ICS 27.120.20
F 83

中华人民共和国国家标准

GB/T 13629—2008
代替 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

2008-07-02 发布　　2009-04-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准修改采用美国标准 IEEE Std 7-4.3.2-2003《核电厂安全系统中数字计算机的适用准则》(英文版),技术内容等同,只是将 IEEE Std 7-4.3.2 中引用的美国标准改为相应的我国标准,编写方法和格式符合 GB/T 1.1—2000 的要求。

本标准代替 GB/T 13629—1998《核电厂安全系统中数字计算机的适用准则》。

本标准与 GB/T 13629—1998 相比主要变化如下:

——第 5 章中增加了 5.3.6“软件工程风险管理”和 5.5.3“故障探测和自诊断”;将独立验证与确认的内容放入正文,增加了 5.3.4“独立验证与确认要求”,而删除了附录 E“验证与确认”;将取消的5.3.2“现有商品级计算机的质量鉴定”修订为 5.4.2,并细化了相关的要求;

——取消了附录 C“抗电磁干扰能力”;

——将附录 F“异常状态和事件的鉴别和解决”修订为附录 D“危害的鉴别和解决”,并重新编写了该附录;

——取消了附录 I“核电厂用软件的质量保证要求”;

——取消了附录 J“本标准附录中引用的标准”。

本标准的附录 A、附录 B、附录 C、附录 D、附录 E、附录 F 都是资料性附录。

本标准由中国核工业集团公司提出。

本标准由全国核仪器仪表标准化技术委员会(SAC/TC 30)归口。

本标准起草单位:核工业标准化研究所。

本标准主要起草人:高丽艳、王忠秋、耿文行。

本标准所代替标准的历次版本发布情况为:

——GB/T 13629—1998。

核电厂安全系统中数字计算机的适用准则

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一般原则。

本标准的要求与 GB/T 13284.1—2008 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。

本标准适用于核电厂安全系统数字计算机。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 9225 核电厂安全系统可靠性分析一般原则(GB/T 9225—1999，eqv ANSI/IEEE Std 352-1987)

GB/T 13284.1—2008 核电厂安全系统 第1部分：设计准则(IEEE Std 603-1998，NEQ)

GB/T 13286 核电厂安全级电气设备和电路独立性准则(GB/T 13286—2001，eqv ANSI/IEEE Std 384-1992)

EJ/T 694 核工业计算机软件质量保证规范

EJ/T 743 核工业计算机软件配置管理计划编制指南

EJ/T 1058 核电厂安全系统计算机软件

HAF 003 核电厂质量保证安全规定

IEEE Std 1012-1998 软件验证与确认的 IEEE 标准

IEEE Std 1061-1998 软件质量度量方法的 IEEE 标准

IEEE Std 1042 软件配置管理的 IEEE 指南

IEEE Std 1540 生存周期过程的 IEEE 标准—风险管理

IEEE/EIA 12207.0-1996 信息技术标准—软件生存周期

3 术语和定义

下列术语和定义适用于本标准。

3.1

验收试验 acceptance testing

1) 为确定系统是否满足验收准则并使客户确定是否接收该系统而进行的正规试验(也可参见鉴定试验、系统试验)；

2) 为使用户、客户或其他授权机构确定是否接收一个系统或设备而进行的正规试验。

3.2

应用软件 application software

为满足某一用户特定的需要而设计的软件，例如用于导航、薪金表或过程控制的软件。

3.3

结构 architecture

系统或部件的组织结构。

3.4

商品级物项 commercial grade item

满足下述条件的物项：

1) 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；

2) 用于非核设施；

3) 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。

3.5

商品级物项适用性确认 commercial grade item 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和验收的过程。

3.6

复杂性 complexity

1) 对一个系统或系统部件的设计或实现难于理解或验证的程度；

2) 测量定义 1)中属性的任一组基于结构性的度量。

3.7

部件 component

组成系统的一个部分。一个部件可以是硬件或软件，并可以再细分成其他的部件。

注：术语“模块”、“部件”和“单元”通常可相互交换使用，或取决于上下文，以不同的方式作为另外一个定义的补充。这些术语的相互关系尚没有标准化。

3.8

计算机 computer

由一个或多个关联的处理单元和外部设备组成的、由内部贮存的程序控制的、不用人为干预便能执行真实计算(包括大量的算术运算或逻辑运算)的功能可编程装置。

3.9

计算机指令 computer instruction

1) 编程语言中的语句，它规定了计算机执行的操作，以及与操作数有关的地址或数值，例如将 A 移动到 B；

2) 简单地说，计算机程序中任何可执行的语句。

3.10

计算机程序 computer program

可使计算机硬件执行运算或控制功能的计算机指令和数据定义的组合。

3.11

计算机系统 computer system

包含一个或多个计算机及相关软件的系统。

3.12

配置 configuration

1) 由数字、属性定义的计算机系统或部件的排列，及其各组成部分之间的相互联系；

2) 在配置管理中，是指在技术文件中规定的或产品达到的硬件或软件的功能和物理特性。

3.13

配置控制 configuration control

配置管理的一个要素，包括在配置项的配置标识正式建立后对配置项变更的评价、协调、批准或不批准，以及实施。

3.14

配置项 configuration item

在配置管理过程中指定要进行配置管理并作为一个整体处理的硬件、软件或两者兼有的集合体。

3.15

配置管理 configuration management

采用技术及行政管理和监督的一种规定，以识别或用文件证明配置项的功能和物理特性、控制对这些特性的变更、记录和报告变更过程和实施状态，并核实与规定要求的一致性。

3.16

正确性 correctness

1) 在系统或部件的技术规范、设计和实现中无缺陷的程度；

2) 软件、文档或其他物项满足技术要求的程度；

3) 无论规定与否，软件、文档或其他物项满足用户需求和预期的程度。

3.17

数据 data

1) 以易于交流、理解，或被人员/自动手段处理的方式对事实、概念或指令的一种表达方式；

2) 有时用作文档的同义词。

3.18

数据结构 data structure

数据各元素之间的物理或逻辑关系，用于支持特定的数据处理功能。

3.19

设计 design

1) 确定一个系统或部件结构、组成、接口和其他属性的过程；

2) 定义 1)中过程的结果。

3.20

文件 document

1) 一种介质及其所记录的信息，通常有永久性并可被人或机器读出。例如在软件工程中包括工程计划、规范、试验计划和用户手册；

2) 创建在 1)中定义的一个文件；

3) 向计算机程序中添加注释。

3.21

文档 documentation

1) 某一特定主题的文件集合；

2) 对活动、要求、过程或结果进行描述、规定、说明、报告或证明的任何文字的或图表资料；

3) 文件产生或修订的过程；

4) 文件管理，包括标识、收集、处理、储存和分发。

3.22

差错 error

1) 一个计算的、观测的或实测的数值或条件与真实的、规定的或理论的数值或条件之间的差异，例如，计算结果与正确值之间差 30 m；

2) 不正确的步骤、过程或数据定义，例如在计算机程序中不正确的指令；

3) 不正确的结果，例如当正确值为 10 时计算值为 12；

4) 产生不正确结果的人的行为。例如在编程器或操作器上的错误动作。

注：当 4 个定义共同使用时，通常将定义 1)称为误差，将定义 2)称为故障，将定义 3)称为失效，将定义 4)称为失误。

3.23

执行 execution

计算机完成计算机程序中一条或多条指令的过程。

3.24

失效 failure

一个系统或部件不能在规定的性能要求内执行所要求的功能。

注：故障容错规则区分人的行为(失误)、其表现形式(硬件或软件故障)、故障的后果(失效)，以及其结果为不正确(差错)的总量。

3.25

故障 fault

1) 在硬件或部件中的缺陷，例如短路或断线；

2) 在计算机程序中的不正确的步骤、过程或数据定义。

注：该定义主要由故障容错理论使用，在通常情况下，差错和隐错用于表达同一含义。

3.26

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。

3.27

功能 function

一个系统或部件规定的目的或作用。例如，一个系统可将总量控制作为其主要的功能。

3.28

功能单元 functional unit

能完成一个规定目的的硬件、软件或两者兼有的实体。

3.29

硬件 hardware

用于处理、贮存或传输计算机程序或数据的物理设备。

3.30

危害 hazard

事故的一种先决条件。危害包括外部事件以及计算机硬件和软件的内在条件。

3.31

危害分析 hazard analysis

研究和确定由正常的设计审查和测试过程未鉴别出来的条件的过程。通过对包括异常事件和带有劣化的设备和系统的核电厂运行的分析，使危害分析的范围扩展到核电厂超设计基准事件。危害分析主要关注系统的故障机理而不是验证正确的系统运行。

3.32

实现 implementation

1) 将设计转化为硬件设备、软件设备，或两者兼有的过程；

2) 定义 1)过程的结果。

3.33

接口 interface

1) 信息通过的共享边界；

2) 用于将信息从一个部件传输到其他部件为目的的，连接两个或多个部件的硬件或软件设备。

3.34

模块 module

1) 就编译、与其他单元的组合及下载而言是分离的和可标识的程序单元。例如向一个汇编程序、编译器、连接编辑器或执行程序的输入，或从其来的输出；

2) 一个程序中逻辑上可分离的部分。

3.35

规程 procedure

1) 为解决问题或为完成给定的任务而采取的动作的过程；

2) 定义 1)中动作过程的书面描述，例如，文件化的试验程序；

3) 指定的并执行规定动作的计算机程序的一部分。

3.36

鉴定试验 qualification testing

为向用户证明软件物项或系统满足其规定的要求而进行的试验。

3.37

需求 requirement

1) 用户为解决某一问题或达到某个目标所要求的条件或能力；

2) 为满足合同、标准、规范或其他正式规定的文件、系统或系统部件应满足的和具备的条件或能力；

3) 在 1)和 2)中规定的条件或能力的文档化的陈述。

3.38

需求规格书 requirements specification

规定对系统或部件需求的文件。通常包括功能要求、性能要求、接口要求、设计要求和研制标准。

3.39

软件 software

与计算机系统运行有关的计算机程序、规程，以及相关的文档或数据。

3.40

软件维护 software maintenance

1) 为改正错误、提高性能或其他特性、或者为适应变化的环境，而对交付后的软件产品进行的修改；

2) 为确保已安装的软件能按照预期连续运行并实现在系统运行中预期的作用而进行的一系列活动。软件维护包括改进、用户帮助，以及相关的活动。

3.41

软件质量度量 software quality metric

其输入为软件数据，输出为单一数值的一种函数，该数值可以被认为是软件具有影响其质量的特性的程度。

3.42

软件工具 software tools

一种用来开发、测试、分析或维护其他程序或其文件的计算机程序。例如：比较程序、交叉引用生成程序、反编译程序、驱动程序、编辑程序、流程图程序、监控程序、测试案例生成程序和时序分析程序。

3.43

规格书 specification

以完整的、准确的和可验证的方式规定了系统的要求、设计、行为或其他属性的文件，以及用于确定是否满足这些规定的程序。

3.44

系统 system

构成完成特定的功能或功能组的设备集合。

3.45

系统软件 system software

为了便于计算机系统及其相关程序的运行和维护而设计的软件。例如操作系统、汇编程序和实用程序。

3.46

系统试验 system testing

为了评价一个完整的已集成的系统与其规定要求之间的一致性，对该系统进行的试验。

3.47

试验 test

1) 在规定的条件下操作一个系统或部件、观察或记录其结果，及对系统或部件的某些方面进行评价的过程；

2) 对软件物项进行分析以发现现有状态与要求条件之间的差异(即隐错)，并评价软件物项特性的过程。

3.48

试验大纲 test plan

1) 描述预期试验活动的范围、方法、资源和进度的文件，它规定了试验项目、试验特点、试验任务、每项任务的完成者，以及需要执行应急计划的风险；

2) 描述对一个系统或部件进行试验所遵循的技术和管理方法的文件。典型的内容应规定被试验物项、需要执行的试验任务、责任、进度，以及试验活动所需要的资源。

3.49

确认 validation

在研制过程中或完成时评价一个系统或部件以确定其是否满足规定要求的过程。

3.50

验证 verification

1) 为确定某一研制阶段的产品是否满足该阶段开始时规定的条件，而对一个系统或部件进行评价的过程；

2) 计算机程序正确性的正式证明。

3.51

验证与确认 verification and validation(V&V)

确定对一个系统或部件制定的要求是否完整和正确、每个研制阶段的产品是否满足前一个阶段提出的要求或条件，以及最终的系统或设备是否符合预定要求的过程。

4 安全系统设计基准

关于本标准与 GB/T 13284.1—2008 的关系参见附录 A。

见 GB/T 13284.1—2008 中第 4 章，参见附录 B。

5 安全系统准则

本章按 GB/T 13284.1—2008 第 5 章的顺序列出安全系统准则。对有些准则，除了 GB/T 13284.1—2008 的规定以外没有附加要求。而对另外一些准则，本章给出其附加要求。

5.1 单一故障准则

见 GB/T 13284.1—2008 中 5.1，参见附录 B。

5.2 保护动作的完成

见 GB/T 13284.1—2008 中 5.2。

5.3 质量

硬件质量要求见 GB/T 13284.1—2008 中 5.3。软件质量要求见 IEEE/EIA 12207.0 及其支持性标准。计算机的研制活动应包括计算机硬件和软件的研制。在研制过程中应考虑计算机硬件与软件的集成以及计算机与安全系统的集成。

典型的计算机系统研制过程由下述生存周期的过程组成：

a) 建立系统的概念设计，将概念设计转化为具体的系统需求；
b) 使用这些需求进行详细的系统设计；
c) 实现硬件和软件功能的设计；
d) 功能试验以保证需求的正确实现；
e) 系统安装并进行现场验收试验；
f) 系统运行和维护；
g) 系统退役。

为了符合质量准则，除了 GB/T 13284.1—2008 的要求之外，还应满足下述活动的附加要求：

a) 软件研制；
b) 现有商品级计算机的质量鉴定(见 5.4.2)；
c) 软件工具的使用；
d) 验证与确认；
e) 配置管理；
f) 风险管理。

5.3.1 软件研制

计算机软件应按经批准的软件质量保证大纲进行研制、修改或验收，这一质量保证大纲应与 IEEE/EIA 12207.0-1996 的要求相一致。软件质量保证大纲应考虑运行时计算机的所有常驻软件(即：应用软件、网络软件、接口程序、操作系统以及诊断程序)。编制软件质量保证大纲的指导见EJ/T 1058 和 EJ/T 694。

在整个软件寿期内，应考虑使用软件质量度量以评价其是否满足软件质量要求。当使用软件质量度量时，应考虑下述的生存周期阶段特性：

a) 正确性/完整性(需求阶段)；
b) 与需求的一致性(设计阶段)；
c) 与设计的一致性(实现阶段)；
d) 功能与需求的一致性(试验和集成阶段)；
e) 现场功能与需求的一致性(安装和调试阶段)；
f) 性能历史记录(运行和维护阶段)。

在软件研制文档中应包括为评价软件质量特性而选择度量的依据。IEEE Std 1061-1998 提供了软件质量度量的应用方法。

5.3.2 软件工具

为支持软件研制过程和 V&V 过程而使用的软件工具应纳入配置管理。

应采用下述一种或两种方法以确认软件工具适合于它的应用：

a) 应开发测试工具确认程序以证明软件工具具有所要求的特性；

b) 未能被软件工具发现到的缺陷应能通过 V&V 活动发现。

软件工具的运行经验可提供在工具适宜性方面的附加可信度，特别是当评价未探测缺陷的可能性时。

5.3.3 验证与确认(V&V)

V&V 是程序管理和系统工程组活动的延伸。在整个系统生存周期中，V&V 用于确定有关数字系统质量、性能和研制过程与整个生存周期一致性的目标数据和结论(即主动反馈)。反馈包括与系统及其接口的预期运行条件有关的不符合项报告、性能改进及质量提高。

V&V 过程用于确定某一活动的研制产品是否满足该活动的要求，以及系统是否按照其预期的用途和用户的需求在运行。这种适宜性的确定过程包括对产品和过程进行的评价、分析、审查、检查和测试。

本标准采用 IEEE Std 1012-1998 规定的过程、活动和任务的定义，其中软件 V&V 过程被分解为多项活动，活动又被进一步分解为多项任务。术语 V&V 工作通常用来指 V&V 过程、活动和任务的这种构架。

V&V 过程应专注于计算机硬件和软件、数字系统部件的集成以及计算机系统与核电厂的相互作用。

V&V 活动和任务还应包括对最终集成的硬件、软件、固件和接口的系统试验。

应依据 IEEE Std 1012-1998 进行软件 V&V 工作。IEEE Std 1012-1998 对最高完整性等级(第 4 级)的 V&V 要求适用于按照本标准研制的系统。

5.3.4 独立验证与确认要求(IV&V)

上节论述了应进行的 V&V 活动，本节规定了 V&V 工作所要求的独立性程度。IV&V 活动由三个方面组成，即技术独立性、管理独立性和财务独立性。在 IEEE Std 1012-1998 的附录 C 中对这三个方面进行了说明。

研制和测试应由具有适当技术能力的、没有参加原设计的人员或小组进行独立的验证与确认。

IV&V 工作的监督应由研制和程序管理组织之外的机构来进行。IV&V 工作应独立地选择：

a) 需要分析及测试的软件和系统部分；

b) V&V 的技术；

c) 需对之采取行动的技术问题和难点。

应为 IV&V 工作分配独立于研制活动的资源。

关于 IV&V 的附加信息见 IEEE Std 1012-1998 的附录 C。

5.3.5 软件配置管理

应按 IEEE Std 1042 的要求进行软件配置管理。编制软件配置管理计划的指导见 EJ/T 743。

至少应进行下述活动：

a) 所有软件设计和程序代码的标识和控制；

b) 所有软件设计功能数据(数据模板和数据库)的标识和控制；

c) 所有软件设计接口的标识和控制；

d) 所有软件设计变更的控制；

e) 软件文档(用户文件、运行和维护文件)的控制；

f) 对提供安全系统软件的软件供应商研制活动的控制；

g) 与软件设计和程序代码有关的鉴定信息的控制和获取；

h) 软件配置审查；

i) 状态统计。

其中某些功能或文件可由其他的质量保证活动来完成或进行控制。在这种情况下，软件配置管理大纲应说明责任的分工。

应在软件生存周期过程中适当的点建立软件基线，以使工程和文档活动相同步。基线建立后产生并经批准的变更应添加到基线中。

对实施配置管理的软件的标签应包括每个配置项的唯一性的标识，以及每个配置项的版本号和(或)日期时间标志。

应按照软件配置管理计划，对软件/固件的变更正式形成文件并得到批准。该文档应包括变更的原因、受影响的软件/固件的标识，以及变更对系统的影响。此外，文档还应包括变更在系统中实施的计划(立即实施变更，或未来版本变更的时间表)。

5.3.6 软件工程风险管理

软件工程风险管理是一种用于问题预防的工具，鉴别可能出现的问题、评价这些问题的影响，并确定为确保达到软件质量目标应考虑的潜在问题。在数字系统工程的各个层次应进行风险管理以充分覆盖每个可能的问题领域。软件工程风险可包括与技术、进度或资源有关的风险，这些风险可能损害软件的质量目标，从而影响安全系统计算机执行安全相关功能的能力。正如 3.31 的定义一样，软件工程风险管理与危害分析的不同之处在于在危害分析中仅关注系统失效机理中技术方面的因素。

风险管理应包括下述步骤：

a) 确定数字系统风险管理的范围；

b) 规定和实施适当的风险管理策略；

c) 在工程风险管理策略中鉴别软件项目的风险，以及它们在项目实施过程中的演变；

d) 分析风险以确定缓解风险的优先次序；

e) 对可能显著影响软件质量目标的风险编制风险缓解计划，并采用适当的度量来跟踪问题的解决过程(这些风险包括可能损害安全计算机系统执行安全相关功能能力的、与技术、进度或与资源有关的风险)；

f) 当未达到预期的质量时采取的纠正措施；

g) 为解决软件工程风险，建立一个在工作人员之间及团队间能够进行有效交流的工作环境。

IEEE/EIA 12207.0-1996 和 IEEE Std 1540 提供了有关风险管理的附加指南。

5.4 设备质量鉴定

除满足 GB/T 13284.1—2008 中 5.4 要求的设备质量鉴定准则外，对安全系统中使用的数字计算机的鉴定还应满足下述要求。

5.4.1 计算机系统鉴定试验

计算机系统鉴定试验应在计算机运行并使用其实际操作中所用的代表性软件和诊断程序时进行。对于计算机完成安全功能所必需的所有部分，或者其运行或故障可能对安全功能有损害的部分，都应在鉴定过程中进行试验。确切地说，这包括存储器、CPU、输入和输出、显示功能、诊断、相关部件、通信路径和接口的试验和监测。试验应证明已满足与安全功能有关的性能要求。

5.4.2 现有商品级计算机的质量鉴定

关于现有商品级计算机适用性确认的信息参见附录 C。

应通过使用本标准的准则评价硬件和软件的设计来实现质量鉴定过程。鉴定的接受应基于证据，证明数字系统或部件包括硬件、软件、固件和接口能执行其要求的功能。验收及其依据应形成文件并与鉴定文件一同保存。

在那些传统的鉴定过程不适用的情况下，为验证一个设备可用于安全应用的一种替代方法是商品

级物项的适用性确认。商品级物项适用性确认的目的是验证被确认的物项在质量上与按照 HAF 003 的设备是相当的。

对计算机的适用性确认应鉴别对计算机物理的、性能的及研制过程的要求，以便对拟用的数字系统或设备能够执行安全功能提供足够的可信度。适应性确认过程适用于完成安全功能所需的硬件、软件和固件。只要有可能，对软件和固件的适用性确认过程应包括对设计过程的评价。在某些情况下，不能将设计过程作为适用性确认过程的一部分来进行评价。例如，实施评价的机构可能得不到安全系统中使用的微处理器芯片设计过程的信息。在这种情况下，不可能进行评价以支持适用性确认。由于适用性确认过程涉及到生存周期过程的所有方面及制造质量，因此商品级物项的适用性确认应限于与其预期使用有关的在功能上相对简单的物项。

商品级物项的适用性确认包括初步阶段和详细阶段的活动，这些阶段的活动在下面描述。

5.4.2.1 商品级物项适用性确认过程的初步阶段

在初步阶段，应评估风险和危害、确定安全功能、建立配置管理和确定系统的安全类别。

5.4.2.1.1 评估系统安全功能的风险和危害

应进行分析以确定安全系统的功能和性能要求，该分析应鉴别妨碍完成安全功能的风险和危害。

5.4.2.1.2 商品级物项应执行的安全功能

一旦确定了系统级功能和评估了风险和危害，适用性确认机构应确定由商品级物项执行的安全功能。这一过程应考虑由商品级物项执行的所有安全功能，以及商品级物项功能对其他安全相关功能或接口的可能影响。

5.4.2.1.3 建立配置管理控制

在安全系统中使用的商品级物项应受配置管理过程所控制，该管理过程提供了商品级物项研制生存周期过程的可追踪性。

5.4.2.2 商品级物项适用性确认过程的详细阶段

在商品级物项适用性确认的初步阶段后，应使用详细的验收准则对商品级物项的可接受性进行评价。应通过技术评价确定将对安全系统中使用的商品级物项进行评估用的关键特性，每个关键特性都应是可检验的(例如，通过检查、分析、演示或试验)。本标准使用商品级物项的下述三类关键特性：

a) 物理特性：包括几何尺寸、电源要求、部件号、硬件和软件的型号及版本号，以及数据通信要求等；

b) 性能特性：包括响应时间、人机功能要求、存储器分配、在异常工况下安全功能的执行、可靠性、差错处理、要求的嵌入功能、以及环境鉴定要求(例如地震、温度、湿度和电磁兼容性)等；

c) 研制过程特性：包括支持生存周期过程的那些特性(例如验证与确认活动、配置管理过程和危害分析)，以及可追踪性和可维护性。

作为确定这些关键特性工作的一部分，应通过分析鉴别可能影响安全功能的危害。参见附录 D。

用于单独评价或组合评价物理的、性能的和研制过程的关键特性的过程参见附录 C。

5.4.2.3 商品级适用性确认的保持

如果计算机硬件、软件或固件已按商品级物项采购，并已通过商品级物项适用性确认过程予以接受，则应通过正式的文件对已经适用性确认的计算机硬件、软件或固件的变更进行追踪。

应按照形成原始接受依据的过程，对已确认的商品级计算机硬件、软件或固件的变更进行评价。在评价过程中应考虑计算机硬件修改可能对软件或固件造成的潜在影响。如果在计算机硬件、软件或固件的修改过程中省略了审批过程的某些步骤，则需要进行进一步的评价。

针对特定的安全系统应用，进行计算机硬件、软件或固件的商品级物项适用性确认。当已经过适用性确认的商品级物项在安全系统中的应用超出了初始适用性确认所包括的范围时，应针对新的应用进行附加的评价。

支持商品级物项适用性确认过程的文件应作为配置项保存。

5.5 系统的完整性

为了达到安全系统中数字设备应用的系统完整性，除了 GB/T 13284.1—2008 中 5.5 的要求之外，还应满足下述要求：

a) 计算机完整性设计；

b) 试验和校准设计；

c) 故障探测和自诊断。

5.5.1 计算机完整性设计

计算机应设计成在所有可能造成安全功能失效的内部或外部条件下完成其安全功能，这些条件如输入和输出处理故障、精度或舍入问题、不适当的恢复动作、电源电压或频率波动，以及信号同时改变的最大可信数量。

如果系统要求已规定安全系统的优选故障模式，则计算机故障不得阻碍安全系统处于该故障模式。计算机完成重启操作不应阻止安全系统完成其功能。

5.5.2 试验和校准设计

试验和校准功能不得对计算机完成其安全功能的能力产生有害的影响。适当地旁通一个冗余通道并不认为是一种有害影响。应验证，试验和校准功能并不影响与校准变更（例如变更整定值）无关的其他计算机功能。

当试验和校准功能由另外的计算机（例如，试验和校准计算机）完成并由该计算机提供试验和校准数据的唯一验证时，则应对这些功能要求进行 V&V、配置管理和质量保证。当试验和校准功能由安全系统中的计算机来完成时，也应对这些功能要求进行 V&V、配置管理和质量保证。

当驻留在另外计算机中的试验和校准功能不是为安全系统的计算机提供试验和校准数据的唯一验证时，则不要求对这些功能进行 V&V、配置管理和质量保证。

5.5.3 故障探测和自诊断

计算机系统能够经受使计算机系统能力降低、但可能不被系统立即探测出来的局部故障，自诊断是一种有助于探测这些故障的手段。在本节中说明对故障探测和自诊断功能的要求。

应使用安全系统的可靠性要求来建立自诊断的需求。在其故障可由其他方法及时探测出来的系统中不要求自诊断功能。如果在系统需求中包含自诊断要求，则这些功能应经历与安全系统功能相同的验证与确认过程。

如果自诊断作为可靠性的必要条件，则计算机程序应包含及时探测和报告计算机系统故障和失效的功能。而自诊断功能不能影响计算机系统执行其安全功能的能力，或引起安全功能的误动作。典型的自诊断功能包括：

a) 存储器功能性和完整性试验（例如 PROM 检查和 RAM 测试）；

b) 计算机系统指令集（例如计算测试）；

c) 计算机外部设备硬件试验（例如监视定时器和键盘）；

d) 计算机结构支持硬件（例如地址线和共享存储器接口）；

e) 通讯链路诊断（例如循环冗余校验）。

不会导致系统故障或系统功能缺失的罕见通讯链路故障不需要报告。

当应用自诊断功能时，系统设计应包括下述自诊断特性：

a) 计算机系统启动期间的自诊断；

b) 当计算机系统运行时定期的自诊断；

c) 自诊断测试故障报告。

5.6 独立性

为了满足独立性准则，除了 GB/T 13284.1—2008 中 5.6 的要求之外，安全通道之间或安全系统与非安全系统之间的数据通信不得阻碍安全功能的执行。

GB/T 13284.1—2008 要求安全功能应与非安全功能相隔离，以使非安全功能不会阻止安全系统执行其预期的功能。在数字系统中，安全功能和非安全功能软件可能驻留在相同的计算机中并使用相同的计算机资源。

下面任何一种都是处理这一问题可接受的方法：

a) 确定屏障要求，以便充分确信软件或固件的非安全功能部分不会妨碍其安全功能部分的执行，这些屏障应按本标准要求进行设计，不要求非安全软件满足这些要求；

b) 如果安全软件和非安全软件之间不设置屏障，则非安全软件的功能应按照本标准的要求进行研制。

关于通信独立性准则的信息参见附录 E。

5.7 试验和校准能力

见 GB/T 13284.1—2008 的 5.7。

5.8 信息显示

见 GB/T 13284.1—2008 的 5.8。

5.9 接近控制

见 GB/T 13284.1—2008 的 5.9。

5.10 维护

见 GB/T 13284.1—2008 的 5.10。

5.11 标识

为确保所要求的计算机硬件和软件按照适当的系统配置进行安装，应满足下述对软件系统的标识要求：

a) 应使用固件和软件标识以确保在正确的硬件部件上安装了正确的软件；

b) 在软件中应包含相关的手段，以便使用软件维护工具可从固件中重新得到标识；

c) 数字计算机硬件的实体标识要求应符合 GB/T 13284.1—2008 的标识要求。

5.12 辅助设施

见 GB/T 13284.1—2008 的 5.12。

5.13 多机组核电厂

见 GB/T 13284.1—2008 的 5.13。

5.14 人因工程考虑

见 GB/T 13284.1—2008 的 5.14。

5.15 可靠性

除 GB/T 13284.1—2008 的 5.15 的要求以外，当规定了可靠性目标时，应证明软件也满足该目标要求。确定可靠性的方法可以包括分析与现场经验或试验的组合。软件差错记录及其趋势分析可以同分析、现场经验或试验结合使用。

6 监测指令设备的功能和设计要求

见 GB/T 13284.1—2008 第 6 章。

7 执行装置的功能和设计要求

见 GB/T 13284.1—2008 第 7 章。

8 对动力源的要求

见 GB/T 13284.1—2008 第 8 章。

附 录 A
（资料性附录）
本标准与 GB/T 13284.1—2008 的相互关系

本标准的第 4 章～第 8 章与 GB/T 13284.1—2008 的第 4 章～第 8 章相对应。

表 A.1 GB/T 13284.1—2008 与本标准的关系

GB/T 13284.1—2008 准则（按标准中出现顺序）	本标准补充的要求	资料性附录
4 安全系统设计基准	安全系统设计基准	B
5 安全系统准则	无	
5.1 单一故障准则	无	B
5.2 保护动作的完成	无	
5.3 质量	软件研制（见 5.3.1）	D 和 F
	软件工具（见 5.3.2）	
	验证与确认（见 5.3.3）	
	独立验证与确认要求（见 5.3.4）	
	软件配置管理（见 5.3.5）	
	软件工程风险管理（见 5.3.6）	
5.4 设备质量鉴定	对软件和诊断程序进行试验（见 5.4.1）	C
	现有商品级计算机的质量鉴定（见 5.4.2）	
5.5 系统的完整性	计算机完整性设计（见 5.5.1）	B 和 C
	试验和校准设计（见 5.5.2）	
	故障探测和自诊断（见 5.5.3）	
5.6 独立性	独立性（见 5.6）	E
5.7 试验和校准能力	无	
5.8 信息显示	无	
5.9 接近控制	无	
5.10 维护	无	
5.11 标识	标识（见 5.11）	
5.12 辅助设施	无	
5.13 多机组核电厂	无	
5.14 人因工程考虑	无	
5.15 可靠性	可靠性（见 5.15）	F
6 监测指令设备的功能和设计要求	无	
7 执行装置的功能和设计要求	无	
8 对动力源的要求	无	

附 录 B
（资料性附录）
多样性需求的确定

B.1 背景

将计算机用作安全系统的组成部分时，对于计算机软件会导致共模故障的可能性已经引起了人们的关注。多样性是处理这一问题的一种方法。本附录提供了确定多样性需求的一种方法。

B.2 讨论

可能存在某些情况，在这些情况下除了由设计和质量保证(QA)大纲(包括软件 QA 和 V&V)所提供的保证以外，还可能需要某种形式的多样性来提供附加保证。在计算机设计复杂(例如，一项安全功能的所有控制在一台计算机上实现)和运行经验有限的情况下，下面提供了一种方法，用来确定依赖于功能多样性和纵深防御的核电厂其他设计特性的充分性。

如果已有适当的多样性或者可将适当的多样性增加到核电厂设计中，则不需要计算机的多样性。对于在设计中可用经验有限且无多样性的复杂系统，应使用计算机的多样性。

B.3 确定多样性需求的方法

根据核电厂设计基准事件的分析，确定由拟用计算机完成的安全功能，并鉴别出其他安全和非安全的设计措施，这些设计措施能执行相同的或不同的安全功能，对已确定的“不可接受结果”提供等效的保护(例如，对于未能紧急停堆预期瞬态的缓解系统可为反应堆保护系统完成紧急停堆功能提供功能多样性)。如果有必需的控制器和显示器支持操纵员在可接受的时间内完成适当的操作，则操纵员的手动操作是可以接受的。如果使用的设备不受拟用计算机假想软件差错的影响从而具有功能多样性，则在拟用系统的冗余通道中使用相同的软件是可以接受的。

如果不存在功能多样性，则应进行纵深防御分析，以便确定在防御的各层次中(即反应堆保护、专设安全设施以及控制与监测系统)是否存在多样性。这一分析鉴别出每一层次中能阻止被分析工况的出现或减轻其后果的设计措施，并确定在每一层次中的假想故障(例如软件差错)是否可能对其他层次产生有害影响。如果能在要求的时间内完成其功能，则可以相信手动操作以及非安全级控制和监测设备。

如果分析表明对不可接受结果存在纵深防御，而且防御的各个层次不受假想软件故障的影响，则在拟用系统的冗余通道中使用相同的软件是可以接受的。

如果分析不能确认存在功能多样性或纵深防御，则应采用多样性设计。这可以用计算机与非计算机通道的结合或者用多样化的计算机来实现。计算机的多样性可通过使用不同的计算机功能规格书、计算机硬件、计算机语言等来实现，以便尽量降低共因故障的概率。

附 录 C
（资料性附录）
现有商品级计算机的适用性确认

C.1 背景

在有些情况下，安全系统设计全部或部分采用了未按本标准的准则研制的计算机（硬件、软件、固件和接口）。5.4.2 提供了商品级物项适用性确认的通用指南，本附录的目的是帮助处理这些情况，以便允许在安全系统设计中使用不是专为核电厂设计的计算机。本附录也论述了对已鉴定的现有商品级计算机适用性确认的保持问题。在本标准中，商品级物项适用性确认过程涉及到商品级物项的初次鉴定以及鉴定的保持。

本附录概述了应遵守的主要步骤，以便确信现有商品级计算机具有高的质量和可靠性，从而允许它们在安全系统中使用，见 5.4.2。当制造商未按 HAF 003 完成部件研制活动时，进行商品级物项适用性确认过程的各项活动可能是适当的。

C.2 讨论

第三方或制造商的安全设备质量鉴定所产生的文件可能达不到按本标准设计和研制所产生的设计文件的深度。然而，现有的商品级计算机可能具有运行经验证据的文件资料。只应相信与核电厂中计算机应用方式相类似的情况下所取得的运行经验。运行经验是对设计过程文件以及验证与确认活动的补充。

相对第三方确认者来说，现有商品级计算机的制造商可能容易取得许多有用的设计资料。例如：关于计算机软件程序信息的可利用性、设计和审查过程（即 V&V）的详细情况、运行经验文件，以及计算机硬件设计和软件设计的维护（即配置管理）。

商品级物项适用性确认的目的是用合理的保证来确定被确认的物项满足为完成安全功能所必需的要求，这包括：

a） 确定计算机应完成的安全功能；

b） 确定计算机为完成这些安全功能所应具备的特性；

c） 证明这些特性满意地得到实现。

C.2.1 确定计算机应完成的安全功能

应进行分析，以便确定为实现安全功能而对计算机的功能和性能要求。这一分析还应确定可能会妨碍计算机完成安全功能的危害，参见附录 D。

C.2.2 确定计算机的特性

应将 C.2.1 确定的计算机功能和性能要求及危害分配给硬件和软件。对软件应确定 5.4.2 要求的研制步骤。

C.2.2.1 硬件

应确定给 5.4.2 要求的硬件部分分配的功能和性能要求及危害。在功能和性能要求及危害方面所确定的计算机硬件特性的一些实例是：历史数据存贮、系统响应时间、抗震鉴定（包括温度、湿度、辐射、电磁干扰在内的环境鉴定）、人机接口以及维修工具。

应进行评价以表明功能和性能要求及危害与验收准则相一致。这可能需要进行特定的试验（例如地震试验和电磁兼容性试验）、进行某些验证与确认活动、评价供货商的规格书，或者信赖在与核电厂计算机的使用相类似的方式下取得的有文件证明的运行经验。

C.2.2.2 软件

应确定给 5.4.2 要求的软件部分分配的功能和性能要求及危害。应确定的计算机软件特性的一些实例是：系统响应时间、在异常情况期间实现已确定的安全功能、要求的嵌入功能、正确实现逻辑和算法、操作系统功能、通信(内部和外部)、存贮器保护、整定值变更的控制、差错处理、同步、中断控制，以及调整常数的控制。

应进行评价以表明功能和性能要求与验收准则相一致。这可能需要进行特定的试验、进行某些验证与确认活动或者评价供货商的规格书，并结合与核电厂计算机的应用相类似的方式下取得的有文件证明的运行经验。

C.2.2.3 研制步骤

应确定 5.4.2 要求的软件研制步骤，研制过程步骤的一些实例是：系统要求和验收准则的确定和文件编制、软件需求的确定、软件设计的文件编制、硬件和软件的 V&V、硬件和软件的集成试验、硬件和软件的配置管理、程序员手册和用户手册，以及差错鉴别、文件编制、通知和改正的过程。

研制过程的验收应基于对计算机的研制、文件编制和验证与确认活动已采用的文件化过程的证据。应完成全部验证与确认活动。对某些研制步骤的文件或实现方面存在的不足之处可通过下列方式之一进行弥补：

a) 在与核电厂中计算机应用相类似的方式下所取得的有文件证明的运行经验；

b) 对已开展的应用项目得到的 V&V 结果，以支持操作系统或嵌入功能的验收。

应鉴别出任何要求的、但此前没有完成的 V&V 活动。

C.2.3 证明特性满意地得以实现

应提供文件证明计算机的特性满意地得以实现，表明设备和系统符合功能和性能要求以及本标准的要求。计算机设备的商品级适用性确认包括：专门的试验和检查、供应商的商品级检查、源验证、合格供应商/物项的性能记录，或者是以上各项的结合。

C.2.3.1 专门的试验和检查

如果技术数据是可得到的、试验设施是可利用的，则应进行专门的试验和检查，并使商品级物项通过验收时的检查和试验可充分验证其关键特性。专门的试验和检查也可与其他可接受的验收方法结合使用。

专门的试验和检查最适用于：

a) 从多个供应商采购的物项；

b) 在性质上相对简单的物项；

c) 可进行安装后试验以验证其关键特性的物项。

关键特性数据通常是在规格书、图纸、说明手册、材料清单以及产品样本中得到的。为了得到要求的数据可能需要与供应商接触。由于专利权方面的原因，当不能从供应商得到充分的数据以进行专门的试验和检查时，应考虑采用其他的验收方法。

专门的试验和检查应在标准验收检查的基础上进行，或与其相结合进行。当确定进行专门的试验和检查时，应编制文件化的大纲或检查表，以验证所选择的关键特性。专门试验和检查的结果应记录在已批准的大纲或检查表中，应包括：

a) 在专门试验和检查范围内包括的商品级物项；

b) 进行的试验和检查项目；

c) 采用的试验方法和检查技术(需要时，可能要求编制好的试验和检查程序)；

d) 规格书、图纸、手册、材料清单、产品样本等；

e) 说明待验证特性的验收准则；

f) 检查和试验结果的文档要求。

C.2.3.2 供应商的商品级检查

供应商的商品级检查是一种手段，通过它采购者可以相信由商品级物项的制造商或供应商所采取的商品级物项控制。当采购者想根据供应商的质量控制准则来验收商品级物项时，应使用供应商的商品级检查。供应商的质量控制是指质保大纲、质保程序或实施规程。

商品级检查最适合于：

a) 未按照 HAF 003 鉴定的设备；

b) 初始设备的制造商/供应商(OEM/OES)；

c) 重新制造设备的供应商；

d) 销售商。

供应商的商品级检查可用于验收简单的或复杂的物项。供应商的商品级检查最适用于下列情况：

a) 商品级物项只有单一的供应商；

b) 不能从供应商处得到所要求的技术数据；

c) 从整个设备系列的一个供应商处重复采购很多种物项；

d) 商品级物项包含许多部件的组合；

e) 采购者不能轻易地通过专门的检查和试验来验证物项的关键性能。

对不同的物项，检查准则和供应商控制可能是不同的。采购者应依据关键特性的数量和类型来确定检查准则和必要的供应商控制。检查应针对被采购的商品级物项的范围。当从一个供应商采购多个物项时，对有代表性的几种商品级物项的检查就足以表明存在适当的控制措施。对于每一个物项，应确认执行适当的质量控制并形成文件。

应对供应商的设计控制、采购、软件生存周期过程、材料控制、制造、组装、校准、试验、监督、问题报告和纠正行动计划进行检查，以确保关键的特性得到控制。当与被验证的关键特性有关时可能还需要其他的控制措施。

商品级检查的结果应记录在已批准的检查大纲/检查表中，应包括：

a) 在检查范围内包括的商品级物项；

b) 由供应商控制的关键特性；

c) 纠正行动和通告；

d) 验证供应商对关键特性的控制；

e) 检查方法或验证活动；

f) 证明供应商控制充分性的结论。

供应商可以通过制定附加的控制措施或使用本标准中的其他可接受的方法来纠正在商品级物项供应商检查中发现的缺陷。

在供应商证明有充分的控制措施且关键的特性已得到验证的情况下，则在对完整的商品级物项验收的标准验收检查过程中，仅要求验证部件号、模块号、型号、版本和修订版本号(当适用时)，以及供应商的符合性证明。

采购者应基于诸如供应商的行为、物项的复杂程度、标准验收检查结果和采购的频度来评估重新确认检查的频度。

C.2.3.3 源验证

源验证是在商品级物项装运前通过见证质量活动进行的关键特性的验证。源验证的基本目的是确认供应商有效控制了所选择的商品级物项的关键特性。源验证最适用于单一的商品级物项或物项的发运，或者极少采购的或快速采购的物项。

当源验证中确认供应商适当地控制了关键特性时，应在验收时检验部件号、型号、系列号、版本号及修订版本号(适用时)，应依据标准验收检查的完成以及源验证结果文件对物项进行验收。

对不同的物项，采购者需见证的控制可能是不同的，并应依据关键特性的数量和类型来确定。监督

的范围应包括见证研制过程、参与软件生存周期过程审查及其活动，或者见证工厂验收试验。应包括确认供应商的设计、采购，及为采购某些特殊的商品级物项而采用的控制方法。

源验证的结果应记录在已批准的监督大纲/检查表中，应包括：

a) 监督范围内包括的商品级物项；

b) 由供应商控制的关键特性；

c) 验证供应商对关键特性的控制；

d) 监督方法和验证活动；

e) 供应商控制充分性评价。

供应商可通过制定附加的控制措施来纠正在源验证期间鉴别的缺陷，或使用本标准中其他可接受的方法以验证其适宜性。

商品级物项适用性确认文件应提供关键特性的控制得到遵守的客观证据。

C.2.3.4 合格供应商/物项的性能记录

使用合格供应商/物项的性能记录，可使采购者根据由物项的性能及其他的商品级物项适用性确认过程对商品级物项所建立的信任，接受商品级物项。

供应商试验的结果可用于验证某些关键的特性，也可考虑能支持物项性能历史的信息，诸如从运行核电厂、供应商或工业用户获得的可靠性数据。在使用下述手段可搜集历史性能结果的情况下，合格供应商/物项的性能记录最适合于商品级物项：

a) 监测的性能；

b) 供应商产品性能数据；

c) 工业产品测试和性能数据；

d) 核电厂中部件故障概述；

e) 其他工业数据库(例如军工或航天工程)；

f) 由核安全当局签发的文件(例如信息通告)。

历史性能记录应与专门的试验和检查、供应商检查和源验证结合使用。性能数据应直接适用于关键特性。

应主要通过对从某一供应商处采购物项的性能监测，并通过安装有该物项的母体设备的性能监测来确定历史性能。这些性能数据通常可通过维护记录来得到。由于并不是所有的设备故障都向供应商报告，或者故障可能发生在分析完成以后，因此鉴定者应谨慎使用这一方法。应定期更新支持性文件并对之进行审查，以确保供应商/物项保持合格的性能记录。

对历史性能数据的评价应整理成文件。该文件应包括下述内容：

a) 被评价的供应商/物项；

b) 对物项或供应商已确定的关键特性；

c) 在评价供应商/物项时使用的用户/工业数据的证明；

d) 工业数据证明物项/供应商可接受性的确定依据；

e) 供应商/物项可接受性的理由概述。

验收基于工程判断，确定具有充分的证据可确信现有商品级计算机的可用性。全部验收活动应按计划进行并形成文件。此外，对于验收准则的例外情况，应当用文件说明理由。

附 录 D
（资料性附录）
危害的鉴别和解决

D.1 背景

计算机研制需要鉴别出可能使安全功能失效的危害(即异常状态和事件,或 ACE)。危害是事故的一种先决条件。危害包括外部事件以及计算机硬件和软件的内部状态。本附录对危害的鉴别、评价和解决提供指导。本附录简略讨论了故障树分析(FTA)及故障模式和后果分析(FMEA)的使用,并以设计过程中可用的考虑方式介绍了 IEEE Std 1228 和 MIL-Std 882B 中所述概念的适用性。这些标准的概念包括各种设计分析和检查表。此外,一旦鉴别出危害,本附录对危害的解决提供指导。应把鉴别出的危害作为适当的 V&V 活动(见 5.3.3)以及可靠性计算(见附录 F)的输入。

分析技术是用来确定危害的一种方法,例如 FTA 和 FMEA。GB/T 13284.1—2008(5.15,并参考 GB/T 9225)建议用 FMEA 进行可靠性分析。这些技术可以用来鉴别可能的危害。IEEE Std 1228 和 MIL-Std 882B 给出了用来鉴别危害的另外一种技术,该技术试图鉴别设计过程中引入的危害。

D.2 讨论

危害是从系统角度(例如:设计基准工况、系统设备的故障模式、人因错误等)考虑得出的结果,或由特定的设计和实施的相互影响(例如:子系统接口的不相容性、缓冲存储器溢出、输入/输出不适时、初始状态不符、乱序的事件等)所产生的结果。通过设计和 V&V 活动应足以确信对鉴别出的危害已作了适当处理。

5.5.1 要求考虑那些很可能对完成安全功能所必需的计算机硬件和软件产生有害影响的危害。危害的重要性基于发生概率和后果,只有产生的后果可能会使要求的安全功能失效的那些事件才应予以考虑。对发生概率的定量或定性判断应足以能确定是否需要采取进一步的行动,只有那些具有明显后果而且发生概率较高的状态才需要在设计过程中予以解决。应将考虑的状态以及确定重要性的依据形成文件。本附录并不意味要取代 GB/T 13284.1—2008 的要求。

D.3 危害分析的目的

危害分析的目的是探索并确定由正常设计审查和试验过程未鉴别出的那些工况。正常的设计验证与确认过程保证安全系统满足设计要求,通常这一过程应评价由核电厂设计基准要求的不同故障组合以及故障对系统的影响。通过包括异常事件及带有劣化的设备和系统的核电厂运行,使得危害分析的范围超出核电厂设计基准事件的范围。危害分析着重于系统的故障机理而不是验证系统的正确运行。基于发生的概率和后果,首先鉴别可导致危害的重要故障模式,然后对其进行评价以确定相关的风险水平(例如高/不可接受风险,或低/可接受风险)。对划分为具有不可接受风险的故障模式,可进一步进行评价以确定特定故障模式的起因。可定量或定性地确定危害发生的概率,大部分的危害分析应是定性的,而定量分析可用于确定优先次序。

D.4 危害分析实施指导

在进行危害分析时应考虑下述指导:

a) 危害的避免;

b) 危害的鉴别和评价;

c) 整个系统寿期内危害的鉴别;

d) 危害的解决；

e) 已研制系统中危害的评价；

f) 危害分析大纲、责任和结果的文件编制。

D.4.1 危害的避免

在设计过程中通常使用下述良好的工程实践以减少在系统设计阶段危害的数量：

a) 使用工业标准作为指导以避免危害，工业界专家已编制了一些标准，这些标准规定了避免某些已发现危害的方法；

b) 使用检查表，使用技术检查表是另外一种避免危害的方法，技术检查表是已知危害或如何避免危害方法的列表，检查表通常是根据过去的危害经验来编制的，由于检查表可能没有包括所有的危害，因此检查表应作为危害分析的一种补充方法；

c) 在不同的开发领域，诸如在软件研制、系统维护、设计工程和运行方面，使用专家系统；

d) 需求分析的使用有助于系统危害的早期鉴别。

D.4.2 在详细设计阶段危害的鉴别和评价

在详细设计阶段，系统危害分析过程应结构化以保持对系统研制过程的影响最小(例如没有组织上的变化，过程变化最小)。此外，该过程应既适用于任一生存周期，也适用于设计后分析。该过程应开始于核电厂升级过程计划编制的初期，该计划描述预期的、工程特定的危害分析活动。在 D.4.3 中描述了生存周期危害分析过程。

D.4.2.1 结构

为了简化危害鉴别过程，应使危害鉴别作为正常设计过程的一个组成部分。在系统研制早期阶段把危害鉴别作为正常设计过程的一部分，与此相对应，在系统研制成功以后则把危害鉴别作为改进过程的组成部分，从而使危害鉴别成为生存周期的组成部分。在系统生存周期早期发现的危害易于纠正，且支出少于后面反馈分析中发现的危害。危害鉴别应使用正常设计过程中所用的系统开发和维护要素，这些要素如下：

a) 工程项目结构和组织；

b) 设计验证；

c) 审查会议；

d) 文件；

e) 配置管理；

f) 试验(工厂验收试验、模拟试验和修改后试验)；

g) 质量保证。

生存周期危害分析应考虑在系统研制、试验和实施过程中发生的变更。

D.4.2.2 计划

在系统研制开始时对危害分析可能存在的最大阻力是要求保持尽可能低的研制费用。在设计过程开始时不存在现实的和可鉴别的危害，因此对危害分析过程的判断和资源分配可能难于定量化或难于论证。认为新的数字系统等于或优于被替换系统的这种观点可能并不总是正确的。

在设计工程开始时，应编制危害鉴别和评价大纲，包括下述步骤：

a) 鉴别诸如反应堆紧急停堆、应急冷却剂注入等关键功能；

b) 鉴别不希望发生的顶级事件(可以导致关键功能丧失的事件)；

c) 确定组织机构的责任；

d) 选择使用的技术；

e) 确定分析假设；

f) 进行危害鉴别分析；

g) 针对后果和发生概率对已鉴别出的危害进行评价；

h) 采取所需的纠正行动并重新评价与关键功能相关的变更的影响。

D.4.2.3 危害鉴别

危害鉴别过程的第一步是确定系统的关键功能。应采用多学科组的方法来确定在系统研制过程整个范围内(例如硬件软件研制、运行、设计、维护和试验)的关键功能。一旦确定了关键功能,就能进行分析以鉴别在发生需求时妨碍这些关键功能的事件。危害鉴别不应当仅依赖于单一技术,而应在分析过程中使用多种不同的技术。下述技术可用于潜在危害的鉴别:

a) 初步危害分析(PHA);

b) 故障树分析及故障模式和后果分析;

c) 系统建模;

d) 软件需求危害分析;

e) 初审(例如设计审查和代码审查);

f) 模拟机/核电厂模型试验。

D.4.2.3.1 初步危害分析

初步危害分析(PHA)是一种初始的鉴别技术,它与专家对系统各个部分的自由讨论会议相似。在危害鉴别大纲过程中确定的系统关键功能和不希望功能的清单提供了 PHA 分析的起点和范围。问题清单或检查表也可用以指导和集中 PHA 的讨论。一个成功 PHA 的关键是选择参与者,参与者应具有各种不同的背景和系统的观察能力。PHA 小组成员应包括系统工程师、设计工程师、操纵员、来自适当专业的维护人员、软件和系统研制人员,以及概率风险评价分析员。

在 PHA 过程中制定的关键功能清单通常集中在安全重要的领域。然后确定这些关键功能可能的故障模式、区分安全重要性,并评估发生的概率。

D.4.2.3.2 故障树分析及故障模式和后果分析

故障树分析(FTA)及故障模式和后果分析(FMEA)是可用于确定危害的技术。这些技术论述了在设计过程中危害的引入。FTA 和 FMEA 是一种结构化的研究方法,它使用 PHA 期间鉴别的顶级故障。FTA 是一种从上到下的方法,它集中在对危害起因特定领域进行分析。FMEA 是一种从下到上的方法,它涉及到更广泛的领域并能针对已鉴别的危害进行评价以确定可能的起因。尽管 FMEA 不考虑应进行评价的多重故障(例如共因故障),但供应商可能更乐于进行 FMEA。所有的这些技术对于潜在危害的鉴别都是有用的。

鉴别危害的一种技术是列举出故障和不希望的后果,然后确定产生每个故障和后果的具体系统的设计或实现。例如,一个不希望的后果可能是在规定条件下没有开启一个阀门。这一后果可作为 FTA 中的顶事件,随后可以被分解为较低层次的中间事件,并在设计的最底层结束,对此可进行定性或定量的概率评价。在这个例子中,较低层次的故障可能是硬件故障、操作系统故障、传感器故障、驱动器故障或应用软件中表决逻辑错误。如果高层次的分析确定了软件错误是不希望后果的可能起因,则 FTA 可扩展到程序代码模块以及软件设计的下层(如果需要)。这种方法用作为一种工具以鉴别设计中最薄弱的部分,而且,如果发生了设计错误或随机故障,这一最薄弱部分可能就是不希望后果的重要起因。

D.4.2.3.3 系统建模

系统建模技术通过建立和随后执行系统设计的软件模型来鉴别系统设计中的危害。通过这种建模方法,可引入异常状态以确定这些状态对系统性能的影响。

D.4.2.3.4 软件需求危害分析

除了重点关注软件需求及软件与其他部件的接口外,该活动与 PHA 相似。此外,软件需求危害分析检查表可用于鉴别软件需求文件中遗漏的和不一致的内容。在软件需求危害风险分析完成后,所有可能的危害应按照它们对关键功能的可能影响进行排序。如果一个高级别的危害直接影响软件,则应对之作进一步的规定和评价。

D.4.2.3.5 初审

需求、设计和程序代码的初审是软件研制过程的一部分。初审集中在对系统特定部分的彻底检查，并应包含代表不同工程领域的人员。初审重点关注的是正确性(例如保证设计正确考虑了分配给它的要求)。关注点应扩展到对相关危害的处理(例如保证设计不使系统以不希望的或未预期的方式运行)。

D.4.2.3.6 模拟机/核电厂模型试验

通过将数字系统与核电厂模拟机或核电厂计算机模型相连接，可对案例进行试验。在试验期间，不仅能验证设计要求，还能针对正确性和系统响应进一步发现潜在的危害并对之进行试验。

D.4.2.4 危害评价

危害评价活动的重点在于评定潜在危害的可信性。在生存周期中应尽早评价所有可能的危害，以使早期危害鉴别的利益最大化。建议采用下列步骤进行危害评价：

a) 评价危害成本效益比；
b) 确定危害的可能后果；
c) 确定危害的种类和类型；
d) 鉴别和评价危害对系统级的影响；
e) 确定危害的处理。

D.4.2.4.1 评价危害成本效益比

分析者应确定与评价危害是否对系统带来显著的风险相比，是否可以更有效地消除潜在的危害。

D.4.2.4.2 确定危害的可能后果

确定危害的可能后果有两个部分。一旦鉴别了可能的危害，分析者应确定系统是否能产生这种危害。然后，分析者应评价作为危害的后果发生差错和故障的可能性。FTA 的结果可用于确定每个危害的相对重要性。这可以通过评定最小概率风险分析割集的概率以及割集的大小来完成(见 GB/T 9225)。如果对于不希望后果的发生来讲，故障或差错的概率低的可以接受，则不需要采取进一步的措施。反之，则可能需要设计变更或需要进行整个系统的安全评价。

其次，分析者应(定性或定量地)确定在运行工况下潜在危害发生的概率，这可能需要硬件设备的可靠性数据。对于软件，这可能包含对软件经受可能引起危害发生的某些条件或输入的概率评估。

D.4.2.4.3 确定危害的种类和类型

危害分析者应确定危害是由下述何种原因引起的：

a) 只是硬件；
b) 只是软件；
c) 硬件和软件(即系统级问题)；
d) 系统研制环境(例如导致不正确危害鉴别的、不完善的故障诊断设备)。

为了确定根本原因，分析者还应确定将危害引入到系统的研制阶段。例如在硬件实现阶段鉴别的危害可追溯到硬件设计中的某个问题，该问题可追溯到硬件需求规格书。在这个例子中，危害的类型是需求危害。危害的其他类型包括设计、实现、试验、安装、维护和运行危害。这些信息可用于确定适合于解决危害的人员。可对危害类型的记录进行比较，以鉴别研制过程中存在的缺陷。

D.4.2.4.4 确定和评价危害对系统级的影响

某一危害对系统层次的影响可能是不十分明显的，例如不正确值的指示可能导致操纵员采取不恰当的操作。相反，某一危害的影响可能是更加显而易见的，例如在不适当的时刻造成系统失效。较高级别的逻辑或联锁可防止可能的危害产生不希望的后果。采用常用的全面分析或作为 FMEA 的一部分能够确定对系统级的影响。功能性的 FTA 可能也是有用的。应根据系统级影响的比较和评价对可能的危害进行排序。例如，对任何单一的计算机引起不希望后果的硬件模件的单一随机故障，在具有足够冗余的系统设计中可能是可接受的。另一个例子是采用多样性和纵深防御以补偿软件共模的弱点。可使用危害对整个系统的影响对危害进行排序。

D.4.2.4.5 确定危害的处理

确定危害的处理就是决定是否确认及随后解决危害。系统研制者应评价危害对系统级的影响和可信性，并确定是否撤消或确认危害。使用多种方法以处理危害，诸如消除、减轻及控制危害后果，或使其后果减至最小。如果消除危害是不经济的，则应通过重新设计系统来对付危害。危害的控制不应是核电厂运行人员的责任。应修改危害分析，以考虑设计变更引入的新危害。

D.4.3 整个系统生存周期内危害的鉴别

下面各节提供了在整个系统生存周期内评价危害的详细指导。

D.4.3.1 安全系统的危害鉴别

安全系统危害的鉴别过程开始于对要求的安全功能、设计基准工况、选定的系统设计要素(如子系统、多样化系统等)和法规标准要求的理解。

危害鉴别过程应考虑：

a) 核电厂安全分析报告中确定的设计基准工况；

b) 认为造成安全设备失效的相互独立的、相关的和同时发生的危害事件，包括动力源和可以产生危害的共因条件；

c) 系统各部分之间的接口考虑，例如电磁干扰、硬件和软件控制的误启动，应包括考虑由软件(包括其他人编制的软件)对于子系统/系统故障的可能贡献，应确定用来控制安全软件的命令和响应(例如误命令、命令失效、不适时的命令或响应、或不希望的事件)的安全设计准则，并应采取适当的措施将这些准则包含到软件(及有关硬件)规格书中；

d) 包括运行环境在内的环境限制(如地震、极限温度、温度瞬变、噪声、暴露于外来物质中、火灾、静电放电、雷击、电磁环境影响和辐射)；

e) 运行、试验、维修和应急规程(如人因工程、操作人员作用、任务和要求的人因差错分析、设备布置、照明要求等因素的影响、噪声或温度升高的影响)；

f) 试验和维修设备的设计和使用，它们可能引入缺陷和软件差错；

g) 安全设备设计和可能的替换方法(如联锁、系统冗余、硬件或软件的故障安全设计以及子系统保护)；

h) 由于其他子系统(包括非安全系统)的运行造成系统的性能劣化；

i) 包括合理的人因差错和单点故障在内的故障模式，以及在子系统设备发生故障时产生的危害；

j) 软件(包括由其他人编制的软件)、事件、缺陷、事件(例如不适当的同步技术)对于系统安全的可能贡献；

k) 潜在的共模故障；

l) 软件设计要求和纠正措施的实施方法，这些方法可能会对安全系统造成损害或使其性能劣化，或引进新的危害；

m) 在系统验收期间及验收以后设计变更的控制方法以保证安全系统性能不会劣化，也不会产生新的危害。

D.4.3.2 计算机的危害鉴别

根据安全系统的分析结果，可确定计算机系统的某些安全功能、设计条件、限制及未解决的危害。计算机系统设计应规定为了阻止系统进入危害状态或者使系统从危害状态进入到非危害状态而需要由硬件或软件完成的那些功能，而且应鉴别和规定软件与计算机系统之间的接口。计算机的危害鉴别应考虑 D.4.3.1 的要求，只是把重点放在硬件和软件的初步设计上。此外，应把下述各项作为可能的危害：

a) 硬件与软件之间的相互依赖性(例如中断和操作系统)；

b) 可能使系统进入危害状态的动作序列；

c) 系统特有的可信危害，例如超前或滞后的输出、传感器输入处理故障、准确度或舍入问题、例外

情况的不适当处理、恢复动作、系统中断、输入电压或频率波动、符合信号改变的最大可信数目、电磁干扰和超量程数值(如被零除或未初始化的指示)。

D.4.3.3 软件需求的危害鉴别

在软件需求的危害鉴别过程中评价软件和接口要求,并鉴别出可能成为危害产生原因的差错和缺陷。在进行软件需求危害鉴别时应将软件要求与硬件设计的相容性作为一个基本问题,这包括下述活动:

a) 应对软件需求进行评价,以便鉴别出对完成安全功能必不可少的要求(即关键要求),应对这些关键要求进行评价,以便评定危害状态的重要性;

b) 程序大小和定时的要求应保证具有适当的资源用于执行时间、时钟时间和存储器分配,以支持关键要求(包括在最坏条件下的最大负载);

c) 在涉及到多软件系统集成的设计中应考虑系统各部分之间的相互依赖性和相互作用;

d) 应对现有软件进行评价以便充分确信没有引进对安全系统的运行有害的"未预期功能",未预期功能的可能解释包括:

1) 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;

2) 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,并采取适当措施解决这些危害,然后应通过V&V过程来确认对这些危害作出的适当响应;

3) 由于设计或实施错误产生的缺陷,V&V过程应处理由设计或实施错误引起的缺陷;

4) 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,以便说明研制辅助手段是否将保留在软件中,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,如果将研制辅助手段保留在软件中,则应进行V&V活动。

D.4.3.4 软件设计的危害鉴别

软件设计危害鉴别所包括的活动应确信没有引进新的危害。应对可能存在的计算问题进行评价,这些问题包括错误的方程、不够的精度、扫描速率和符号约定错误。应对方程、算法和控制逻辑中可能存在的问题进行评价,这些问题包括逻辑错误、未作处理的情况或步骤、重复逻辑、忽略的极端情况、不必要的功能、错误解释需求、遗漏条件测试、检查错误变量和不正确的迭代循环等。

对数据结构和预期使用中的数据从属性进行评价,这种从属性损害隔离分区、数据别名使用和故障抑制问题,从而会影响安全和对危害的控制或缓解。对可能存在的数据处理问题进行评价,这些问题包括不正确的初始化数据、已读取或贮存的数据、数据的换算或单位、计算出的数据和数据的范围。

应对接口设计进行审查,包括内部接口以及同系统其他模块之间的外部接口,对接口关注的主要方面是适当规定的协议以及控制和数据链接。对外部接口应进行评价,以便核实设计中的通信协议同接口要求是相容的,接口的评价应支持冗余管理分区和危害抑制的要求,可能存在的接口和定时问题包括不正确处理的接口、不正确的输入和输出时限、以及子程序/模块失配。

应确信设计符合已确定的系统限制。物理环境对于危害分析的影响可能包括:当使用最长的安全定时限制从最远的电路板获取数据时,高频时钟对于电路板的位置和关系以及总线锁存器的定时等。

应鉴别出完成关键功能的软件模块,在同其他模块连接和进行数据通信时,可能会发生某些潜在的问题,例如:字格式或数据结构的不相容性,为实现数据共享同其他模块的同步问题等。此外,应对非安全模块进行评价,以便确信它们不会对安全软件产生有害影响。

D.4.3.5 软件实现的危害鉴别

在软件实现阶段可能产生危害,在这一阶段应进行下述活动:

a) 对方程、算法和控制逻辑中可能存在的问题进行评价,这些问题包括逻辑错误、遗漏的情况或

步骤、重复逻辑、忽略的极端情况、不必要的功能、错误解释需求、遗漏条件测试、未检查变量和不正确的迭代循环等；

b) 确认算法的正确性，包括准确性、精度，以及方程的不连续性、超量程条件、断点、错误的输入、扫描速率等；

c) 评价程序中的数据结构和使用，以便确信对数据项已适当定义和使用；

d) 确认软件模块与外部硬件和软件之间接口的相容性；

e) 确认软件在由要求、设计和目标计算机系统对软件提出的约束范围内运行，以便确保程序在这些约束范围内运行；

f) 检查非关键程序，以便保证它不会对关键软件的功能产生有害影响，作为通用规定，安全软件应与非安全软件相隔离，检查的目的是证明这种隔离是完整的；

g) 验证软件编码处在定时和大小的恒定值内；

h) 验证良好的软件实践(例如程序大小的限制、避免多用户注册、可重复使用代码的控制、代码初始化等)的使用。

D.4.3.6 对于危害条件的计算机系统集成试验

计算机集成试验核实各种危害要求(禁止、俘获和联锁)已经正确实现，这种试验可验证软件在其规定的环境内正确工作。这种试验应在计算机研制过程中作为试验活动的固有部分来进行。在计算机系统集成试验中应进行下述活动：

a) 计算机软件单元级试验，以检验安全软件各组成部分的正确执行；

b) 接口试验，以检验安全软件各单元按预期要求运行；

c) 计算机软件配置项试验，以检验软件作为一个单元的执行情况；

d) 系统级试验，以检验软件在整个系统内的性能；

e) 承受能力试验，以检验软件在异常情况下(例如未预期的输入值)不会引起危害。

D.4.3.7 计算机系统确认试验

作为整个 V&V 过程的一部分，应对在最终硬件配置上运行的软件进行类似 D.4.3.6 的试验，以便确信已对鉴别的危害作了处理。

软件的故障树分析(见 D.4.2.3.2)可用于鉴别可能导致安全功能丧失的软件故障，或者证实不存在这样的故障。

D.4.3.8 维护和修改危害分析

应考虑系统验收后所作的维护和修改可能引起的危害的鉴别问题。依据维护和修改的范围来确定分析的范围，应按 D.4.4 的指导来考虑这些危害。

D.4.4 危害解决的一般指导

基于计算机的安全系统包括有完成安全功能必不可少的硬件和软件。此外，计算机系统可能也包括有对完成安全功能不是必需的设备(如自检)。危害鉴别和解决的焦点是保证安全功能不受已鉴别危害的影响，同时当非安全设备经受已鉴别的危害时，非安全功能不对安全功能产生危害。可考虑的一般指导如下：

a) 在系统的整个寿期内鉴别、评价和消除与每个系统有关的危害。在研制生存周期的每一阶段，解决上一阶段未解决的危害，并对当前研制阶段的设计进行分析，以鉴别新的危害；

b) 使极端环境条件(例如温度、压力、地震、振动、湿度、辐射和电磁干扰)引起的风险降低到最小；

c) 在系统设计中对系统操作和支持中由于人因差错所引起的风险作出处理；

d) 应给出明确的要求定义，以减少研制者误解释的可能性，可能出现的问题包括意义含糊的语句、未指明的条件、不明确的精度要求、未规定对危害的响应，以及不完整的、不正确的、相互矛盾的、难于实现的、不合逻辑的、不合理的、不可核实的或不能达到的要求；

e) 考虑和使用历史的危害数据，包括从其他系统取得的教训；

f) 只要可能，通过使用现有的设计和试验技术使风险减至最小；

g) 对设计配置或系统要求中的危害和文件变更进行分析，见 D.4.6；

h) 将鉴别出的危害及其解决办法（即设计变更或决定不采取进一步行动）形成文件，见 D.4.6。

一旦鉴别了一个危害，就应考虑危害的解决方法。下述指导可用于解决已鉴别的危害：

1) 如果可能的话，通过设计消除已鉴别的危害或者降低有关的风险；

2) 如果不能通过系统设计变更消除已鉴别的危害，则通过增加安全设备将有关的风险降低到可接受的水平；

3) 当设计或安全设备都不能有效地消除已鉴别的危害或者适当地降低有关的风险时，则应使用设备探测这种状态并产生适当的报警信号以便提醒人们出现了危害，报警信号及其应用应设计得尽可能减小人员对信号作出不正确反应的概率，并应在同类型系统内部实现标准化；

4) 在不能通过设计选择消除危害或者用安全和报警设备适当降低有关风险的情况下，则应编制规程和进行培训，以便对危害的发生作出反应。

D.4.5 已研制系统的危害评价

在安全系统设计中可以使用已开发系统中研制过的计算机、硬件或软件。5.4.2 要求通过商品级物项适用性确认来鉴定这些已研制的系统。附录 C 提供关于商品级物项适用性确认的指导，包括考虑硬件、软件或固件的故障（即可能影响安全功能完成的危害）。应在可能的范围内应用 D.4.3 和 D.4.4 的指导，因为彻底的软件设计危害鉴别和软件代码危害鉴别可能是不可实现的或是不必要的。

D.4.6 危害分析大纲、责任和结果文件

有关危害分析大纲、责任和结果的文件编制是很重要的，以保证这些活动按有序方式进行并产生可审查的结果。应将本附录说明的活动结合到计算机研制过程中，可将这些活动以检查表形式形成文件并纳入到管理和记录研制过程的那些文件中，而不推荐形成独立的一组文件。

D.4.7 初步的危害分析问题

下述问题举例对进行危害分析提供指导：

a) 系统故障怎么会花费公司大量的费用（未考虑随后的设计变更）？

b) 系统故障以怎样的方式导致安全功能失效？

c) 用户与新系统的相互作用方式与现有系统的作用方式有明显差别或仅有细微的差别吗？

d) 当使用新系统时，如果操纵员采用旧规程将会发生什么？

e) 当使用新系统时，如果维护人员采用旧规程将会发生什么？

f) 如果维护人员对系统进行在线变更将会发生什么？

g) 系统输入和输出与相关的核电厂接口（在电气上和机械上）是否兼容（即存在接口问题吗）？

h) 是否存在未显示给操纵员的系统潜在故障（特别是引起系统锁死的故障）？

i) 在所有运行条件下（在需求规格书规定的运行环境内）是否可能存在总线争用和定时问题？

j) 新的运行、维护或培训规程与当前的规程是否冲突？（核电厂人员是否知道使用新系统将要干什么？）

k) 新的系统试验程序是否会向系统引入新的危害（例如在一项试验完成后使安全系统功能被禁止）？

l) 自诊断功能是主动的还是被动的？自诊断如何影响系统？

m) 系统是否存在硬件或软件中断？如果存在，它们对系统的影响如何？未使用的硬件中断是连接到参考电位（例如接地）还是使之浮空，这是否导致系统故障？

附 录 E
（资料性附录）
通信独立性

E.1 背景

计算机在安全系统中的应用为单个安全通道内部的计算机之间、安全通道之间以及安全计算机与非安全计算机之间的高水平数据通信提供了可能(见 5.6)。这种通信能力的不适当使用可能导致计算机完成其本身功能或多项功能的能力丧失，从而妨碍安全系统完成其功能。本附录提供一些详细的方法，它们可用来最大限度地使用通信而不致对安全系统产生有害影响。为了防止安全通道之间的故障扩散以及防止故障从非安全计算机扩展到安全计算机，需要考虑采用隔离。

E.2 讨论

使用通信技术时主要关注的问题是需要排除由于通信活动可能造成安全功能的丧失。通信活动包括数据传输以及确认数据接收或指示数据传输故障用的任何载体。不能使任何通信故障的探测和校正妨碍或干扰安全功能的完成。

为使安全计算机对非安全设备具有适当的独立性，应保证电气隔离和通信隔离，但应注意的是实际的电气隔离点和通信隔离点可以不同。电气隔离要求见 GB/T 13286。下面推荐通信隔离的方法。

E.2.1 不同安全通道中计算机之间的通信

不同安全通道中计算机之间的通信可用于实现表决逻辑或标记同步时间标签。在发生通信故障时，如果该故障已被鉴别，则应置于优先故障状态。图 E.1 和图 E.2 表示实现这一要求的方法。

图 E.1 表示通道 A 中安全计算机和通道 B 中安全计算机之间的广播通信，单向通信路径提供一个软件隔离点。计算机之间的物理连接提供电气隔离，电气隔离可用光学方法来实现，例如光缆或光隔离器。通信隔离通过广播通信来提供。

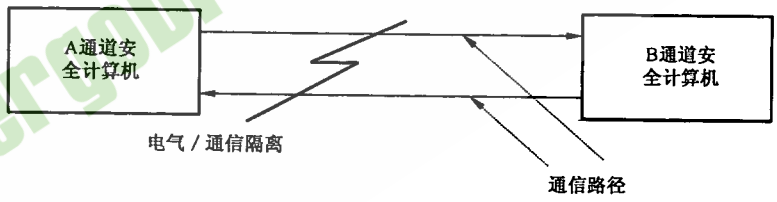

图 E.1 安全通道之间的通信(单向通信)

缓冲电路提供一个接口，用于确认或不确认通道之间的数据传送、免除冲突等。缓冲电路作为通信链路与安全功能设备之间的缓冲装置，以保证安全功能的完整性。缓冲电路应与完成安全功能的处理器隔开(至少装在不同的插件板上)，它可以是另一个处理器、存储器插件等。验证与确认(V&V)活动应包括缓冲电路。缓冲电路之间的物理连接应作为电气隔离点。

图 E.2 表示有两个分离隔离点的方法，一个是电气隔离点，另一个是通信隔离点。只要使用缓冲电路，这一方法就可以实现安全计算机之间的双向通信。

安全功能与缓冲电路之间的广播通信链路作为安全计算机发送数据的一个路径，与缓冲电路相分离的通信可使安全功能处理器从另一个通道接收数据。从另一通道请求和接收数据的过程不应导致任一安全功能的丧失。

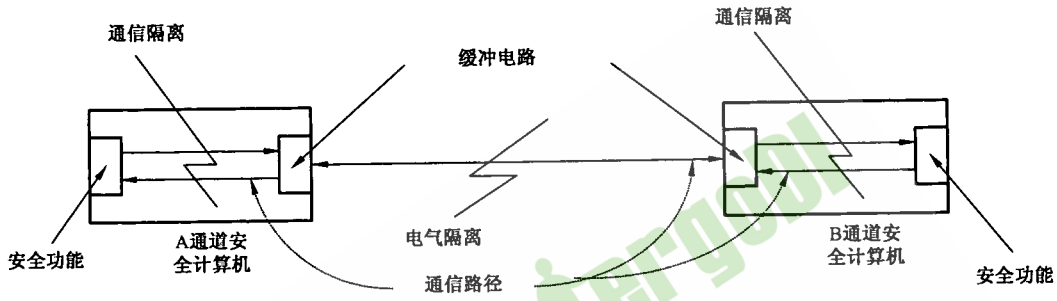

图 E.2 安全通道之间的通信(双向通信)

E.2.2 安全计算机与非安全计算机之间的通信

安全计算机与非安全计算机之间的通信可用于标记同步时间标签和设置已批准的整定值变更,但是,安全计算机在任何时候都不应从非安全计算机输入数据来完成其安全功能。图 E.3～图 E.5 表示了实现安全计算机与非安全计算机之间通信的方法。

图 E.3 表示安全计算机与非安全计算机之间的广播通信,单向通信路径提供通信隔离,计算机之间的物理连接可同时提供电气隔离和通信隔离。电气隔离可用光学方法实现(例如光缆或光隔离器),通信隔离通过广播通信路径来提供。

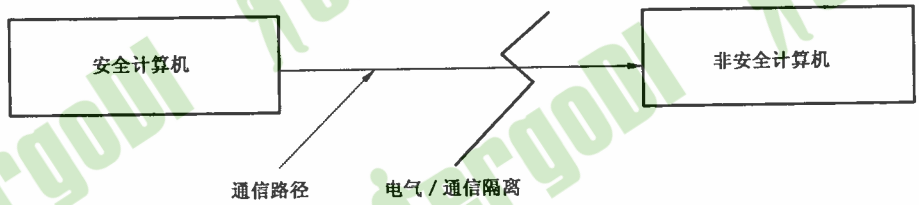

图 E.3 安全计算机与非安全计算机之间的通信(单向通信)

图 E.4 表示有两个分离隔离点的方法,一个是电气隔离点,另一个是通信隔离点。只要在安全计算机中使用一个缓冲电路,该方法便允许在安全计算机与非安全计算机之间进行双向通信。当一台独立的计算机用于试验和校准目的时,使用这一方法可能是必要的。

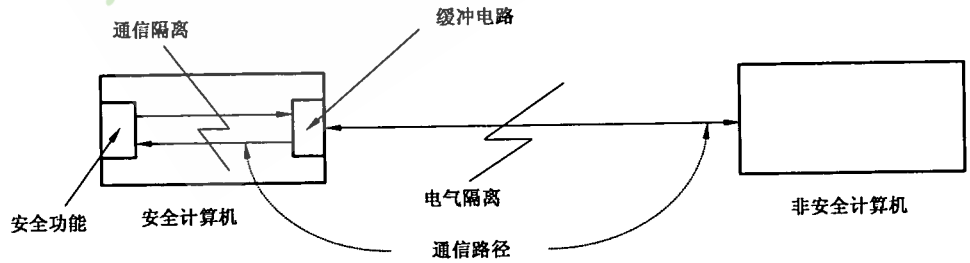

图 E.4 安全计算机与非安全计算机之间的通信(双向通信)

缓冲电络提供一个接口,用于确认或不确认通道之间的数据传送、免除冲突等。缓冲电路作为通信链路与安全功能之间的缓冲装置,以保证安全功能的完整性。缓冲电路应与完成安全功能的处理器分隔(至少装在不同的插件板上),它可以是另一个处理器、存储器插件等。验证与确认(V&V)活动应包

括缓冲电路。按要求，缓冲电路与非安全计算机之间的连接提供电气隔离。

安全功能与缓冲电路之间的广播通信链路作为安全计算机发送数据的一条路径，发送数据的过程不应导致安全功能的丧失。当使用一台独立的试验和校准用计算机时，从缓冲电路至安全功能的广播通信链路是必需的。

图 E.5 与图 E.4 类似，只不过非安全计算机中也使用可选择的缓冲电路和通信路径。

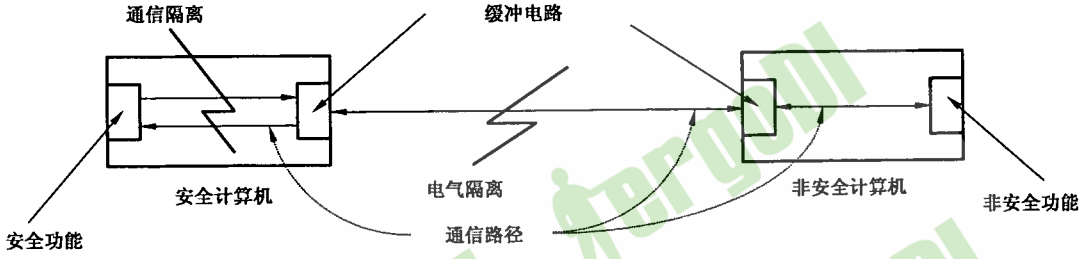

图 E.5 安全计算机与非安全计算机之间的通信

附 录 F
（资料性附录）
计算机可靠性

F.1 背景

当要求有定量的可靠性目标时，5.15 要求对硬件和软件都要予以考虑。本附录提供关于如何进行可靠性测定的指导，采用的方法是把计算机作为一个整体（即硬件、系统软件、固件和应用程序）来考虑。采用如规模、几何复杂性、数据流、从研制、故障和校正经验得到的平均故障间隔时间（MTBF）外推等结构特性来预测软件可靠性的其他方法，都尚未达到足以能给可靠性预测提供适当置信度的完备状态。

本附录介绍的方法给出可靠性的定量测定，但有下述限制：

a) 计算机可靠性按规格书中的功能要求测定，这一方法没有考虑规格书中的缺陷，在已试验的系统中很大一部分故障是由规格书中的缺陷引起的；

b) 这一方法得到非冗余计算机（即单个通道中的单列处理）的可靠性定量测定，但没有考虑共模故障或共因故障对冗余计算机可靠性影响的测定方法或其他方法。

在可靠性预测中应用具有这些限制条件的可靠性测定结果时，应对该结果进行调整，以便考虑规格书中可能的差错以及由共模故障和共因故障产生的不可用性影响。由于安全系统设计和软件结构的种类繁多，本附录不可能广泛说明完成这些调整的适用方法。

实时计算机故障的特点和后果是：

a) 这些故障在不可预测的时刻发生，因而任何故障（不论是起因于软件或硬件）都可以按类似于模拟硬件故障的方式作为随机事件来处理；

b) 这些故障是在处理器通过传感器、驱动器、通信接口和显示器与环境相互作用时软件在处理器上执行的结果而产生的，因而与执行该软件的整个计算机一起讨论软件的可靠性才是最有意义的。

这些故障是各个事件同硬件、软件或固件中的缺陷相互影响的结果，因而其中某些故障在研制过程中是潜在的，通常未予考虑。

这些故障一般涉及许多细节问题，包括同系统软件（操作系统、设备驱动程序等）的接口、未预期的性能、故障/差错处理、或定时和处理器负荷。

由于硬件或软件问题都能够引起计算机故障，因此有必要讨论如何能最好地描述、测定和分析由硬件和软件两者产生故障的概率。

对于计算机可靠性评定最难的问题是软件处理。本附录未对软件故障采取与硬件故障不同的方式来处理。但是，区分两种类型的计算机可靠性计算是有必要的，即面向预测的计算和面向测定的计算。

作为确定安全系统可靠性的组成部分，计算机可靠性测定既是可能又是希望的。计算机可靠性的一种量度是故障率，即单位时间内的故障数。计算机可靠性的测定与安全系统或硬件的可靠性测定是相似的，而且实际上应依据同样的数据组，即确定试验期间的故障数和试验时间。

测定过程中的一个关键因素是故障的记录和报告。按 IEEE Std 1012 的规定，使用术语“不符合项报告”来表示问题或故障报告。不符合项的报告和分析对评价计算机的可靠性是重要的。

不符合项报告提供的信息包括要求或设计不适当、故障模式的定性数据、计算机（软件和硬件）可靠性的定量数据、性能能力的数据（如容量、响应时间、处理能力）。不符合项报告包含的具体项目见 IEEE Std 1012。由于收集了数据，如在整个运行系统中测定的那样，可对数据进行平均故障间隔时间的分析，从而确定有缺陷的硬件或软件模块、故障探测和恢复的有效性（即有效域），以及未预期危害的发现比例，见附录 D。

F.2 讨论

计算机可靠性评定的必要条件是有完整的不符合项数据记录。如果有一个完整的不符合项数据库，就可以分析研制过程的有效性并确定计算机的可靠性。

F.2.1 研制过程评价

研制过程评价可尽量降低由于各个事件同硬件、软件或固件缺陷的相互影响而产生的计算机故障，见 F.1。对不符合项报告(按遗漏要求或不正确要求、故障模式鉴别、故障探测、恢复有效性等编写)和可靠性评定应进行认真研究。对根本原因的分析和研制阶段中的数据项应进行评价。

F.2.2 不符合项报告数据的使用

不符合项报告表明原先未鉴别出的故障模式、无效探测机理和无效恢复机理，应将该报告看作是确定计算机可靠性的输入。

将计算机集成到安全系统可能会增加危害的数量。可能没有预计到结构、应用、硬件和其他设计特点所特有的故障模式。因此，应不断进行故障模式和后果分析(FMEA，见附录 D)，并且当不符合项报告鉴别出新的故障模式时应进行更新。

为了区分不同类型的故障，有必要建立故障分类和判别准则。例如，根据操作系统失效还是只有应用软件失效，可将计算机“崩溃”与计算机“停机”区分开。将计算机故障数据用于可靠性测定的必要条件是故障发生和扩展所采取方式的概念性依据。

还应特别收集和分析故障模式数据，以表明软件处在及超过最大承受极限条件(处理能力、容量和数据)时的性能，并确定在外部异常条件下的软件性能。在这段时间内，应观测到对于新的故障模式发现比例呈现下降趋势。未出现这一趋势就可能表明，系统的故障特点尚未充分地表现出来，计算机可靠性测定过程可能需要延长，直到观察到这一下降趋势为止。

故障探测和恢复的有效性(即有效域)是影响冗余计算机可靠性的一个重要因素。这一有效性或有效域可以估算为：故障发生后的成功恢复次数除以在适当置信区间内发生的有关故障(取决于 FMEA 中应用的分类)的次数。在研制过程中，应进行充分的故障注入和故障模拟试验。然而，有效域的最有效测定是通过运行期间自然发生的故障来进行。提供关于有效域和各有效域机理方面数据的故障报告是进行这种估算的主要依据。可靠性确定可能需要一直延续到能探测和恢复有效性时为止。

对于不符合项报告的上述评价在研制新的系统和商品级计算机的集成中是有用的。在类似应用中的运行经验数据，特别是故障模式和可靠性分析数据，对确定已研制的软件或商品级软件的可靠性是很重要的。确定相似程度和已收集数据的完整性与全面性，对定量与定性表征这类软件的可靠性是很重要的。

F.2.3 计算机可靠性

一个安全通道中非冗余计算机的可靠性可以分成两个可测量的部分：平均故障间隔时间(MTBF)测定和正确响应概率。MTBF 是长时期内持续运行的一种表示法。正确响应概率是在假定硬件、系统软件和其他的运行环境因素都正常起作用时计算机对于始发事件响应的一种表示法。

F.2.3.1 MTBF 测定

MTBF 可用累计运行时间除以故障数来测定。应特别明确测定运行时间和计算机故障的方法，在确定运行时间时应处理的问题包括(但不限于)：

a) 有关硬件和软件配置的规格书，据此可收集计算机的运行时间；

b) 对未曾修改的模块在原状态下运行所采用的方法可用于确定运行时间；

c) 外部输入和输出的重现精度，以及如何收集处理器的运行时间。

在确定故障时应考虑的问题实例如下：

a) 故障成因；

b) 认为故障由计算机引起而不是瞬时故障或其他现象所使用的判别准则；

c) 统计已经排除的故障；

d) 统计由于同一缺陷引起的多重故障。

一旦确定了累计运行时间和故障，在假定 MTBF 在测定期间内保持不变的条件下，应用 MIL-HDBK 781 中程序计算出 MTBF 的上、下边界值。一旦按这种方式测定了故障率，同时假定可靠性按指数分布或其他方式分布，就能确定规定时间间隔内定量的可靠性。

F.2.3.2 正确响应概率

正确响应概率是在提出要求时成功概率的测定值，它可用系统试验时取得的数据来得到。通过实施有关的测试案例以及确定成功与不成功案例之比，便可测定成功概率。应把下述问题视为这种测定的一部分：

a) 确立一组有代表性的和无偏的测试案例，在只需要一次输出的案例中（例如反应堆紧急停堆的驱动信号），测试案例组只需要考虑输入的组合，然而，在涉及到连续闭环控制的场合下，测试案例组还应考虑预计运行时间的范围以及被控制系统的动态过程；

b) 在只测试输入空间的一次取样而不是测试整个输入空间时（对于许多较简单的安全系统，测试整个输入空间可能是可行的），可确定成功比例所采用的方法；

c) 试验环境的真实性以及相对于试验环境而言运行环境中不确定性的处理；

d) 可将以前的试验结果同追溯性检查和试验相结合所采取的方法；

e) 部分成功结果（相对于全部成功）的处理，特别是在连续控制情况下（例如阀门在部分行程上的振荡）；

f) 确定实际成功或失效所用的方法，特别是对于连续控制功能。

综合试验结果以便确定单一的正确响应总概率所采用的方法取决于试验的种类以及预期的结果。例如，在可以确定离散的成功/失败结果的场合下（如具有检测和控制功能的典型情况），成功和失败的加权平均值以及应用二项式分布得到的置信区间可能是适当的。在涉及到长时期内连续闭环控制的其他情况下，可采用连续记录法。此时，采用不同方法确定置信区间可能是必要的。

F.2.3.3 MTBF 与正确响应概率的综合

按下述假设可将 MTBF 和正确响应概率综合为单一的可靠性数值：

a) 采用指数分布将 MTBF 变换为可靠性估计值，除非另有说明；

b) MTBF 代表了整个计算机，包括系统硬件、软件、设备驱动器以及运行环境的其他部件，可靠性估计值表示该系统在给定时间间隔内无故障运行的概率，因此如对安全系统提出任务要求，有关的数据将成功地作为该应用的输入；

c) 假如安全系统任务的有关数据已成功地置于输入缓冲区中，则正确响应概率表示该应用将输出正确结果的概率；

d) 基本系统软件和运行环境的故障概率以及安全系统应用中所用逻辑的故障概率是独立的。

在给出这些假设之后，就能确定通道可靠性：

$$Rch = Rc \times S$$

式中：

Rch——通道可靠性；

Rc——由测得的 MTBF 推算得到的通道可靠性；

S——正确响应概率。

F.2.3.4 结合通道可靠性来确定安全系统可靠性

可用 GB/T 9225 给出的与硬件所用技术相类似的方法来确定安全系统可靠性，但应考虑：

a) 通道故障独立到什么程度，也就是共模故障和共因故障的相对重要性，后者可能由于使用相同的硬件、操作系统、运行条件或监督和维修规程所引起；

b) 对各个通道输出进行组合所采用的方法，以及在组合点发生故障所达到的程度；

c) 恢复和修理时间要求与系统响应时间要求的相互关系。

在 MTBF 可满足可靠性分配或目标，但对共模和共因故障的正确响应概率未能满足上述可靠性分配或目标的情况下，将特定功能软件的多样化实施方法引入安全系统可能是必要的，见附录 B。当必须采用多样化措施时，应对多样化实施方法进行评价（见附录 D），以便证实故障模式是多样化的而且是不相关的。

参 考 文 献

[1] GB/T 9225 核电厂安全系统可靠性分析一般原则.

[2] GB/T 13286 核电厂安全级电气设备和电路独立性准则.

[3] ANSI/ANS 51.1-1983(R1988), Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants.

[4] ANSI/ANS 52.1-1983(R1988), Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants.

[5] IEEE 100, The Authoritative Dictionary of IEEE Standards Terms, New York, Institute of Electrical and Electronics Engineers, Inc.

[6] IEEE Std 1012-1998, IEEE Standard for Software Verification and Validation.

[7] IEEE Std 1012a-1998, IEEE Standard for Software Verification and Validation—Content Map to IEEE/EIA 12207.1.

[8] IEEE Std 1061-1998, IEEE Standard for a Software Quality Metrics Methodology.

[9] IEEE Std 1228-1994, IEEE Standard for Software Safety Plans.

[10] IEEE Std 1042-1987 IEEE Guide to Software Configuration Management.

[11] IEEE Std 1540-2001, IEEE Standard for Life Cycle Processes—Risk Management.

[12] IEEE/EIA 12207.0-1996 Industry Implementation of International Standard ISO/IEC 12207: 1995(ISO/IEC 12207 Standard for information technology—Software life cycle process—Description).

[13] MIL-HDBK 781, Reliability Test Methods, Plans, and Environments for Engineering Development, Qualification and Production.

[14] MIL-STD-882B, System Safety Program Requirements.

[15] Title 10 of the Code of Federal Regulations.

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—2008
*
中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
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 2.5 字数 67 千字
2008 年 11 月第一版 2008 年 11 月第一次印刷
*
书号:155066·1-33630 定价 28.00 元

GB/T 13629-2008