 1
3 定义 …… 1
4 安全系统设计基准 …… 2
5 安全系统准则 …… 2
6 监测指令设备的功能和设计要求 …… 5
7 执行装置的功能和设计要求 …… 5
8 对动力源的要求 …… 5
附录 A(提示的附录) 本标准与 GB 13284—1998 的相互关系 …… 6
附录 B(提示的附录) 多样性需求的确定 …… 7
附录 C(提示的附录) 抗电磁干扰能力 …… 7
附录 D(提示的附录) 现有商品级计算机的质量鉴定 …… 9
附录 E(提示的附录) 验证与确认 …… 11
附录 F(提示的附录) 异常状态和事件的鉴别和解决 …… 17
附录 G(提示的附录) 通信独立性 …… 22
附录 H(提示的附录) 计算机可靠性 …… 24
附录 I(提示的附录) 核电厂用计算机软件的质量保证要求 …… 27
附录 J(提示的附录) 本标准附录中引用的标准 …… 31

前　言

本标准等效采用 IEEE Std 7-4.3.2—1993“Criteria for Digital Computers in Safety Systems of Nuclear power Generating Stations”，技术内容等同，编写方法和格式符合 GB/T 1.1—1993 的要求。

与 IEEE7-4.3.2 相比，本标准的基本结构和内容未变，只是将 IEEE 7-4.3.2 中引用标准改为相应的我国标准，将 ASME NQA-2a—1990 part 2.7 增加作为本标准附录 I，将附录中引用的有关标准目录增加作为本标准的附录 J。

本标准与下列标准结合使用，能对核电厂数字化仪表和控制系统提供指导：

- GB 13284—1998(eqv IEEE 603—1991)　核电厂安全系统准则
- EJ/T 529—1990(eqv IEC 987—1989)　用于核电厂安全重要系统数字计算机
- EJ/T 694—1992(eqv IEEE 730—1989)　核工业计算机软件质量保证规范
- EJ/T 743—1993(eqv IEEE 828—1990)　核工业计算机软件配置管理计划编制指南
- EJ/T 890—1994(eqv IAEA 282 号技术报告)　核电厂安全有关计算机软件质量保证细则
- EJ/T 1058—1998(eqv IEC 880—1986)　核电厂安全系统计算机软件
- EJ/T 1060—1998(eqv IEC 643—1979)　数字计算机在核电厂仪表和控制中的应用

本标准的附录 A～附录 J 都是提示的附录。

本标准由全国核仪器仪表标准化技术委员会提出并归口。

本标准起草单位：国家科委核安全中心。

本标准主要起草人：耿文行、王忠秋。

IEEE 前言

本前言不是 IEEE Std 7-4.3.2—1993"Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"的组成部分。

本标准规定了计算机的附加特定要求(包括硬件、软件、固件和接口),以补充 IEEE603—1991 的准则和要求。当计算机用作安全系统的设备时,本标准应与 IEEE 603—1991 一起使用以保证安全系统设计的完整性。

本标准所述的计算机特定要求只适用于作为安全系统设备的计算机,不一定适用于整个核电厂运行所需的所有计算机。本标准 5.5 和 5.6 要求对安全系统中的计算机进行保护,以免受非安全计算机故障的影响,对非安全计算机没有特殊的安全要求。但是,许多原则适用于核电厂的其他重要系统,这些原则同 IEEE 603—1991 规定的原则是一致的。

本标准对计算机在安全系统级的应用规定了设计要求。本标准的附录提供了在设计技术和方法方面的详细信息,以满足各种准则和要求。本标准考虑了计算机系统持续不断的发展过程,因此不应把本标准提供的信息视为唯一的解决办法。只要满足 IEEE 603—1991 与本标准的准则和要求,就希望使用数字技术方面的新成果。例如,虽然本标准并未特别涉及到人工智能系统和第四代语言,但并不排除它们的应用。

本标准不适用于安全系统设计过程中使用的工程软件,对这类软件应参考 ASME NQA-2a—1990 第 2.7 部分(以下简称为第 2.7 部分)。

演变

本标准由 ANSI/IEEE-ANS-7-4.3.2—1982"Application Criteria for Programmable Digital Computer systems in Safety Systems of Nuclear Power Generating Stations"演变而来的,它体现了 IEEE/ANSI 联合工作组为支持核电厂安全系统中计算机的规格书、设计和实施所作出的持续不断的努力。

ANSI/IEEE-ANS-7.4.3.2—1982 详细讨论了对硬件和软件进行集成的研制过程。其中主要讨论了第 2.7 部分中详述的活动,参考第 2.7 部分提出具体的软件研制要求。为了研制出可靠的、高质量的软件并尽量减少设计差错,应对软件研制规定质量要求。

应明确指出,本标准并不提供关于计算机安装后运行和维修的要求(例如监督试验频度),发现任何问题应分别按相应的硬件和软件标准 ASME NQA-1—1989 和 ASME NQA-2a—1990 第 2.7 部分中的适当要求来处理。

与其他标准的关系

本标准编制过程中采用了 IEEE 标准和其他标准。在本标准及其支持性附录中注明了这些标准。

本标准引用了第 2.7 部分(除第 7 章和 10.2 以外),以提出质量准则的某些见解。这样做的依据有:

a) 第 2.7 部分的第 3 章和第 4 章清楚地指出在整个软件研制过程中应进行验证和确认(V&V)。第 7 章说明了在软件研制过程中进行验证审查的要求,这可以解释为对第 3 章和第 4 章所述要求的附加要求。因此工作组认为,这可以解释为第 3 章和第 4 章所述的 V&V 不足以符合 ASME NQA-1—1989 的设计验证要求。在第 2.7 部分的表决过程中,IEEE NPEC(核动力工程委员会)注意到 V&V 在多章中作了讨论,建议合并 V&V 的要求;

b) 在讨论商品级物项适用性确认的过程中,工作组认为第 2.7 部分的 10.2 节规定的过程能处理

商品级软件的适用性确认。但由于这节有可能被申请者不正确地使用，因此目前正在修订之中。据此工作组认为，赞同这一节是不合适的。

非预期的功能

第 2.7 部分第 4 章使用了定义“非预期功能”，该定义可解释为：

a) 无用的驻留功能

设计过程应处理任何无用的驻留功能，见 5.6。在某些情况下，例如对于操作系统和编译程序，当可能不知道总的数量时，V&V 过程对于处理无用的驻留功能是不适宜的。

b) 对外部或内部条件的不可预测响应

在设计过程中应对外部或内部条件的不可预测响应进行鉴别并形成文件，并采取适当措施加以解决。然后，应通过 V&V 过程来确认对这些条件作出的适当响应。

c) 由于设计或实施错误产生的缺陷

需要由 V&V 过程来处理由于设计或实施错误引起的缺陷。

d) 未从软件中消除的研制辅助手段

应作出有文件依据的判断，以便说明是否将研制辅助手段保留在软件中。如果决定将研制辅助手段保留在软件中，则可以使它们运行或不运行。无论何种情况，如果决定将研制辅助手段保留在软件中，则要求进行 V&V。

共因故障/多样性

IEEE 603—1991 的 5.1 规定了单一故障准则，IEEE 379—1988 给出了对这一准则应用的指导。IEEE 379—1988 的 5.5 提出了在单一故障分析中要考虑共因故障的要求，其中说明，不进行单一故障分析的“共因故障”包括那些可能由“设计缺陷、制造差错”等引起的故障，准备用设计鉴定、质量保证大纲来预防这些缺陷和差错。这种方法对于按 IEEE 603—1991 和本标准的要求研制的计算机硬件和软件有关的潜在共因故障也是适合的。

在本标准的制定过程中，工作组花费了很多时间讨论用多样性来处理潜在共因故障的必要性。工作组认为存在适合应用多样性的实例。一项安全功能的所有控制设备应用同样结构来实现的情况就是应考虑用多样性来防止共因故障的一个实例。这可以从 IEEE 379—1988 的前言推断出来，该前言中说明：“如果确认当一起考虑任务需求率和共因故障率时某些后果可能不可接受，则可使用其他的措施。在这些情况下，使用如多样性的设计技术来提出可接受的设计”。附录 B 给出了关于确定多样性需求的补充指导。

电磁环境

本标准要求瞬态和稳态条件的范围应包括电磁环境（含静电放电），作为 IEEE603—1991 第 4.7 节举例的补充。在本标准表决过程中，已注意到这是安全系统的问题而不是只有计算机才有的问题。因此建议从本标准中删去这一主题而包括到 IEEE 603—1991 年的修订版中。SC6 主席已同意将这一问题同 IEEE 603—1991 的下次修订一起考虑。但是，工作组和 SC6 主席认为这是一个很重要的问题，至少在 IEEE 603—1991 处理这一问题之前将其保留在本标准中。

商品级物项适用性确认

在本标准表决过程中，对商品级物项适用性确认要求的必要性表示了关切。作为审查 ASME NQA-1C—1993 附录 7A-2 的结果，工作组决定，为了确定商品级物项在安全系统中应用的可接受性，

仅进行试验是不够的。因此，已把软件研制方法的考虑作为商品级物项适用性确认过程的组成部分。商品级物项适用性确认还要求制造商对现有产品进行质量鉴定。这两项要求对未按本标准研制的计算机在安全系统中应用的评价提供坚实的依据。

未来的工作

在第 2.7 部分下次修订后，工作组应考虑目前对 2.7 部分所述例外的适宜性问题。这应是有意全面赞成第 2.7 部分。

在本标准的制定过程中，工作组考虑了许多人因方面的问题。由于颁布了 IEEE 603—1991，突出了对这一问题的关注。IEEE 603—1991 要求把人因同安全系统准则一起考虑。同 SC7 成员进行了讨论，以确定工作组应采取怎样的行动。SC7 目前正在进行重新确认工作和编制关于 CRT 的标准。在本标准表决过程中，再一次提出了对人因问题的关切，已将这些意见转交给 SC7 作为他们工作的输入。

工作组建议将分级要求增加到 IEEE 603—1991 中。这一思想已被美国核管会审评人员在 SECY-91-192“先进轻水堆数字计算机系统”中所认可。在 ANSI/ANS 51.1—1983 和 ANSI/ANS 52.1—1983 中也提出了类似的安全分级概念。在修订 IEEE 603—1991 时应将这一概念应用到该标准中。

在本标准表决过程中还提出了关于软件共因故障的问题。虽然附录 B 给出了关于处理共因故障的多样性要求的某些考虑，但对多样性的考虑尚未达到应有的程度。工作组和某些表决者认为，对多样性的要求是一个安全系统级的问题。因此，工作组建议在修订 IEEE 603—1991 时考虑这一问题。

本标准没有涉及软件工具选择的合理性以及编译程序、操作系统和程序库的验收准则。工作组认为这一主题超出了他们的职责范围，因此工作组建议编制标准来讨论这些要求。

在本标准表决过程中，提出了关于接地技术的标准适宜性问题。工作组认为这一问题超出了本标准的范围。因此，建议编制另一标准来处理这一问题。

在本标准表决过程中，要求区分对同一计算机上运行的安全软件与非安全软件的要求。在 5.6 和附录 G 中引入了软件屏障概念，作为分隔这两类软件的一种措施。据工作组了解，尚无工业标准能适当地处理这一问题。工作组建议把处理这一主题的标准纳入到未来的编制计划中。

中华人民共和国国家标准

核电厂安全系统中数字计算机的适用准则

GB/T 13629—1998

Applicable criteria for digital computers in safety systems of nuclear power plants

1 范围

本标准规定了计算机用作核电厂安全系统设备时的有关准则。

GB 13284—1998 规定了核电厂安全系统(动力源、仪表和控制部分)最低限度的功能和设计要求,但不包括计算机用作安全系统组成部分时的附加要求。本标准用来补充这方面的要求,与 GB 13284—1998 一起规定了计算机用作安全系统设备时的最低功能要求和设计要求。

在本标准范围内,术语"计算机"是一个包括计算机硬件、软件、固件和接口的系统。

2 引用标准

下列标准所包含的条文,通过在本标准中引用而构成为本标准的条文。本标准出版时,所示版本均为有效。所有标准都会被修订,使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 7163—1987 核反应堆保护系统的可靠性分析要求

GB/T 9225—1988 核反应堆保护系统可靠性分析一般原则

GB/T 12788—1991 核电厂安全级电力系统准则

GB 13284—1998 核电厂安全系统准则

GB/T 13626—1992 单一故障准则用于核电厂 安全级电气系统

EJ/T 694—1992 核工业计算机软件质量保证规范

EJ/T 743—1993 核工业计算机软件配置管理计划编制指南

EJ/T 797—1993 人因工程原则在核电厂系统、设备和设施中的应用

EJ/T 1058—1998 核电厂安全系统计算机软件

HAF 0400(91) 核电厂质量保证安全规定

3 定义

本标准采用下列定义。

3.1 商品级物项 commercial grade item

满足下述条件的物项:

a) 不是为核设施专门设计或不以核设施特有的技术要求为条件;

b) 用于非核设施;

c) 按制造厂产品说明(例如样本)中规定的技术条件从制造厂或供货商处采购。

3.2 商品级物项适用性确认 commercial grade dedication

为了充分确信商品级物项适合于核安全应用,对商品级物项进行评价(包括测试)和验收的过程。

国家质量技术监督局 1998-11-17 批准 1999-07-01 实施