ICS 27.120.20
F65
备案号：46483-2014

NB

# 中华人民共和国能源行业标准

NB/T 20298—2014
代替 EJ/T 529—1990

# 核电厂安全重要数字仪表和控制系统 硬件设计要求

**Nuclear power plants - instrumentation and control important to safety - Hardware design requirements for digital systems**

2014-06-29 发布　　2014-11-01 实施

国家能源局　发布

# 目　次

前言 ..... II
1　范围 ..... 1
2　规范性引用文件 ..... 1
3　术语和定义、缩略语 ..... 1
4　项目结构 ..... 3
5　硬件需求 ..... 4
6　设计和开发 ..... 6
7　验证和确认（V&V） ..... 9
8　鉴定 ..... 11
9　制造 ..... 11
10　安装和调试 ..... 11
11　维护 ..... 11
12　修改 ..... 13
13　运行 ..... 13
附录A（资料性附录）　本标准与IEC　60987:2007相比的结构变化情况 ..... 14
附录B（规范性附录）　预开发硬件的评估 ..... 15
附录C（规范性附录）　可编程逻辑器件开发的适用性 ..... 16
附录D（资料性附录）　系统生命周期总貌 ..... 17
附录E（资料性附录）　鉴定示意图 ..... 18
附录F（资料性附录）　维护程序举例 ..... 19
参考文献 ..... 20

# 前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准代替EJ/T 529—1990《用于核电厂安全重要系统数字计算机》，与EJ/T 529—1990相比，主要技术变化如下：

——本标准考虑了近些年计算机设计工程技术显著发展的现状（见第 1 章）；

——增加和替换了相关标准要求，特别是NB/T 20026、NB/T 20054和NB/T 20055（见第1章、第2章、3.1、4.1、5.1.1、5.3.5、5.5、6.5、7.1.2、7.9、10.4、10.8、11.2.6、12.2和第13章）；

——增加了术语“固件”、“预开发”、“鉴定寿命”、“显性硬件故障”、“单一故障”、“安全重要系统”、“系统确认”、“隐性硬件故障”、“验证”及定义（见 3.1.1～3.1.5、3.1.7～3.1.10）；

——删除了术语“可用性”、“计算机”、“计算机系统”、“部件”、“设计”、“研制”、“多样性”、“综合测试”、“可维修度”、“维修”、“模件”、“合格寿命”、“冗余”、“可靠性”、“软件”、“子系统”、“系统”、“鉴定”、“检验”及定义（见 1990 版的 3.1～3.14、3.16～3.20）；

——修改了术语“单一故障准则”的定义（见 3.1.5，1990 版的 3.15）；

——增加了缩略语（见 3.2）。

本标准使用重新起草法修改采用IEC 60987:2007《核电厂基于计算机安全重要仪表和控制系统的硬件设计要求》。

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

本标准与IEC 60987:2007的技术性差异及其原因如下：

——修改了第 1 章范围的内容，以满足 GB/T 1.1—2009 的要求；

——关于规范性引用文件，本标准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：

- 用等同采用国际标准的GB/T 7826代替IEC 60812（见5.3.4）；
- 用修改采用国际标准的GB/T 12727代替IEC 60780（见第8章、11.2.4）；
- 用等同采用国际标准的NB/T 20026代替IEC 61513（见第1章、第2章、3.1、4.1、5.1.1、5.3.5、5.5、6.5、7.9、10.4、10.8、11.2.6、12.2、第13章）；
- 用修改采用国际标准的NB/T 20054代替IEC 60880（见第2章、3.1.8、3.1.10、7.1.2、7.9、第13章）；
- 用修改采用国际标准的NB/T 20055代替IEC 62138（见第2章、7.1.2、7.9、第13章）；
- HAF 003代替IAEA 50-C/SG-Q（见第2章、4.3.1）；
- 删除ISO 9001的引用。

——删除了下述在标准中未使用的术语及其定义：

- 3.2　商品化的；
- 3.3　多样性；
- 3.7　核电厂；
- 3.11 安全有关系统；

● 3.12 安全系统。

——增加缩略语（见3.2）

本标准由能源行业核电标准化技术委员会提出。

本标准由核工业标准化研究所归口。

本标准起草单位：中核控制系统工程有限公司。

本标准参编单位：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。

本标准主要起草人：王怀敬、刘瑞、梁嘉琳、韦智康、张鑫、孙武、金成日、李灵坡。

# 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

本标准规定了核电厂1级和2级（见NB/T 20026中的定义）计算机系统硬件设计要求，包括硬件需求、验证和确认、鉴定、制造、安装和调试、维护、运行等相关内容。

本标准适用于核电厂1级和2级计算机系统新硬件的设计，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。

本标准不适用于用于软件下载和检查的计算机硬件设施。

注1：本标准不关注 3 级计算机系统硬件，此类系统宜采用商用级标准开发。

注2：支持可编程逻辑设备设计过程的基于软件的工具宜总体上服从相应软件标准中所提供的指导，见 NB/T 20054（1 级系统）或 NB/T 20055（2 级系统）。

注3：对于预开发硬件的开发见附录 B，对于可编程逻辑器件的开发见附录 C。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 7826—2012 系统可靠性分析技术 失效模式和影响分析（FMEA）程序（IEC 60812:2006, IDT）

GB/T 12727—2002 核电厂安全系统电气设备质量鉴定（IEC 60780:1998, MOD）

NB/T 20026—2010 核电厂安全重要仪表和控制系统总体要求（IEC 61513：2001, IDT）

NB/T 20054—2011 核电厂安全重要仪表和控制系统执行A类功能的计算机软件（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类和C类功能的计算机软件（IEC 62138:2004, MOD）

HAF 003 核电厂质量保证安全规定

HAD 102/10 核电厂保护系统及有关设施

IEC 61000（所有部分） 电磁兼容（electromagnetic compatibility）

IEC 61025 故障树分析（Fault tree analysis）

## 3 术语和定义、缩略语

### 3.1 术语和定义

NB/T 20026—2010界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了NB/T 20026—2010中的某些术语和定义。

3.1.1

**固件 firmware**

安装于硬件中并与该硬件特性密切耦合的软件。

注：固件的表现形式通常对硬件部件的用户是“透明的”，由此可认为是硬件设计的一个有效组成部分（这类软件很好的一个例子如处理器微代码）。总之，固件可以只通过用户更换硬件部件（例如，处理器芯片、卡件、EPROM）来修改，这里所指的硬件部件包括了与部件一起的软件，即更换后部件包括了修改的软件（固件）。在这种情况下，设备用户对硬件部件的配置控制可有效用于对固件的配置控制。本标准所指的固件实际上是嵌入硬件中的软件。

3.1.2

**预开发　pre-developed**

现有的、作为商品或专有产品可得到的，用于基于计算机系统的物项。

注：这个定义与NB/T 20026—2010中“预开发软件”定义是一致的。

3.1.3

**鉴定寿命　qualified life**

一个构筑物、系统或部件通过试验、分析和（或）运行经验已证明其能够在特定运行工况下在验收标准范围内运行，同时保持在设计基准事故或地震条件下能够实施其安全功能的时间。

[NB/T 20063—2012，定义6.1.8]

3.1.4

**显性硬件故障　revealed hardware failure**

可自动探测并告知的硬件故障，例如，一块板卡的故障可通过看门狗电路自动探测并触发报警。

3.1.5

**单一故障　single failure**

导致某一部件不能执行其预定安全功能的一种故障，以及由此引起的各种继发故障。

[NB/T 20063—2012，定义2.40]

3.1.6

**单一故障准则　single failure criterion**

要求系统或设备组合在其任何部位发生可信的单一随机故障时仍能执行其正常功能的设计准则。

[NB/T 20063—2012，定义2.41]

3.1.7

**安全重要系统　system important to safety**

属于某一安全组的一部分和（或）其失效或故障可能导致对厂区人员或公众的辐射照射的系统。

[IAEA Safety Glossary:2006]

3.1.8

**系统确认　system validation**

通过检查和提供其他证据，证实该系统完全满足预期的需求规格书（功能、响应时间、容错、鲁棒性）。

[NB/T 20054—2011，定义3.37]

3.1.9

**隐性硬件故障　unrevealed hardware failure**

不能被系统自动探测，并且只有在试图使用依赖该故障硬件的某一功能时才能显现的硬件故障。这类故障可通过功能测试或对该系统有运行请求时发现。

3.1.10

**验证　verification**

通过检查和提供客观证据，证实该过程某种活动的结果是否符合为此活动规定的目标和需求。

[NB/T 20054—2011，定义3.38]

### 3.2 缩略语

下列缩略语适用于本文件。

COTS：商品化的（Commercial Off The Shelf）

ATE：自动化测试设备（Automated Test Equipment）

FMEA：故障模式和影响分析（Failure Mode and Effects Analysis）

FTA：故障树分析（Fault Tree Analysis）

## 4 项目结构

### 4.1 综述

基于计算机的安全重要系统的开发项目宜分为若干阶段。每个阶段宜在一定程度上是完备的但要依赖其他阶段提供输入，同样也要提供输出作为其他阶段的输入。项目的各个阶段共同构成整个安全生命周期（见NB/T 20026—2010第5章）。NB/T 20026—2010允许在不影响开发过程完整性的前提下，项目的各个阶段可并行开展。

质量保证大纲应应用于硬件生产过程。

### 4.2 项目分解

下列总体要求定义了本标准范围内计算机系统的硬件开发生命周期要求：

a) 硬件开发生命周期应与整个系统生命周期一致（参见附录 D）；
b) 硬件开发生命周期的每个分阶段应由明确定义和文档记录的活动构成；
c) 设计所包括的现有硬件产品（如 COTS）在使用前应进行相应的核对、验证和测试；
d) 应提供足够的手段（如备品备件、测试和维护设备等）和场所（如实验室、车间、场地等）来执行与每个开发阶段相关的任务；
e) 每个开发阶段应形成适当的文档；
f) 每个开发阶段应进行总结性验证（见第 7 章）；
g) 每个验证活动的结果应形成可审计的文件，记录所达成结论和执行验证而导致的任何设计变更；
h) 应制定所有工作活动的进度计划以保证下列活动的足够时间：
   1) 解决软件和硬件开发阶段之间的任何相互影响的问题，以确保系统软硬件的兼容；
   2) 形成文件与执行测试、验证和质量保证活动。

### 4.3 质量保证

4.3.1 设计和开发过程应满足 HAF 003 的相关要求。硬件质量保证大纲应作为一个独立文件（或多个文件）或整个质量保证大纲的一部分。大纲应关注现有硬件的使用和需要的硬件开发。作为硬件开发过程的一部分，由电厂操纵员、业主、承包商和分包商所执行的所有硬件质量相关活动宜包括在质量保证大纲中。

4.3.2 硬件质量保证大纲宜涉及以下阶段，这些阶段在任何特殊系统或开发中均适用：

a) 设计和开发；
b) 采购；
c) 制造；
d) 建造和调试；
e) 运行和维护。

4.3.3 在设计过程开始前并不要求覆盖上述所列所有阶段，但是在每个阶段启动之前，该阶段要求的大纲应准备就绪。

4.3.4 质量保证大纲宜描述质量有关活动的组织、管理和执行，包括：

a) 文档配置控制；
b) 设计过程；
c) 产品和服务的采购过程；
d) 建造指导、建造程序和图纸的配置控制；
e) 用于建造系统硬件的物料和物项的配置控制；
f) 质量控制活动，诸如正式检查；
g) 测试设备的控制；
h) 硬件搬运、储存、运输的控制；
i) 测试过程；
j) 监督不符合项的产生和纠正措施的实施；
k) 质量保证记录存档流程；
l) 内审程序。

## 5 硬件需求

### 5.1 综述

5.1.1 硬件需求应与系统要求一致，并构成计算机系统技术规格书的一部分（见NB/T 20026—2010中第6章）。计算机系统技术规格书是对软件和（或）硬件组合系统的描述，规定了系统设计目标和计算机系统所执行的功能（系统既可以是为某一特定应用所开发，也可以是为通用应用所开发，即平台开发。对于后一种情况，系统开发是基于通用的系统要求）。

5.1.2 硬件需求应在系统硬件需求规格书或其他适宜的文件中予以规定。

5.1.3 硬件需求应根据一种技术或方法予以呈现，其格式不应妨碍可读性，即硬件需求宜易于理解。

5.1.4 硬件功能需求应是明确的、可测试的和（或）可验证的和可实现的。

5.1.5 硬件需求规格书宜给出一个总体性的硬件要求，确定核安全重要的硬件功能（但是，如果与系统软件一起提出，则这些要求宜在系统需求规格书中定义），确定硬件设计要求，规定硬件可靠性要求和硬件环境适应性要求。

5.1.6 计算机系统的硬件需求可包括硬件通用要求和对计算机系统硬件特殊要求（例如，电缆、外壳的表面处理）。

5.1.7 硬件功能需求宜描述应该做什么，而不宜描述应该怎么做。但是，使用现有的部件和（或）平台可导致一定程度的自下而上的硬件设计。在选用这类现有部件前，应进行评估以确认其硬件性能特性（例如，故障模式）与系统要求一致。如果发现任何异常，则通过修改硬件设计或系统设计使其一致（同时保证不降低系统核安全要求）。

### 5.2 功能和性能需求

5.2.1 硬件功能和性能需求应与安全重要系统的功能和性能要求一致。

5.2.2 硬件功能和性能需求，结合软件要求（必要时，涉及所有硬件需求）应进行系统要求的一致性验证。

5.2.3 系统直到部件级的所有组成部分（含软件）应按照附录B的范围进行如下评估：

a) 硬件功能需求应包括但不限于对下述内容的定义：

1) 整个计算机系统硬件和每个硬件子系统的用途；
2) 与计算机系统连接的传感器和执行器的数量和类型；
3) 人机接口设备（诸如显示器、打印机和键盘）的数量和类型。

b) 供货商所移交的准备集成到系统中的每个部件和子系统宜附有一个规格书，关注其所有与安全有关方面的性能。如果不能提供这样一份规格书，则应进行分析，至确定部件的硬件设计特性达到与其适用性相符所必要的程度；

c) 硬件性能要求应包括（适用于任何特殊应用）：
1) 要求的数据采集速率；
2) 要求的数据处理能力；
3) 要求的计算容量；
4) 要求的可靠性和（或）可用性；
5) 要求的通讯接口（协议、传输速度）；
6) 要求的计算和转换精度；
7) 要求的信号抗噪声能力；
8) 要求的响应时间；
9) 物理尺寸限值；
10) 布置（位置）要求（例如，数据传输线的长度）；
11) 要求的备用容量（如果要求）；
12) 环境适应性鉴定要求；
13) 供电要求。

d) 应说明系统或软件设计对硬件设计的任何约束。

## 5.3 可靠性和（或）可用性要求

5.3.1 硬件可靠性和（或）可用性要求应与整个系统的可靠性要求一致。要求应包括任何故障类型的描述，这些故障在没有功能丧失或在已定义的有限功能丧失条件下都必须是被容许的。宜提供硬件可靠性目标。

注：本条所述硬件可靠性涉及随机硬件故障，不包括任何逻辑设计错误引发的故障。

5.3.2 不论硬件可靠性和（或）可用性如何要求，核电厂整个仪表和控制系统结构应满足HAD 102/10中7.5的单一故障准则。

5.3.3 硬件要求宜给出硬件可靠性参数的目标值[诸如平均故障间隔时间（MTBF，对显性和隐性的），平均修复时间（MTTR，对显性故障）。由硬件设计详细分析支持的可靠性描述的要求宜予以说明，例如，子组、板卡级或部件级分析。

5.3.4 可用于分析可靠性和系统硬件故障影响的方法包括：

——FTA，其中考虑了引起或促使一个确定不期望事件发生的条件和因素的识别和分析（见 IEC 61025 关于此技术的建议）。

——FMEA，其中确定了对系统性能有重大影响后果的故障，例如，可靠性、安全、可用性（见 GB/T 7826 关于该技术的建议）。

如果使用适合于1级和2级硬件系统的任何分析技术，应确保任何潜在的硬件故障没有不可接受的核安全影响。

5.3.5 诸如FTA与已知的部件故障数据相结合的技术，可用于系统硬件可靠性特性的数值计算。除有足够的运行经验可提供很高的置信度证明该硬件可靠性目标是可达到之外，这种方法应应用于1级系统硬件分析（见NB/T 20026）。这种技术宜同样用于2级系统，或者，尤其在对硬件可靠性要求不过于苛刻

的情况下，采用定性化论证（例如，部件质量、硬件冗余度、运行经验、显性硬件故障对隐性硬件故障的比例等）来证明其有足够的可靠性。

5.3.6 应确定保证计算机系统全寿期内可靠性和可用性的策略和规定。这些措施应作为维护要求形成文档，这些文档应包括防止维护活动引入可能导致共因故障的缺陷的要求。对多重序列系统的维护活动，通常被认为最有可能引入这些缺陷，因而，系统设计时应使这类活动减少到适当的程度。当要求的维护活动有可能导致共因故障时，则设计要求应详细说明是如何使这类故障的风险最小化的。

5.3.7 维护要求宜涉及下述内容（适用任何特殊系统）：

a) 硬件维护活动期间对系统运行的要求；

b) 易耗品更换，例如，空气过滤器；

c) 子系统、模件和（或）部件常规更换的任何要求；

d) 要求硬件维护活动后进行硬件再确认的程度（如测试）。

5.3.8 在需求规格书宜确定“做什么”而不是“怎么做”的原则下，在一个项目的需求规格书阶段详细确定维护要求可能是不切实际的，因此，这些要求宜在开发过程的稍后阶段予以完全确定。

### 5.4 环境适应性要求

5.4.1 硬件环境适应性要求应涉及适用的物理限制、气候、地震、化学、电气和辐射条件。宜同样包括安装和调试期间的任何适用的特殊要求。

5.4.2 应根据运行环境的要求规定抗电磁干扰的程度，并按适用的标准进行试验（如IEC 61000）。运行场所的电磁环境有可能受到多种类电气干扰源的影响，例如开关柜、移动电话、继电器、对讲机、静电放电、雷电、接地故障。

5.4.3 所规定的电磁鉴定水平宜与运行条件中所有可信的最恶劣情况的实际估算一致。

5.4.4 硬件要求应明确任何禁用的构材，以及任何待用的特殊材料或特殊生产工艺类型的要求。

5.4.5 如果要求一个特殊的硬件鉴定过程，则该要求宜体现在硬件需求中。

### 5.5 文档要求

硬件文档要求应作为计算机系统文档要求的一部分处理（见NB/T 20026）。形成的文档宜包括：

a) 设计文件（系统硬件部件、接口硬件设计等）；

b) 操作手册；

c) 维护手册。

## 6 设计和开发

### 6.1 综述

6.1.1 新硬件的设计和开发过程宜把硬件需求规格书作为一个输入。设计过程宜通过不同设计阶段逐渐深入，最终生产出满足需求规格书要求的硬件。

6.1.2 较总体层面的设计活动可称为“初步”设计，包括不同设计可选方案的分析，以确定至子系统和模块一级的硬件系统结构。

6.1.3 初步设计之后一般是一个或更多个层次的详细设计。详细设计活动应把初步设计扩展到子系统、模块和部件一级的详细设计，使整个硬件设计描述充分完备达到可实施的程度。

6.1.4 可搭建硬件模拟件，不仅用于验证硬件模块间的相互作用是否正确，还可用于检查硬件和软件的兼容性。

6.1.5 预开发（例如COTS）部件可用于所有的系统硬件或硬件部件的子组件。6.2～6.7主要是考虑要求定制硬件开发的情况，但是，适当情况下，这些小节也提供了定义如何可用于预开发部件使用的指导。

## 6.2 设计活动

6.2.1 硬件设计应涉及基于硬件性能的系统性能要求，并且论据应可用，通过分析或测试来表明硬件设计满足这些要求。这些要求可包括计算精度、时间响应、环境适应性能力和供电要求（对于现有部件，应进行部件硬件规格书与系统硬件要求的对照验证，确保现有部件满足规定要求，或者通过测试验证硬件性能）。

6.2.2 任何与硬件需求的差异应通过修改设计，或者修改需求来解决（任何修改的影响应进行全面评估并形成文档）。

6.2.3 硬件设计者应识别出那些表明性能要求已经达到的必要测试。这些测试可以对硬件单独执行，或者在软硬件集成时执行，即作为系统集成测试阶段的一部分。

6.2.4 硬件设计者应规定任何需要的维护活动，以提供设备全运行寿期内能达到性能和可靠性要求的置信度，可包括运行测试、标定、维修、定期更换和维护程序。宜使此类活动的执行达到这样程度，即为设备正确运行提供充分置信度，又使对系统的人为干扰和介入系统工作的执行最小化，进而降低这些维护活动引入的错误的可能性（诸如潜在的共模故障缺陷）。

6.2.5 一旦规定了一个鉴定的目标寿命，则应论证该目标是现实并可达到的。

## 6.3 可靠性

6.3.1 宜在硬件需求文档中规定可靠性要求（见5.3）。

6.3.2 为支持系统级的安全分析，设计期间应进行硬件潜在故障分析。一旦执行一个核安全功能要用到一个系统的多个序列或多个系统（每个系统可能有单个或多个序列设备），则分析中应包括潜在硬件共因故障的适当考虑。硬件共因故障的可能途径如下：

——对设备的多个序列同时或顺序进行维护活动（特别是可能引入隐性硬件故障的活动）；

——定期测试；

——影响一个（多个）核安全功能的设备的多个序列同时发生隐性随机硬件故障；

——影响多个设备序列的，并且设计过程不能被发现的隐性设计错误。

6.3.3 可用于分析硬件可靠性和系统硬件故障影响的方法包括FTA和FMEA（见5.3.4）。

6.3.4 硬件设计宜使下列对核安全因素的潜在影响最小化：

——维护活动；

——随机硬件故障导致的系统故障；

——环境条件导致的硬件故障。

6.3.5 如果认为针对硬件某一特殊用途而评估出的可靠性是不足的，则应采取补救措施，可通过设计改进或运行变更的方式进行（诸如提高运行测试频度）。但是，宜谨慎选择增加运行测试的方式，因为任何引入运行电厂的活动都可能会由于引起或引入缺陷而带来一定程度的风险（即，综合衡量之后的运行测试对安全的最终影响可能是负面的）。理想情况下，所有的测试宜在测试过程中潜在缺陷不会对核安全造成影响时进行，例如，电站停运期间或被测试设备与运行电厂隔离时。

6.3.6 当使用概率安全评价来支持核电厂的安全案例时，则所评估的硬件可靠性概率值（例如，采用FTA）可引入到核电厂的分析中，并有助于全厂可靠性计算的准确性。

## 6.4 维护

硬件设计应涉及硬件需求规格书中所包含的任何维护要求。此外，可行时，设计宜包括降低由于维护活动所引入的错误风险的措施。例如下列措施：

——由于故障可能要求更换的部件宜易于接近；
——可更换部件宜标识清晰，使维护人员易于检查使用了正确的部件；
——宜有足够的端接空间；
——宜提供足够的专用端子用于标定和（或）测试活动（这样不需要断开接线以便于此类活动）；
——硬件设计宜提供一张标识清晰的结构布置图以减少可能的维护错误。

## 6.5 接口

防止故障通过系统接口扩展的系统接口要求见NB/T 20026—2010的 6.1.1.2.1，。

## 6.6 修改

硬件应设计成具有满足硬件需求规格书要求程度的可修改能力（见第12章）。

## 6.7 电源故障

计算机系统应设计成满足硬件需求规格书要求程度，对短期电源故障的后果和供电电源的可能波动[电压和（或）频率]是不敏感的。应提供将此类电源波动通知给运行维护人员的系统措施（本功能可能不在硬件中，因此可能超出本标准的范围）。

## 6.8 部件选择

一旦使用现有部件，则部件设计应与其在系统硬件中的作用兼容。

## 6.9 设计文档

6.9.1 硬件设计文档应描述硬件设计和已涉及硬件要求的措施。推荐使用标准化的设计文档格式和自动化的硬件设计工具。

6.9.2 计算机系统硬件设计文件宜按若干个文档“层次”的结构发布。每个层次的设计文档宜详细规定该与层次设计相关的各方面设计，并定义其下一层次的硬件要求。在设计过程中应发布制造和（或）组装、工厂测试、安装、调试、维护和运行的文件（如果适用）。

6.9.3 可发布初步的硬件设计描述对硬件结构进行定义，即系统不同部分间的结构和关系，宜包括硬件的总体布置连同下一层次的子系统和模块的结构图，也宜包括详细设计的硬件要求，例如：

——中央处理器单元和其他处理器的数量和类型；
——计算机存储器的硬件要求；
——接口的数量和类型；
——数据链和总线的数量和类型。

6.9.4 在硬件设计和开发结束时应形成文档，包括全部和最终的描述，涵盖直到最底层的全部设计细节和硬件的性能、限值以及其他特性。

6.9.5 最终描述文档应提供下列信息：

a) 设计综述；
b) 支持设计文件的参考资料；
c) 硬件子系统中分解硬件的描述；
d) 每个子系统的主要模块和部件的描述（例如，结构图、电路图）；
e) 子系统硬件接口描述，接口应就逻辑、物理、电气和其他方面进行适当描述；
f) 计算机系统硬件接口描述，任何与核电厂内部或外部其他系统的接口应明确表明详细的接口和相关硬件要求；
g) 物理布置— 宜提供设备物理布置的图文描述；

h) 鉴定数据（见第 8 章），包括维持规定鉴定寿命所要求的任何必要行动（诸如部件更换）的定义。同样宜提供备品备件储存期限的相关鉴定数据；
i) 维护要求；
j) 如何满足硬件可靠性和故障安全性能要求的描述。

## 7 验证和确认（V&V）

### 7.1 综述

7.1.1 设计与开发过程应包括正式检查，以证明每个设计和开发阶段所移交的硬件设计满足前一阶段所提要求。

7.1.2 硬件验证过程一般认为开始于硬件设计需求与系统设计需求的对比验证，结束于系统软件集成到硬件中。对于1级和2级系统硬件和（或）软件集成阶段的相关要求见NB/T 20054 和NB/T 20055。

### 7.2 验证大纲

应编制正式的验证大纲来确定验证硬件设计和控制验证过程所采用的方法。在启动验证活动前应编制大纲。大纲文件宜包括所使用的人员和（或）组织、组织结构、采用的验证方法、执行验证的等级、进度和其他验证有关的重要项目活动。

a) 验证可与设计过程并行进行（只要充分的配置控制就位），以尽可能早地发现和纠正错误；
b) 设计人员发布设计部件用于验证前，不应开展正式验证活动。一旦用于验证，则应在正式的配置控制下进行设计和相关文档的维护；
c) 用于验证的发布后，设计变更过程应确保所有对硬件设计的后续变更得以足够的验证（见 7.7 的要求）。

### 7.3 验证的独立性

7.3.1 对于1级硬件设计，验证者宜与硬件设计者在管理上独立，例如，两者可来自同一机构的不同部门或来自不同机构。对于2级系统，验证者不应是被验证项的设计者，但是，验证人员可以作为负责设计的个体来自同一机构。此外，还包括下列要求：

a) 验证人员在技术上应胜任；
b) 任何验证结果及设计对这些结果的响应应当正式形成文件；
c) 应按照文件程序进行验证。

7.3.2 对于2级硬件开发，当使用ATE验证其硬件的正确性时，则上述定义的详细的独立性要求适用于ATE的设计者，而不是使用ATE执行性能测试的监督人员。但是，对于所有1级硬件的开发，负责测试的（不管是否使用ATE）个体不能是硬件部件的设计者。

### 7.4 方法

硬件设计验证可采用关键性审查、审计、分析、手动测试或使用ATE测试、或上述方法的组合。验证方法的选择基础应形成充分详细的文件，使非直接参与设计或验证活动的人员能够进行审计。

a) 选择相应的验证方法时，应考虑下列相关问题：
   1) 系统的安全分级（即 1，2 级，对于 1 级要求最严格的技术）；
   2) 在集成的硬件和软件上进行的形成文件的审查和测试的活动将作为系统验证和确认（V&V）过程的一部分，即在硬件 V&V 过程中取消这些活动，以免由于重复工作造成资源的使用率不高；

3) 之前对硬件或包含硬件的系统所进行的验证活动（即，该设备已经过有效鉴定）；
4) 系统设计特点，例如规模、采用的设计原则的成熟度和（或）创新度、故障模式和复杂性；
5) 可从其他资源获取的支持数据，诸如从质量保证和环境鉴定过程获取的。

b) 应选用适当的工具和方法来支持子系统和电子部件的测试，以确保测试的充分性。适用时，宜采用 ATE 以提高测试的可重复性和充分性。
c) 当需要确认验证或测试过程中所使用的测试仪器的精度时，应对其标定，此时程序应保证只有标定过的仪器才能使用。
d) 基于软件的测试工具在使用前应予以确认，并应置于配置控制之下。

应记录所有正式测试的结果（非正式测试可在设计过程中作为正式测试的一个预测试进行）。应具有正式测试的可审计记录，以充分证明所有测试已被执行且任何测试异常已被成功解决。

## 7.5 文档

验证活动的可审计记录应包括测试大纲、测试程序、测试结果、设计变更记录和任何硬件验证过程中发现的不符合项文档（结合了说明每一个不符合项是如何消除的记录）。

测试程序应满足以下要求：

a) 测试程序宜书写清晰，为硬件验证提供一步一步的指导，并宜包括测试装置的详细信息；
b) 测试程序应包括明确的通过和（或）失败判据；
c) 通过软件执行的测试程序应形成文件。

## 7.6 不符合项

验证过程中所发现的不符合项应形成正式文件，并交给相关人员予以解决。应以正式文件作出响应，以提供一个可追溯的途径来确保对所有不符合项都进行了评价，并且任何识别出的设计不足已被修正或接受。一旦接受了设计不足，所有对系统文档的影响应全部论及。

## 7.7 变更和修改

7.7.1 所有设计变更应进行设计影响评估，以确定哪些文档要求修改和哪些设计和验证过程宜重做。
7.7.2 应按照相关的质量控制程序来确定修改部分。

## 7.8 安装验证

应按第10章的要求对系统的正确安装进行验证。

## 7.9 确认

应按NB/T 20026、NB/T 20054或NB/T 20055（如适用）的要求对集成硬件和软件进行系统确认。

## 7.10 现有设备平台的验证

当准备使用一个现有设备平台时，应评估该平台与预期应用的适合性。评估过程应考虑下列设计方面：

a) 用于硬件开发的设计过程，即按第 6 章相关的要求进行评估；
b) 使用经验（一旦实际的硬件可靠性数据能够确认硬件可靠性目标可实现，则可获得预期应用中该硬件性能的很大置信度）。支持要求的硬件可靠性目标的相关经验数据可用来抵消上述 a)中所发现的开发方法的偏差；

如果上述a)项不能提供足够的信息来证明硬件适合其预期应用，则可进行额外工作来支持评估，例如，测试、分析、证明材料。

## 8 鉴定

GB/T 12727规定了核安全应用中硬件鉴定的要求，其相关要求宜予以采用。见附录E给出的鉴定过程的资料性信息。

## 9 制造

计算机系统中使用的子系统、模块和部件，应按本标准的相关要求进行构建和评价。包括预开发产品（例如，COTS）和定制硬件产品。

## 10 安装和调试

10.1 包装、搬运、运输、储存和开箱应防止任何对系统的损坏。

10.2 在系统开箱和安装前，应验证系统所安装的环境满足5.4所给出的硬件环境要求。

10.3 应具备足够的程序和信息，能按照设计要求（例如，接地要求）对系统进行安装、敷设电缆和接线。设备物项标识应是信息的一部分。为此应有专用质量计划。系统应按照确定的程序进行安装、敷设电缆、测试和投运。

10.4 适当的现场系统工作应按NB/T 20026规定的已计划的和已规定的调试测试的要求进行检查。

10.5 试验应按照相关标准进行（如IEC 61000）。

10.6 电磁干扰试验的严酷等级应按相当或高于系统投运时所处的最差的预期情况的方法进行选择。

10.7 对于1和2级系统宜进行场外的抗电磁干扰型式试验。对于2级系统此类型式试验一般仅考虑能提供充分的正确运行保证；而对于1级系统，如果可行和有效，也宜进行现场试验。

10.8 当完成安装和调试，并且确认已满足了所有验收准则时（或特许），系统的所有权可移交给用户，见NB/T 20026的描述。

## 11 维护

### 11.1 概述

硬件维护包括：

——测试、检查和标定（可是在规定的最大期限内定期进行，或是部件更换、换件、大修或维修后进行（即再确认））；

——使计算机硬件保持良好运行状态所需要的维护，例如，耗材更换，或设备、子单元、部件或元件的预防性更换或大修；

——维修，即恢复故障设备、子单元和元件的可操性。

### 11.2 维护要求

11.2.1 应制定一个（或多个）正式程序并用于控制维护活动的执行和记录（参见附录F）。应考虑：

——要求有减少潜在错误引入和潜在人员伤害出现的预防性活动；

——如果维护活动对电厂运行，或安全功能或安全相关功能的可用性有潜在影响，则要求做好组织性和运行性准备。

11.2.2 应由有资质和授权的人员承担维护。应按照规定程序执行维护。该程序应对人员资质进行限制（通过人员授权，或通过自动测试），以使可能直接影响安全的各项任务都圆满完成。

应记录所有相关的信息，诸如时间和日期、合适的更换等。

11.2.3 维护工作所形成的记录应随时备查。

11.2.4 对于一些关键部件，可建立一套预防性维护体制，而不是仅当在出现故障时进行部件更换。在这种情况下，宜加以控制以保证部件在不长于其鉴定寿命内进行更换（如适用，见GB/T 12727）。

11.2.5 运行组织所经管的备品备件应在满足其仓储所有要求的任何环境条件下储存。必须根据硬件的老化特性及已储存的时间，对备品备件的储存寿命应加以必要的控制和修正。维持备品备件随时可用状态所需的任何活动都应予以关注，诸如定期通电。

11.2.6 备品备件宜按照运行部件鉴定所采用的等同的标准进行鉴定。任何降低1或2级系统部件鉴定要求，或延长该类部件鉴定寿命的建议，都宜视为一个系统修改来处理，并进行相应的评估。见第12章（按NB/T 20026的规定控制对系统的修改）。

11.2.7 所有备品备件应置于配置控制之下，并且应有恰当的识别标志或标签。

11.2.8 推荐备品备件的未来供应宜保证在切合实际的程度（例如，可通过备件持有、供货商的保证、或取得制造能力）。

## 11.3 故障数据

11.3.1 设备运行期间获取的故障数据是用来提高下列水平的主要信息来源：

——部件可靠性数据知识（通过考虑实际的运行环境条件）；

——设备可靠性评价（通过确定实际的现场错误故障和探查在运行条件下的可用性）；

——维护策略（通过更好的备品备件优化、更好的预防维护计划和更好的维护人员培训要求）。

11.3.2 相应的现场故障数据（来自维护报告中的可用信息）宜在故障数据库中记录。

11.3.3 维护报告应包括（相关的和已知的）：

——故障部件所处系统的标识；

——故障场景和故障影响；

——故障部件标识；

——部件在系统中的位置；

——引起故障的原因描述；

——故障引入日期；

——故障部件的寿命；

——起草报告的人员身份；

——诊断错误的人员身份。

11.3.4 应对安全重要系统的故障数据进行周期性检查，以确保部件故障的频度维持在可接受的限值内。宜对任何数据统计表明的有显著的恶化趋势进行实际程度推断，以确保该设备继续满意地运行，直到对该设备故障数据的下一次评估时，或是对设备可能被更换时（这里所指为最短周期）。

## 11.4 维护文档

11.4.1 应以程序、手册、指南等的书面或电子形式提供维护指导。

11.4.2 维护文件应描述在役设备硬件维护策略，包括要求定期检查、再标定或更换的硬件部件标识。

11.4.3 维护文件应描述任何宜用于探测特定模块故障的相关诊断过程。

11.4.4 文档应描述维修策略，即：

——维修或替换不同子系统、模块和部件的方法；

——系统在维修期间宜受到的任何限制（例如，应使系统或系统中的某些部分应停运）；

——设备维修后应进行再确认的程度。

除计划性定期维护程序外，还宜提供诊断程序，一旦相关和适用时，可用于支持异常系统运行行为的研究和识别出故障部件。

## 12 修改

12.1 可能要求对硬件设计进行修改以纠正有缺陷的性能，或关注新的或已修改的性能要求。

12.2 应按NB/T 20026—2010中6.3.6，控制硬件设计过程中的变更。

12.3 当硬件设计变更的影响超出某一独立设计阶段时（即，不包括在设计过程设计者所做出的任何变更）应由一个形成文件的程序对变更加以控制。这类设计变更程序宜考虑对系统设计其他方面的任何潜在影响，诸如其他硬件部件和软件。

12.4 设计变更程序应确保所有硬件变更对硬件和系统的验证、确认和鉴定过程的影响是确定的，并确保执行任何要求的返工。

## 13 运行

系统运行的相关要求见NB/T 20026（见NB/T 20054和NB/T 20055的相关补充信息）。

# 附 录 A
（资料性附录）
本标准与 IEC 60987:2007 相比的结构变化情况

本标准与IEC 60987:2007相比在结构上有较多调整，具体章条编号对照情况见表A.1。

表A.1 本标准与 IEC 60987:2007 的章条编号对照情况

| 本标准章条编号 | 对应的IEC 60987:2007章条编号 |
|---|---|
| — | 1.1 |
| 3.2 | 3.1、3.2、3.5、3.6 |
| 3.1.1 | 3.4 |
| — | 3.3 |
| - | 3.7 |
| 3.1.2～3.1.4 | 3.8～3.10 |
| — | 3.11、3.12 |
| 3.1.5～3.1.10 | 3.13～3.18 |
| 4.3.1 | — |
| 4.3.2～4.3.4 | 4.3.1～4.3.3 |
| 11.1 | — |
| 11.2 | 11.1 |
| 11.2.1～11.2.8 | 11.1.1～11.1.8 |
| 11.3 | 11.2 |
| 11.3.1～11.3.4 | 11.2.1～11.2.4 |
| 11.3 | 11.2 |
| 11.3.1～11.3.4 | 11.2.1～11.2.4 |
| 11.4 | 11.3 |
| 11.4.1～11.4.4 | 11.3.1～11.3.4 |
| 12.1 | — |
| 12.2～12.4 | 12.1～12.3 |
| 附录A | — |
| 附录B | 1.2 |
| 附录C | 1.3 |
| 附录D | 附录A |
| 附录E | 附录B |
| 附录F | 附录C |

# 附 录 B
（规范性附录）
预开发硬件的评估

尽管本标准的主要目的是关注新硬件的开发，但本标准所确定的过程同样可用于对预开发硬件的评价和使用提供指导，诸如，COTS硬件。当用于对这类部件进行评价时，相应的指导在本标准要求的相关解释中提供。特别是4.3的质量保证要求提到的配置控制、应用。

预开发部件可包括固件（见3.1.3的定义），如果固件的软件是嵌装的并且对用户实际上是“透明的”，则本标准应用于对这类部件的评价过程的指导。例如，考虑本标准规定的方法对含有微代码的处理器进行评价时是适用的。这类代码通常是“硬件”的一个完整的组成部分，因而使用本标准把处理器（包括微代码）评价为一个集成的硬件部件考虑是适用的。

如上所述，对于非固化软件，宜按相关的软件标准（例如，按用于1级系统的NB/T 20054和2级系统的NB/T 20055）进行开发和评价。

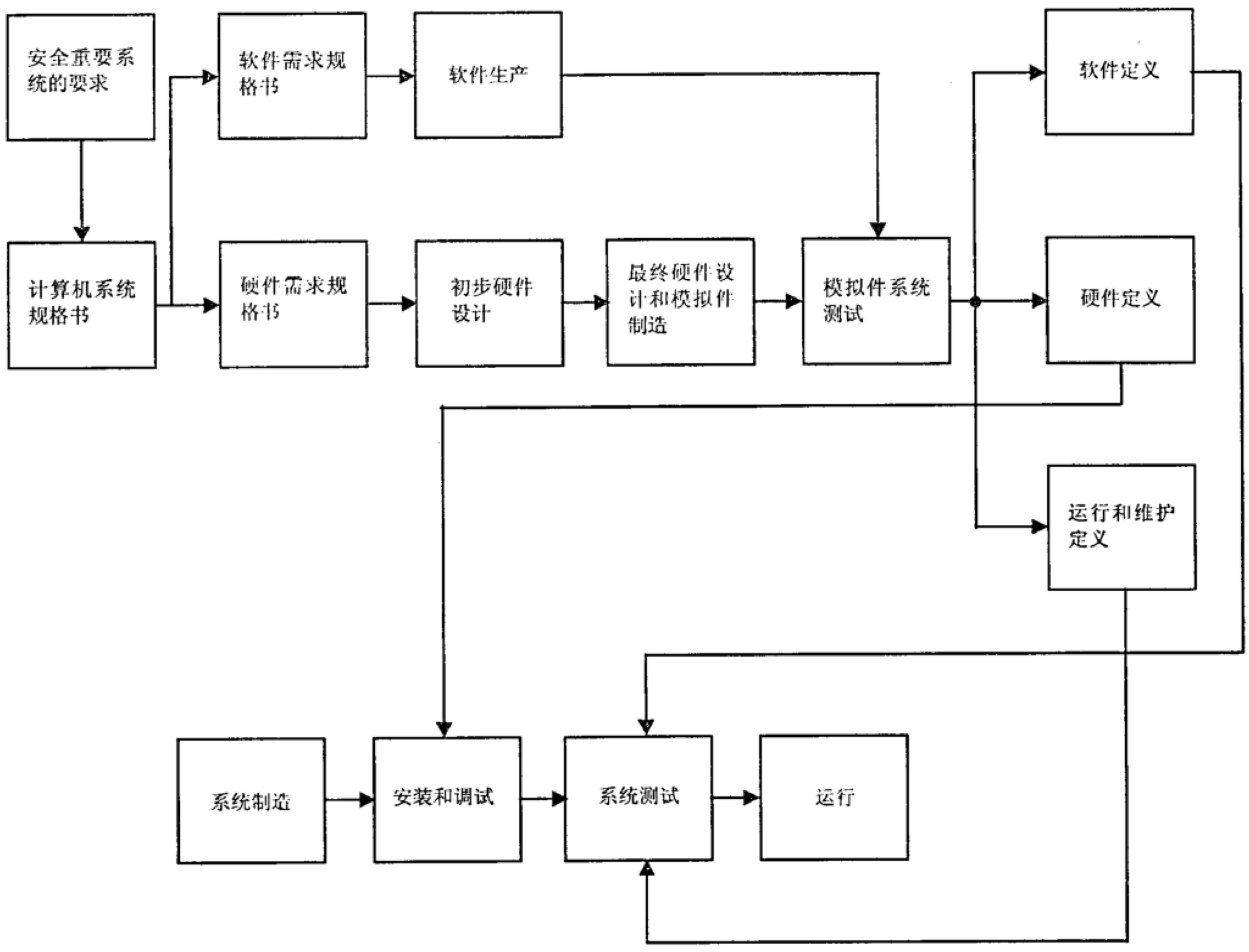
# 附 录 C
（规范性附录）
可编程逻辑器件开发的适用性

仪表和控制部件可包括可编程逻辑器件，相对于芯片制造商，仪表和控制部件的设计者赋予其特定的应用逻辑设计。这类器件如复杂的可编程逻辑器件（CPLD）和现场可编程门阵列（FPGA）。

当这类器件的可编程特性用于仪表和控制部件的开发过程时，则用于这类器件的软件开发过程和设计过程与用于离散门和集成电路包的逻辑电路设计实施非常相似。因此，用于可编程逻辑器件的设计过程和设计验证宜遵照本标准的有关要求（即，考虑这类器件设计过程的特点）。用于支持可编程逻辑器件设计过程的软件工具，一般宜遵照相应软件标准对软件开发工具提供的指导，见NB/T 20054（1级系统）或NB/T 20055（2级系统）。

# 附 录 D
（资料性附录）
系统生命周期总貌

系统生命周期见图D.1。

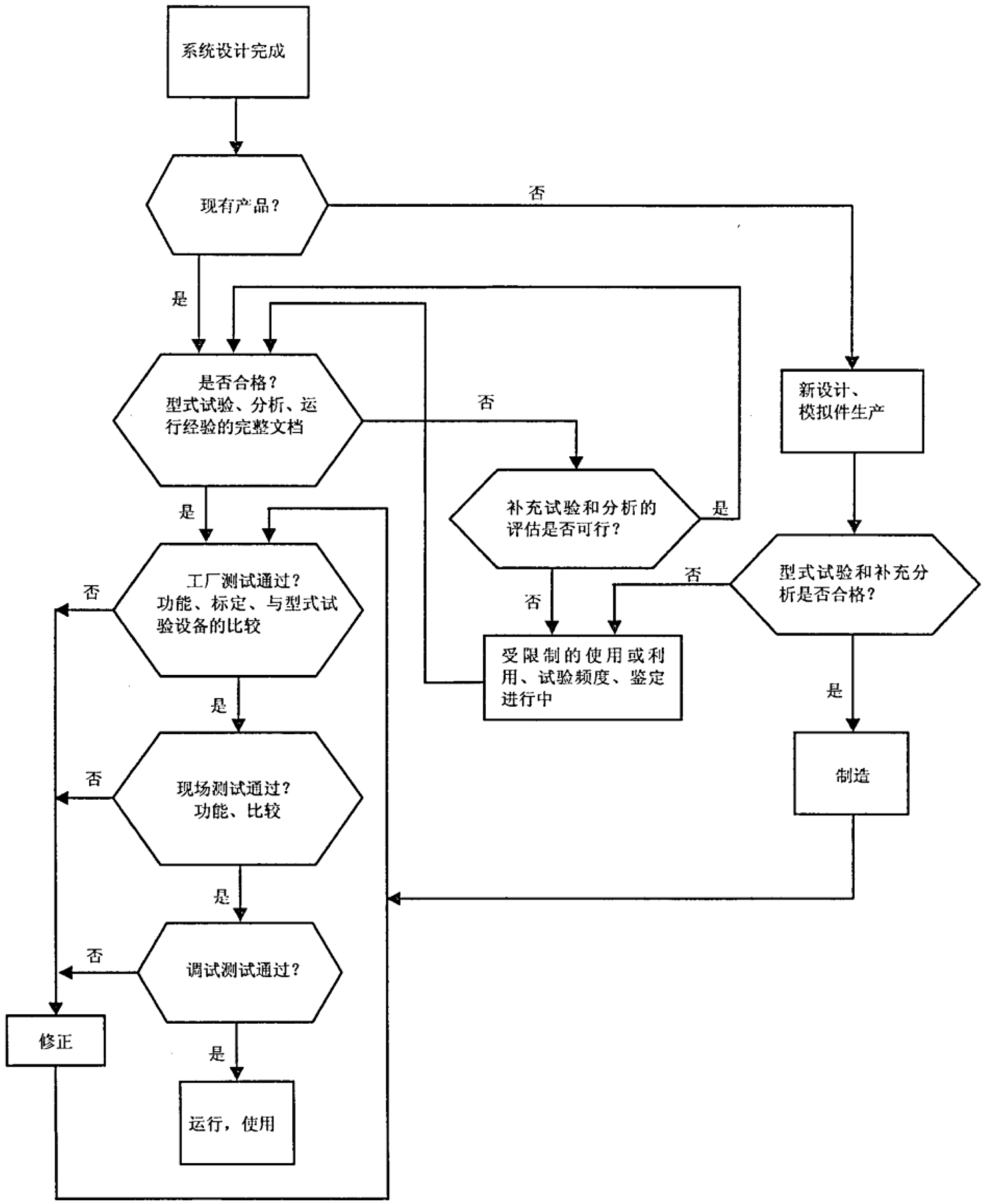



注：为清晰起见，未表示出反馈路径。

图D.1 系统生命周期

# 附 录 E
（资料性附录）
鉴定示意图

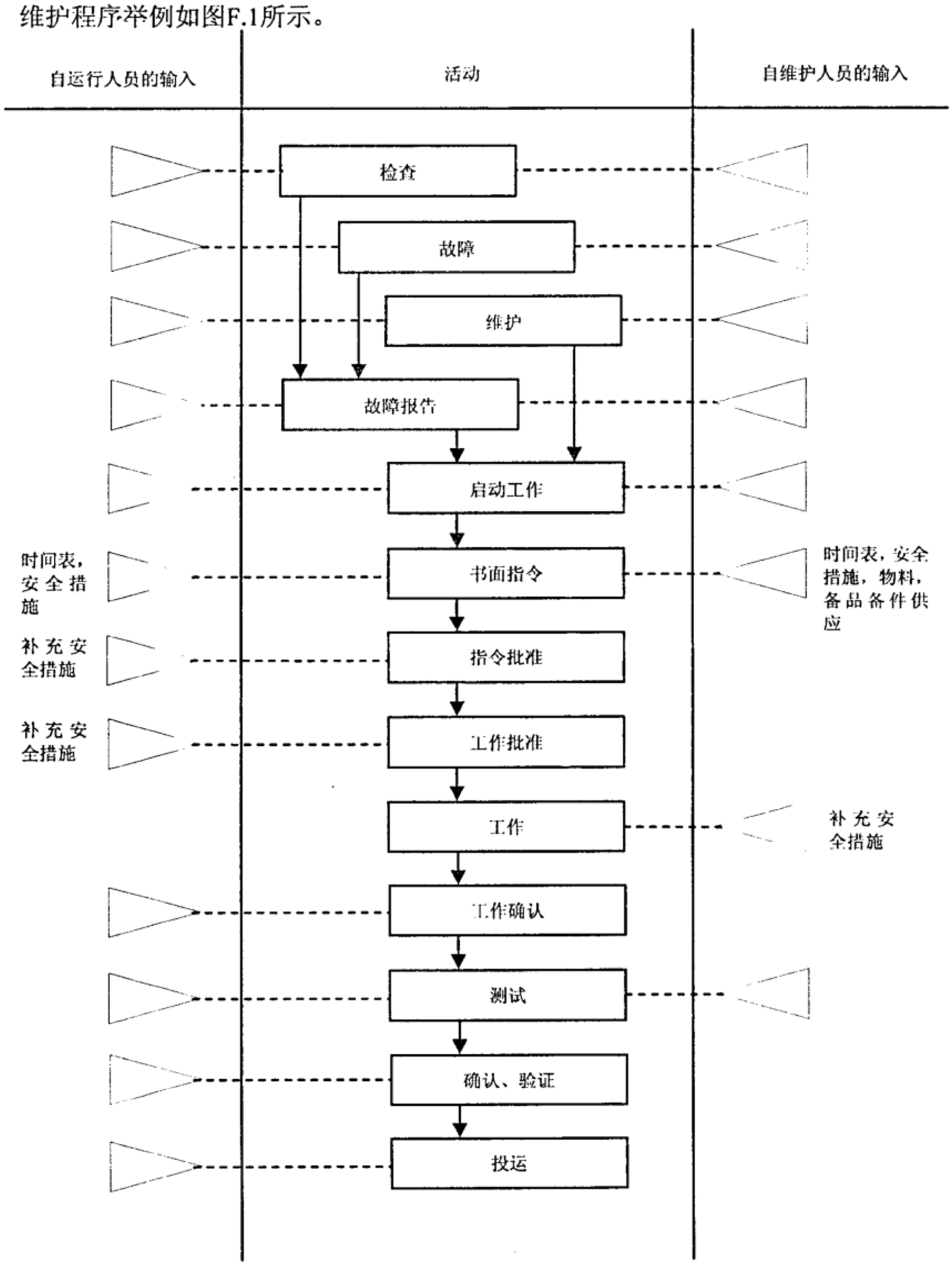
鉴定示意图见图E.1。




图E.1 鉴定示意图

# 附 录 F
（资料性附录）
维护程序举例

维护程序举例如图F.1所示。




图示说明：
表示与所示活动相关的人员。

图F.1 维护程序举例示意图

## 参 考 文 献

[1] GB/T 15474—1995 核电厂仪表和控制系统及其供电设备安全分级
[2] NB/T 20063—2012 核电厂仪表和控制术语
[3] ISO 12207 Information technology – Software life cycle process
[4] IAEA Safety Glossary:2006 Terminology Used in Nuclear Safety and Radiation Protection
[5] IAEA NS-R-1:2000 Safety of nuclear power plants: Design

中 华 人 民 共 和 国
能 源 行 业 标 准
核电厂安全重要数字仪表和控制系统
硬件设计要求
NB/T 20298—2014
*
核工业标准化研究所发行
北京海淀区骚子营 1 号院
邮政编码：100091
电话：010-62863505
机械信息研究院印制部印刷
**版权专有　侵权必究**
*
2014 年 11 月第 1 版　　2014 年 10 月第 1 次印刷
印数 1—200