ICS 27.120
F 64
备案号：26382-2009

DL

中华人民共和国电力行业标准

DL / T 1142 — 2009

核电厂反应堆控制系统软件测试

Software test for reactor control system of nuclear power plants

2009-07-22发布　　2009-12-01实施

中华人民共和国国家能源局　发布

目　次

前言 …… II
1　范围 …… 1
2　定义 …… 1
3　测试的总体要求 …… 2
4　安全性测试 …… 3
5　功能测试 …… 4
6　性能测试 …… 6
7　接口测试 …… 7
8　文档测试 …… 8
9　测试报告 …… 8
附录 A（规范性附录）　软件的基本要求 …… 10
附录 B（资料性附录）　测试用例的设计 …… 12

前　言

本标准是根据《国家发展改革委办公厅关于印发 2007 年行业标准项目计划的通知》（改办工业[2007] 1415 号）的要求安排制定的。

本标准的附录 A 是规范性附录，附录 B 是资料性附录。

本标准由中国电力企业联合会提出。

本标准由电力行业核电标准化技术委员会归口并解释。

本标准起草单位：中国广东核电集团苏州热工研究院有限公司。

本标准主要起草人：李蔚、吴帆、王峰。

本标准在执行过程中的意见或建议反馈至中国电力企业联合会标准化中心（北京市宣武区白广路二条一号，100761）。

核电厂反应堆控制系统软件测试

1 范围

本标准给出了核电厂反应堆控制系统软件测试的条件、基本过程、常用方法和不同阶段的测试要求。

本标准适用于压水堆核电厂反应堆控制系统软件在开发过程中各个阶段的测试。

其他堆型核电厂可以参照执行。

2 定义

下列术语和定义适用于本标准。

2.1

系统 system

a） 人、机器和方法的集合，用来实现一组规定的功能。

b） 一个完整的整体，由种类不同的、相互作用的、专门的结构和子功能部件所组成。

c） 由某些相互作用或相互依赖关系联合起来的小组或子系统，可执行多种职能，但是作为一个单位而发挥作用。

2.2

软件 software

相对于硬件的，与计算机系统的操作有关的计算机程序、规程和可能相关的文档。

2.3

测试用例 test case

a） 为具体的目标而编制的一组测试输入、执行条件以及预期结果。

b） 对于测试项，规定输入、预料的结果和一组执行条件的文档。

2.4

可靠性 reliability

在规定时间间隔和规定条件下，系统或部件执行所要求的功能的能力。

2.5

安全性 security

对系统或部件进行的保护，以防止其收到意外的或蓄意的存取、使用、修改、毁坏或泄密。

2.6

功能 function

系统或部件的定义的目标或特征动作。

注：本标准中的功能指反应堆控制系统的各项控制功能。

2.7

性能 performance

系统或部件在给定的约束，例如速度、精度或存储器使用条件下实现指定的功能的程度。

2.8

测试单元 test unit

一个或多个计算机程序模块与相关的控制数据（例如表格）、用法规程、操作规程一起的集合，这些集合满足下列条件：

a） 所有模块属于同一个计算机程序系统。

b） 集合中至少有一个模块（新的或改变过的模块）尚未完成单元测试。

c） 模块与相关的数据和规程是测试过程的唯一目标。

2.9

文档 document

一种数据媒体和其上所记录的数据。它具有永久性并可以由人或机器阅读。在软件工程中的例子里包括项目计划、规格说明书、测试计划、用户手册。

3 测试的总体要求

3.1 测试目的

3.1.1 确认软件可以在系统要求的硬/软件平台上工作正常。

3.1.2 确认软件能够满足全部操作要求，包括启动、从外部设备输入数据、程序输入、重新启动、在各种控制台上监督和控制该系统的操作。

3.1.3 确认软件达到需求说明和设计说明中规定的功能要求。

3.1.4 检测软件任务的执行和对系统运行产生的影响。

3.1.5 确认软件满足系统的性能需求，能够处理系统要求的负载。

3.1.6 软件应满足附录 A 的通用软件的基本要求。

3.1.7 检测软件的潜在缺陷。

3.2 测试的基本过程

3.2.1 软件测试过程至少应包括以下基本的测试活动：

a） 进行软件测试需求分析，拟定测试计划。

b） 编制软件测试大纲和软件测试技术规范书。

c） 设计和生成测试用例。

d） 实施测试。

e） 生成软件测试报告。

3.2.2 反应堆控制系统软件的测试过程应与整个软件开发过程平行进行。测试计划应在需求分析阶段开始制定，在测试阶段之前应进行测试大纲的制定、测试用例的生成、测试工具的选择和开发等相关工作。测试用例的设计参见附录 B。

3.2.3 软件测试大纲和软件测试技术规范书应明确规定在测试中针对系统的每一项功能或性能应完成的基本测试项目和测试评判依据。无论采用自动测试还是手动测试，都应满足测试大纲和技术规范书的要求。

3.2.4 软件测试应考虑在不同的开发设计阶段，软件的设计深度不同（例如模块级、子系统级、系统级），从而具有不同的测试要求并采用不同的测试方法，见 3.5 的规定。

3.3 测试条件

反应堆控制系统软件测试至少应满足以下条件后才能进行：

a） 对软件需求说明书、设计说明书的审查已经完成。

b） 制定相应的测试计划，并已经通过评审和批准，所有文档均得到有效控制。

c） 已做好测试的各项准备工作，包括设计适当的测试用例、选取合适的测试工具、成立相关的测试小组等。测试记录报告、纠正跟踪单已准备齐全。

d） 测试模拟台或试验平台的配置已先行验证、测试是可行的。

3.4 常用的测试方法

3.4.1 白盒测试

白盒测试也称为逻辑驱动测试，是针对程序代码进行正确性检验的测试，测试中发现的缺陷可以定

位到代码级。根据测试工具原理的不同，又分为静态白盒测试和动态白盒测试。

静态白盒测试直接对代码进行分析，不需要运行代码，也不需要对代码编译链接和生成可执行文件，一般是对代码进行语法扫描，找出代码中的错误或者不符合编码规范的地方。动态白盒测试则利用开发工具中的调试工具进行测试，一般采用“插桩”的方式，在代码生成的可执行文件中插入一些监测代码，用来统计程序运行时的数据。

3.4.2 黑盒测试

黑盒测试也称为数据驱动测试，是独立于程序代码，从用户的角度，通过一定的测试步骤和测试用例来验证软件功能、性能等指标满足需求的测试工作。在测试时，把程序看作一个不能打开的黑盒子，不应考虑程序内部结构和内部特性，只检查程序功能应满足软件需求说明书的规定，程序应能适当地接收输入数据而产生正确的输出信息，并且保持外部信息（如数据库或文件）的完整性。

注：白盒测试和黑盒测试的具体方法参见附录 B.3。

3.5 各阶段的测试要求

3.5.1 反应堆控制系统软件应依次进行单元测试、集成测试、系统测试和验收测试。

3.5.2 单元测试

单元测试贯穿于软件开发的整个过程，针对单个或相关联的程序单元进行测试，检验其正确性。单元测试集中在软件设计的最小单位——程序单元（或称程序模块）上，通过测试检验该单元的 I/O 条件和程序的逻辑结构。

单元测试主要完成对各程序模块的控制功能、正确性、一致性等的测试任务。单元测试可采用白盒法测试，应能达到彻底测试程序模块的逻辑结构；再辅之以黑盒法测试，使之对任何合理和不合理的输入都能正确鉴别和响应。

3.5.3 集成测试

集成测试是在单元测试的基础上，将所有程序模块按设计要求组装成系统或者子系统，对程序模块的组装过程和程序模块接口进行正确性检验。

集成测试主要针对结合起来的不同程序模块以及相互间接口，进行功能测试、接口测试、正确性测试、容错性测试、文档测试等任务，确定软件系统或各子系统达到设计要求。

3.5.4 系统测试

系统测试一般在开发过程的后阶段进行，要求软件设计和开发已经基本完成，并且已经进行和通过了软件的单元测试和集成测试。系统测试应包括测试整个软件系统的功能、质量和性能等方面的特性。

系统测试主要完成安全性测试、可靠性测试、性能测试、正确性测试、兼容性测试、文档测试等任务，宜采用黑盒法测试。

3.5.5 验收测试

验收测试是在整个开发过程的最终阶段进行的，测试整个软件系统应达到可以交付使用的状态。确定软件应符合需求说明书或设计说明书的要求。

验收测试是一种有效性测试或合格性测试，以用户为主，软件开发人员、实施人员、运行/维修人员和质量保证人员（或验收人员）共同参与。验收测试应以软件需求说明书、设计说明书和技术规范书为准，分别进行安全性测试、可靠性测试、功能测试、性能测试、接口测试、文档测试等全方位的测试。

4 安全性测试

4.1 综述

反应堆控制系统软件，首先应测试其满足整个核电厂对控制系统的安全与可靠性要求；其次，还应测试数字化控制系统（基于计算机的控制系统）满足软件的有关安全要求。

4.2 可靠性测试

4.2.1 测试时的使用环境应具有代表性，涉及软件系统运行时所需的各种支持要素，如硬件配置、操作

系统、输入数据格式和范围以及操作规程等。

4.2.2 可靠性测试应保证输入覆盖和环境覆盖，这是准确估计软件可靠性的基础。

4.2.3 在规定条件下和时间内软件应实现所需求的功能。

4.2.4 在规定条件下和时间内软件系统不应陷入用户无法控制的状态，既不应崩溃也不应丢失数据。

4.3 安全性测试

4.3.1 用户和密码封闭性。测试对用户名和密码的校验和保护措施，对密码应有屏蔽功能。

4.3.2 用户权限限制。测试用户权限应满足按功能模块划分的要求：仅使用规定的权限，任何人不得越权进行操作。

4.3.3 数据备份和恢复。测试软件的数据备份和恢复能力。应记录所有数据并存档，包括输入/输出数值、计算值、报警、事件等，面向用户提供备份和恢复手段。

4.3.4 异常情况的响应。异常情况包括：

a） 系统突然失电；

b） 硬件故障或切换；

c） 计算机死机。

测试发生异常情况时，系统的故障处理能力，如数据是否受损等。

4.3.5 网络故障影响。数字化控制系统是一个网络化的控制系统，应考虑网络故障对软件的安全影响。测试当网络故障或中断连接时，各层次软件应能保持正常运行，不应造成数据的丢失。

4.3.6 留痕功能，即可追溯性。测试软件应提供操作日志，包括每一个用户的登录时间、所有执行的操作动作、注销时间等，应对所有用户信息都能记录，并提供操作日志供查询。

4.3.7 诊断功能。反应堆控制系统软件应该不仅具有自诊断功能，还能实时监视硬件、传感器、执行器等的状态，进行故障诊断。

5 功能测试

5.1 综述

5.1.1 本章所提及的输入/输出不仅仅指实际的模块输入/输出点，也包括相对这些控制系统而言的输入/输出信号，如中间变量、函数计算值。

5.1.2 反应堆控制系统应实现使一回路产生的功率与二回路所吸收的功率相等，同时保证一、二回路的温度、压力等热工参数及堆功率分布等参数应满足机组安全运行要求的主要控制功能。

5.2 功率调节的功能测试

5.2.1 输入/输出测试。

通过加载信号发生器或利用 I/O 信号软接线等方法，测试所有功率量程范围内的输入/输出应达到设计要求。

输入主要有来自汽轮机控制系统的需求负荷信号、由棒组计数器实时给出的功率调节棒测量棒位等。输出主要有棒组逻辑升/降信号、频率与需求棒速成比例的脉冲信号等。

5.2.2 控制功能测试。

利用 I/O 软连接创建模拟测试环境，或通过动态调试（单步执行、断点操作等）的方法，分别测试稳态运行和瞬态运行工况下的功率调节功能，应能够实现使反应堆的功率迅速跟踪二回路的功率，使电站具有参与电网调峰、快速跟踪负荷变化的控制功能。

5.2.3 根据设计说明书的具体要求进行功率调节功能的其他测试项。

5.3 平均温度调节的功能测试

5.3.1 输入/输出测试。

通过加载信号发生器或利用 I/O 信号软接线等方法，测试所有功率量程范围内的输入/输出值应符合设计要求。

输入主要有反应堆冷却剂平均温度测量值、反应堆功率的中子注量率测量值等。输出主要有反应堆冷却剂平均温度设定值、控制棒的棒速设定值等。

5.3.2 控制功能测试。

利用 I/O 软连接创建模拟测试环境，或通过动态调试（单步执行、断点操作等）的方法，分别测试稳态运行和瞬态运行工况下的温度调节功能，应能够实现通过调节温度调节棒在堆芯的位置来保持一回路的平均温度，尽可能接近由负荷决定的整定值，以满足二次侧负荷变化的控制功能。

5.3.3 根据设计说明书的具体要求进行平均温度调节功能的其他测试项。

5.4 稳压器压力控制的功能测试

5.4.1 输入/输出测试。

通过加载信号发生器或利用 I/O 信号软接线等方法，测试所有功率量程范围内的输入/输出应达到设计要求。

输入主要有稳压器压力定值、稳压器压力测量值等。输出主要有压力调节器输出信号、喷雾阀极化控制信号。

5.4.2 控制功能测试。

利用 I/O 软连接创建模拟测试环境，或通过动态调试（单步执行、断点操作等）的方法，分别测试稳态运行和瞬态运行工况下的稳压器压力调节功能，应能够实现使反应堆一回路系统保持正常运行压力的控制功能。

5.4.3 根据设计说明书的具体要求进行稳压器压力控制功能的其他测试项。

5.5 稳压器水位控制的功能测试

5.5.1 输入/输出测试。

通过加载信号发生器或利用 I/O 信号软接线等方法，测试所有功率量程范围内的输入/输出应达到设计要求。

输入主要有稳压器水位测量值、反应堆冷却剂温度等。输出主要有流量设定值、稳压器水位设定值等。

5.5.2 控制功能测试。

利用 I/O 软连接创建模拟测试环境，或通过动态调试（单步执行、断点操作等）的方法，分别测试稳态运行和瞬态运行工况下的稳压器水位调节功能，应能够实现使稳压器水位保持在预定的程序值上的控制功能。

5.5.3 根据设计说明书的具体要求进行稳压器水位控制功能的其他测试项。

5.6 蒸汽排放控制的功能测试

5.6.1 输入/输出测试。

通过加载信号发生器或利用 I/O 信号软接线等方法，测试所有功率量程范围内的输入/输出应达到设计要求。

输入主要有蒸汽母管压力、蒸汽发生器压力、汽轮机入口压力等。输出主要有蒸汽排放阀开启信号、排放阀工作模式（调节开启或快开）信号、二回路压力设定值等。

5.6.2 控制功能测试。

利用 I/O 软连接创建模拟测试环境，或通过动态调试（单步执行、断点操作等）的方法，分别测试稳态运行和瞬态运行工况下的蒸汽排放控制功能，应能够实现将主蒸汽直接排放到主凝汽器和除氧器或者大气，降低由汽轮机负荷衰降引起的核蒸汽供应系统温度与压力变化的幅度的控制功能。

5.6.3 根据设计说明书的具体要求进行蒸汽排放控制功能的其他测试项。

5.7 蒸汽发生器水位控制的功能测试

5.7.1 输入/输出测试。

通过加载信号发生器或利用 I/O 信号软接线等方法，测试所有功率量程范围内的输入/输出应达到设

计要求。

输入主要有蒸汽发生器水位测量值、蒸汽流量、给水流量和温度、给水母管和蒸汽母管之间的差压等。输出主要有蒸汽发生器调节阀的开启和开度信号、给水流量需求信号、主给水泵速度控制信号等。

5.7.2 控制功能测试。

利用 I/O 软连接创建模拟测试环境，或通过动态调试（单步执行、断点操作等）的方法，分别测试稳态运行和瞬态运行工况下的蒸发器水位调节功能，应能够实现维持蒸发器相应水位的控制功能。

5.7.3 根据设计说明书的具体要求进行蒸汽发生器水位控制功能的其他测试项。

6 性能测试

6.1 负载性能测试

负载性能是指各种工作负载下软件系统的性能，通常用来度量系统的可扩展性。可以通过测试当负载逐渐增加时系统各组成部分的响应输出项，如通过率、响应时间、CPU 负载、内存使用等情况，通过综合分析来决定系统的性能。

6.2 压力性能测试

压力性能是指在软件系统稳定运行情况下，能够处理的最大工作量强度或提供的最大服务性能。可以通过测试临界负载、容量变化、资源占用等指标，综合分析功能执行情况和系统性能表现，并确定一个系统的瓶颈或者不能接受的性能点，从而获得最大工作量强度或最大服务性能。

6.3 容错性能测试

6.3.1 反应堆控制系统软件容错性能应至少满足：

a） 采用计算机的控制系统，应具有双机备份，人为退出工作主机，备用主机应能自动投入工作。

b） 在双机切换过程中，控制系统应保持正常工作，维持机组的正常运行。

c） 重要参数的检测元件应为符合逻辑所需的冗余配置，采用去掉一个测量元件信号或在一个测量元件输出端改变信号的方式，检查其冗余的可靠性。

6.3.2 容错性能测试应包括：

a） 键盘操作的容错测试。在操作员站的键盘上操作任何错误的键或未经定义的键时，系统不得出错或出现死机情况，应视为不允许的输入，不加处理。

b） 控制单元切换时的容错测试。人为退出控制站中正在运行的控制单元，这时备用的控制单元应自动投入工作，在控制单元的切换过程中，系统不得出错或出现死机情况。

c） 通信总线冗余切换能力的测试。在任意节点人为切断每条通信总线，系统不得出错或出现死机情况。切、投通信总线上的任意节点，或模拟其故障，总线通信应正常。

6.4 重置性能测试

重置性能是指在出现电源跳闸或者切换、硬件故障或者切换、网络故障等情况下，整个系统保持正常运行的能力，或是迅速恢复正常运行的能力。当切除并恢复系统的外围设备时，反应堆控制系统软件不得出现任何异常情况。

6.5 实时性能测试

6.5.1 显示画面响应时间的测试

通过键盘调用显示画面时，从最后一个调用操作完成到画面全部内容显示完成所用的时间为画面响应时间。画面响应时间规定如下：

a） 在调用被测画面时，对一般画面，响应时间不得超过 1s；对于复杂画面，画面响应时间不得超过 2s。

b） 在发生中断时，显示画面自动退出的时间也应符合上述的规定。

6.5.2 系统响应时间的测试

将系统输出的开关量操作信号直接引到该操作对象反馈信号的输入端。测量通过操作台的键盘发出操作指令，直到屏幕上显示反馈信号之间的时间，操作信号响应时间应为 2.0s～2.5s，或技术说明书中

规定的时间。

6.5.3 模拟量信号采集实时性的测试

测试时应按不同采样周期各选 3 个～6 个测点进行测试。

6.5.4 开关量信号采集实时性的测试

选择 3 个～5 个开关量输入通道，接入测试用开关量信号，使之按设计的开关量采样周期改变状态。通过画面状态显示或开关量状态记录，检查开关量信号采集的实时性。

6.5.5 事件顺序记录分辨力的测试

利用一台开关量信号发生器进行测试，信号发生器应能送出间隔时间可在 1ms～5ms 之间调节的 3 个～5 个开关量信号。将信号发生器的信号接入事件顺序记录的输入端，改变信号发生器的间隔时间，直至事件顺序记录无法分辨时为止，即为事件顺序记录的分辨力。分辨力应为 1ms～2ms，或技术说明书中规定的时间。

6.5.6 控制器处理周期的测试

分别选择模拟量控制器和开关量控制器测试处理周期。

6.6 抗干扰性能测试

抗干扰性能是指软件程序抵抗外部干扰的能力。反应堆控制系统软件应具有良好的抗干扰能力，为抵抗干扰而增加的防卫措施应不仅能够抵抗干扰，并且对软件原有性能没有影响或者影响不大，即不影响软件的正常运行。

6.7 可用率测试

软件可用率是指在需要软件投入使用时，能实现其指定功能的能力。反应堆控制系统软件可用率的测试与整个控制系统可用率的测试一起进行。

7 接口测试

7.1 基本要求

软件的接口应符合数据传输机制和接口间协议的要求，接口通常包括：

a） 软件之间的接口，与用户其他系统或软件的接口。

b） 人机接口，即人机界面。

c） 与外部设备的接口，包括与计算机硬件的接口。

7.2 软件之间的接口测试

软件之间的接口包括软件本身内部各个程序单元之间的接口，与其他软件（如操作系统、数据管理、专用计算包等）的接口，以及与用户其他系统的接口。

a） 测试数据穿过接口时不应丢失或失真。

b） 测试程序单元之间不应由于疏忽而造成有害影响。

c） 测试子功能组合起来应产生预期的主功能。

d） 测试全程数据库不应有错。

e） 测试接口信息的内容和格式。

f） 测试不同软件之间不应存在冲突。

7.3 人机接口测试

7.3.1 工作站

a） 工程师站基本操作的测试。

b） 操作员站基本操作的测试。

c） 工程师站和操作员站之间的闭锁和保护的测试。

7.3.2 显示

显示画面包括流程图、参数图、实时趋势图、历史趋势图、棒形图和报警显示等。

a） 测试显示画面的种类及数量，应与原设计相符。

b） 测试显示画面的更新频率和画面更新数据量。

c） 测试显示分区的划分及其使用方法。

7.4 与硬件的接口测试

软件产品与硬件设备是紧密联系的，尤其在反应堆控制系统中，只有软硬件协调工作才能实现对反应堆的控制功能，满足安全的要求。

a） 测试所有与软件接口的设备。

b） 测试软件与硬件之间的配置特性，如端口的数目、指令装置等。

c） 测试软件与硬件之间的通信方式和协议。

8 文档测试

8.1 测试内容

进行文档测试时，应主要考虑以下方面：

a） 明确文档验收的标准，软件开发人员和用户应对此达成一致。

b） 确定文档的重要性和项目文档需求，在软件开发的不同阶段，各类文档的重要性有不同。

c） 检验文档完整性，主要是文档的种类和内容的完整性。

d） 检验文档的一致性和可追溯性，包括：

1） 软件的设计描述应按照需求定义进行。

2） 应用程序应与设计文档的描述一致。

3） 用户文档应客观描述应用程序的实际操作。

4） 关于同一问题的描述不应存在不同的说法。

e） 检验文档的准确性，主要是文档描述应准确无歧义，文字表达不应存在错误。

f） 检验文档的可理解性，主要审核文档应针对指定的用户，表达应易于理解并且详细。

g） 检验文档的易浏览性，主要审核文档应易于浏览，各类文档之间的相互关系应明确；每个文档都应有目录表和/或索引表。

8.2 文档的种类

反应堆控制系统软件的文档应包括：

a） 软件程序，包含系统软件程序和应用软件程序，主要有可执行程序、源程序、配置脚本、测试程序或脚本等。

b） 开发类文档，主要有《技术规范书》、《需求说明书》、《概要设计说明书》、《详细设计说明书》、《测试计划》、《程序维护手册》、《用户手册》、《联机帮助文件》、《数据库说明》等。

c） 管理类文档，主要有《项目计划书》、《质量保证和控制计划》、《配置管理计划》、《用户培训计划》、《质量总结报告》、《评审报告》、《开发进度报告》、《项目总结报告》等。

9 测试报告

反应堆控制系统软件的测试活动和测试结果应汇总在测试报告中。测试报告可采用以下结构：

a） 测试报告名称。

b） 概述。

1） 简述测试活动。

2） 被测试项及其版本/修订级别。

3） 测试环境（主要指测试用的计算机系统软硬件配置）。

4） 所参照的技术规范书或设计说明书及其版本。

c） 测试活动描述。

1） 测试日期和时间。
2） 测试数据（测试用例）。
3） 预期结果。
4） 实际结果。
5） 异常现象。
6） 测试参与人员。

d） 评价。
1） 测试评价：以测试结果和测试项的通过准则为依据，对每个测试项进行总的评价。
2） 差异评价：报告测试项与技术规范书或设计说明书之间的差别，指出测试活动与测试计划之间的差别，并说明原因。

e） 总结。
1） 测试活动的总结，指出测试活动的作用和意义。
2） 测试结果的总结，说明所有已解决的问题及其解决方法，指出尚未解决的问题。
3） 意见和建议。

附 录 A
（规范性附录）
软件的基本要求

A.1 完整性

a） 用户文档应包含产品使用所需信息。
b） 如果安装能由用户来完成，则用户文档应包括安装手册，其中包含所有必要的信息。
c） 如果维护能由用户来完成，则用户文档应包括程序维护手册，其中包含各种维护该软件所需要的信息。

A.2 一致性

a） 用户文档、程序和数据本身内容不能自相矛盾，相互之间也不应矛盾。
b） 每个术语的含义宜处处保持一致。
c） 由用户行使的软件操作和行为（如消息，屏幕输入格式和打印报表）宜有一致的结构。

A.3 正确性

a） 用户文档中的所有信息应是正确的，不能有歧义和错误的表达。
b） 程序和数据应与用户文档中的全部说明相对应。
c） 程序功能应以正确的方式执行。

A.4 易用性

a） 软件应方便用户学习和操作。
b） 软件应方便输入信息和输出结果。

A.5 易理解性

a） 软件的功能目标、程序结构和操作要求应是易理解的，如通过使用适当的术语、图形表示、详细的解释以及引用有用的信息源来表现。
b） 出错消息应提供解释相应差错产生的原因和纠正的详细信息。

A.6 易浏览性

a） 用户文档应易于浏览，以便相互关系明确。
b） 软件程序宜以易观察易读的形式向用户提供信息，并通过对信息的编码和分组对用户提供指导。
c） 屏幕输入格式，报表和其他输入/输出宜设计清晰和易于浏览。

A.7 实时性

a） 软件应能在由外界要求所确定的时间内对数据进行处理。
b） 可通过软件的时间特性来判断实时性，即在规定的边界条件下，执行某一任务的指定功能所需要的时间，或因这些功能调用资源所需要的时间，例如响应时间和吞吐率等参数。

A.8 开放性和可扩展性

a） 软件应能在不同规模、不同档次的运行环境平台上进行正常运行。

b） 软件系统或程序在增加新项目的条件下，应能保持原系统基本结构不变并且保持正常运行。

A.9 可维护性

a） 软件应能按照预定的要求对某一功能组件进行修改或维护。修改包括为了适应环境的变化以及功能规格说明的变化而对软件进行的修改、改进或更改。

b） 软件的可维护性确定了对软件进行维护的容易程度，包括对软件内模块、模块间接口、软件间接口等的维护。

A.10 可追溯性

软件程序应能建立前后阶段的联系，具有为用户提供追踪查询的能力。追溯的内容包括：

a） 过程变量。

b） 开关量变态，模拟量变化。

c） 机组启、停参数。

d） 参数越限。

e） 事件、事故追忆。

附 录 B
（资料性附录）
测试用例的设计

B.1 设计的基本准则

a） 测试用例的代表性：应能代表各种合理和不合理的、合法和非法的、边界和越界的，以及极限的输入数据、操作和环境设置等。
b） 测试结果的可判定性：测试执行结果的正确性应是可判定的或可评估的。
c） 测试结果的可再现性：对同样的测试用例，系统的执行结果应是相同的。

B.2 基本的编制方法

编写测试用例文档。编写测试用例文档应有文档模板，须符合内部的规范要求。测试用例文档由简介和测试用例两部分组成。简介部分应包括测试目的、测试范围、定义术语、参考文档、概述等。测试用例部分则逐一列示各测试用例，每个具体测试用例都应包括下列详细信息：用例编号、用例名称、测试等级、入口准则、验证步骤、期望结果（含判断标准）、出口准则、注释等。

设置测试用例。常见的设置有按功能设置和按路径设置。按功能测试是最简捷的，即按测试用例的规约遍测每一功能。但对于复杂操作的程序模块，各功能的实施是相互影响、紧密相关的，没有严密的逻辑分析，产生遗漏在所难免。因此，最好结合路径分析方法，以避免漏测试。

测试用例可以分为基本事件、备选事件和异常事件。设计基本事件的用例，应该参照用例规约（或设计说明书），根据关联的功能、操作按路径分析法设计测试用例。而对孤立的功能则直接按功能设计测试用例。基本事件的测试用例应包含所有需要实现的需求功能，覆盖率达 100%。而设计备选事件和异常事件的用例，则相对复杂和困难得多，可以采用软件测试常用的基本方法来设计完整的测试用例。

B.3 常用的设计方法

B.3.1 白盒技术

B.3.1.1 逻辑覆盖方法

逻辑覆盖方法是指程序内部的逻辑覆盖程度。当程序中有循环时，覆盖每条路径是不可能的，设计的测试用例要使覆盖的程度较高或是覆盖最有代表性的路径。

a） 语句覆盖：为了提高发现错误的可能性，在测试时应该执行到程序中的每一条语句。语句覆盖是指设计足够的测试用例，使被测试程序中每条语句至少执行 1 次。
b） 判定覆盖：设计足够的测试用例，使得被测程序中每个判定表达式至少获得 1 次“真”值和“假”值，从而使程序的每一个分支至少都通过 1 次，因此判定覆盖也称分支覆盖。
c） 条件覆盖：设计足够的测试用例，使得判定表达式中每个条件的各种可能的值至少出现 1 次。
d） 判定/条件测试：设计足够的测试用例，使得判定表达式的每个条件的所有可能取值至少出现 1 次，并使每个判定表达式所有可能的结果也至少出现 1 次。
e） 条件组合覆盖：比较强的覆盖标准，设计足够的测试用例，使得每个判定表达式中条件的各种可能的值的组合都至少出现 1 次。
f） 路径覆盖：设计足够的测试用例，覆盖被测程序中所有可能的路径。在实际的逻辑覆盖测试中，一般以条件组合覆盖为主设计测试用例，然后再补充部分用例，以达到路径覆盖测试标准。

B.3.1.2 循环覆盖方法

B.3.1.3 基本路径测试方法

B.3.2 黑盒技术

B.3.2.1 等价类划分方法

等价类划分方法是把所有可能的输入数据，即程序的输入域划分成若干部分（子集），然后从每一个子集中选取少数具有代表性的数据作为测试用例。该方法是一种重要的常用黑盒测试用例设计方法。

首先，要划分等价类。等价类是指某个输入域的子集合。在该子集合中，各个输入数据对于揭露程序中的错误都是等效的，并合理地假定：测试某等价类的代表值就等于对这一类其他值的测试。因此，可以把全部输入数据合理划分为若干等价类，在每一个等价类中取一个数据作为测试的输入条件，就可以用少量代表性的测试数据，而取得较好的测试结果。

等价类划分可有两种不同的情况：

a） 有效等价类：是指对于程序的规格说明来说是合理的，有意义的输入数据构成的集合。利用有效等价类可检验程序是否实现了规格说明中所规定的功能和性能。

b） 无效等价类：与有效等价类的定义恰巧相反。

设计测试用例时，要同时考虑这两种等价类。因为软件不仅要能接收合理的数据，也要能经受意外的考验，这样的测试才能确保软件具有更高的可靠性。

划分等价类基本遵循以下原则：

a） 如果输入条件规定了取值范围或值的个数，则可确定一个有效等价类（输入值或数在此范围内）和两个无效等价类（输入值或个数小于这个范围的最小值或大于这个范围的最大值）。

b） 如果输入条件规定了输入值的集合或规定了“必须如何”的条件，则可确定一个有效等价类和一个无效等价类。

c） 如果输入条件是一个布尔量，则可确定一个有效等价类和一个无效等价类。

d） 如果规定了输入数据的一组值（假定 n 个），而且程序对不同的输入值做不同的处理，则每个允许输入值是一个有效等价类即可确立 n 个有效等价类和一个无效等价类（任何一个不允许的输入值）。

e） 如果规定了输入数据必须遵循的规则，可确定一个有效等价类（符合规则）和若干个无效等价类（从各种不同角度违反规则）。

f） 如果已划分的等价类中各元素在程序中的处理方式不同，则应将该等价类进一步划分为更小的等价类。

其次，要确定测试用例。在确立了等价类后，可建立等价类表，列出所有划分出的等价类。然后从划分出的等价类中设计测试用例。

a） 为每一个等价类规定一个唯一的编号。

b） 设计一个测试用例，使其尽可能多地覆盖尚未被覆盖过的有效等价类。重复此步，直到所有的有效等价类都被覆盖为止。

c） 设计一个测试用例，使其仅覆盖一个尚未被覆盖的无效等价类。重复此步，直到所有的无效等价类都被覆盖为止。

B.3.2.2 边界值分析方法

边界值分析方法是对等价类划分方法的补充，通常与等价类划分结合起来设计测试用例。使用边界值分析方法时，首先应确定边界情况，通常输入和输出等价类的边界，就是应着重测试的边界情况。应当选取正好等于、刚刚大于或刚刚小于边界的值作为测试数据，而不是选取等价类中的典型值或任意值作为测试数据。

运用边界值分析方法设计测试用例应遵循以下原则：

a） 如果输入条件规定了值的范围，可以选择正好等于边界值的数据作为有效的测试用例，同时还

要选择刚好越过边界值的数据作为无效的测试用例。

b） 如果输入条件规定了值的个数，则按最大个数、最小个数、比最小个数少 1、比最大个数多 1 等情况分别设计测试用例。

c） 对每个输出条件分别按照以上两个原则确定输出值的边界情况。

d） 如果程序的规格说明给出的输入域或输出域是个有序集合，则应选取集合的第一个元素和最后一个元素作为测试用例。

e） 分析规格说明，找出其他可能的边界条件。

B.3.2.3 错误推测方法

在测试程序时，可以根据经验或直觉推测程序中所有可能存在的各种错误，从而有针对性地设计测试用例的方法。

错误推测方法的基本思想就是列举出程序中所有可能存在的错误和容易发生错误的特殊情况，根据这些情况选择测试用例。

B.3.2.4 因果图方法

等价类划分和边界值分析的缺点是没有检查各种输入条件的组合，而因果图是一种适合于描述对于多种输入条件的组合而相应产生多个动作的设计方法。借助因果图列出输入条件的各种组合与程序对应动作结果之间的阶段联系，构造判定表，是生成测试用例的有效办法。

运用因果图方法生成测试用例的步骤如下：

a） 分析设计说明书（或技术规范书）中的原因（输入条件或者输入条件等价类）、结果（输出可能性），对每个原因/结果进行编号。

b） 找出原因/结果之间、原因/原因之间的对应关系，画出因果图。

c） 在因果图上用一些记号表明约束或限制条件，将因果图转换为判定表。

d） 对判定表中每一列生成测试用例。

B.3.2.5 综合策略方法

每种方法都能设计出一组有用的测试用例，用这组测试用例可能很容易发现某种类型的错误，但不易发现另一类型的错误。因此，在实际测试中，应该联合使用各种测试方法，形成综合策略。通常是先用黑盒法设计基本的测试用例，再用白盒法补充一些必要的测试用例。

B.4 测试用例的作用

B.4.1 指导软件测试的实施

测试用例主要适用于集成测试、系统测试。在实施测试时测试用例作为软件测试的标准，测试人员一定要严格按照测试用例的测试项目和测试步骤逐一实施测试，并将测试情况记录在测试用例管理软件中，以便自动生成测试结果文档。

B.4.2 规划测试数据的准备

按照测试用例配套准备一组或若干组测试原始数据，以及标准测试结果。除了正常数据之外，还必须根据测试用例设计大量边缘数据和错误数据。

B.4.3 评估测试结果的度量基准

完成软件测试后需要对测试结果进行评估，并且编制测试报告。判断软件测试是否完成，衡量测试质量需要有量化的结果，如测试覆盖率是多少、测试合格率是多少、重要测试合格率是多少等。采用测试用例作度量基准将更加准确、有效。

B.4.4 分析缺陷的标准

通过收集缺陷，对比测试用例和缺陷数据库，分析确证是漏测还是缺陷复现。漏测反映了测试用例的不完善，应立即补充相应测试用例，最终达到逐步完善软件质量的目的。如果已有相应的测试用例，则反映实施测试或变更处理存在问题。

B.5 其他要求

B.5.1 测试用例的评审

测试用例是软件测试的准则，但并不是一经编制完成就能成为准则的。测试用例在设计编制过程中要组织同级互查。完成编制后应组织专家评审，需获得通过才可以使用。评审委员会可由项目负责人、测试、编程、分析设计等有关人员组成，也可邀请用户代表参加。

B.5.2 测试用例的修改更新

测试用例在形成文档后还需要不断完善，主要来自三方面的原因：

a） 在测试过程中发现设计测试用例时考虑不周，需要完善。

b） 在软件交付使用后反馈的软件缺陷是由于测试用例存在漏洞而造成的。

c） 软件自身的新增功能以及版本的更新，测试用例也必须配套修改更新。

B.5.3 测试用例的管理软件

运用测试用例还需配备测试用例管理软件，主要功能有：

a） 能将测试用例文档的关键内容，如编号、名称等自动导入管理数据库，形成与测试用例文档完全对应的记录。

b） 可供测试实施时及时输入测试情况。

c） 最终实现自动生成测试结果文档，包含各测试度量值、测试覆盖表、测试通过或不通过的测试用例清单列表。

中 华 人 民 共 和 国
电 力 行 业 标 准
核电厂反应堆控制系统软件测试
DL / T 1142 — 2009
*
中国电力出版社出版、发行
（北京三里河路 6 号 100044 http://www.cepp.com.cn）
北京博图彩色印刷有限公司印刷
*
2009 年 12 月第一版 2009 年 12 月北京第一次印刷
880 毫米×1230 毫米 16 开本 1.25 印张 31 千字
印数 0001—3000 册
*
统一书号 155083 • 2265

155083.2265
销售分类建议：规程规范/
电力工程/新能源发电