2019年11月

信息系统项目管理师

辅导班课程

马军老师

23.1 测试基础

23.1.1 软件测试模型

1、软件开发的主要模型有瀑布模型、原型模型、螺旋模型、增量模型以及Rational统一过程(RUP)模型等

2、软件测试过程的主要模型有以下几种（1）V模型（2）W模型（3） H模型（4）X模型（5）前置测试模型。

3、V模型存在一定的局限性,其优缺点如图所示。它将测试过程作为在需求分析、概要设计、详细设计及编码之后的一个阶段，这样会导致需求分析或系统设计阶段隐藏的问题一直到后期的验收测试时才被发现，当在最后验收测试中发现这些需求错误时，可能已经很难再更改程序的逻辑结构去修正问题，从而导致项目的失败。等到软件编码完成后才开始软件测试工作，那么必须在代码完成后给测试工作预留足够的时间，否则将导致测试不充分，并且开发前期未发现的错误可能会传递并扩散到后面的测试阶段才被发现。

4、V模型失败的原因是它把系统开发过程划分为具有固定边界的不同阶段，导致测试人员很难跨过这些边界来采集测试所需要的信息，并且也阻碍了测试人员从系统描述的不同阶段中取得信息进行综合考虑。

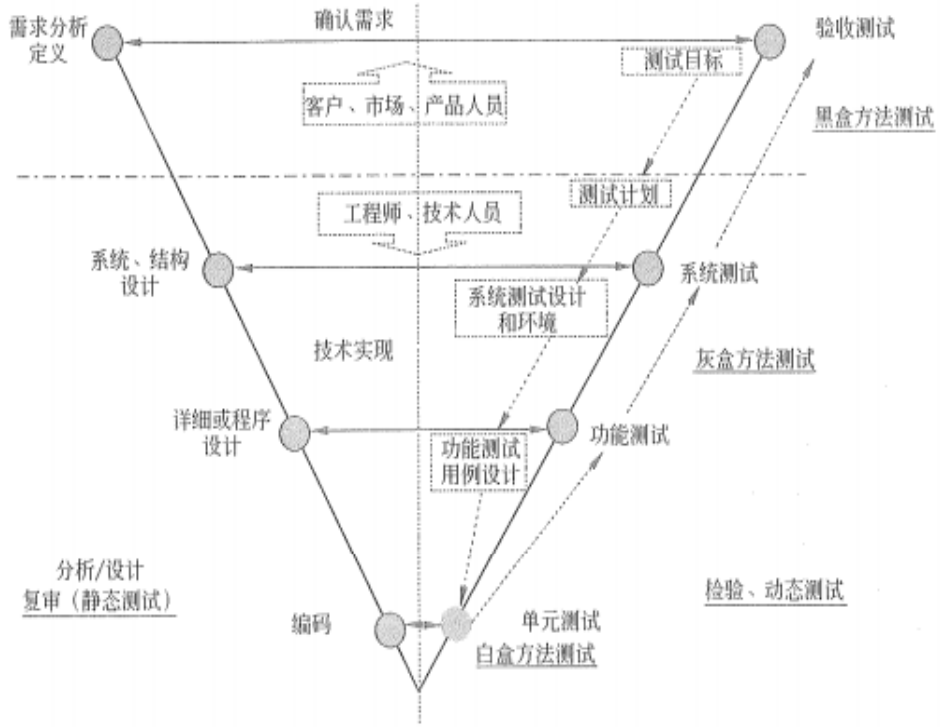


图 23-1　软件测试 V 模型

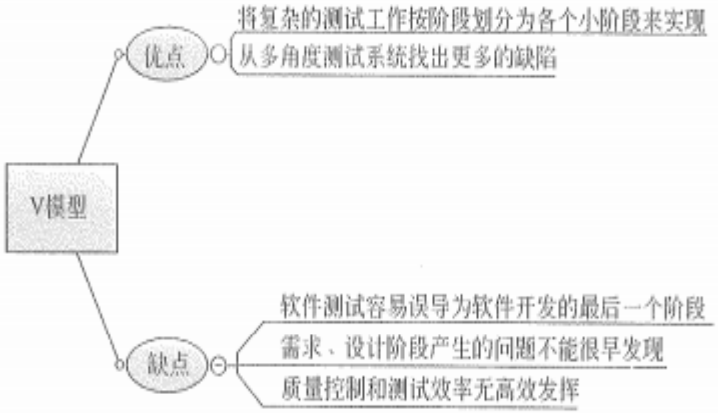


图 23-2　V 模型优缺点

5、由于V模型在软件开发编码完成后才介入测试工作，导致一些在需求和设计中的问题在后期验收测试中才被发现，这样不能体现“尽早地和不断地进行软件测试”的原则。由此演化成一种W模型。

6、相对于V模型，W模型增加了软件各开发阶段中同步进行的验证和确认测试活动。W模型由两个V字型模型组成，分别代表测试与开发过程，表示出了他们的并行关系。

7、W模型相当两个V模型的叠加，一个是开发的V，一个是测试的V，由于在项目中开发和测试的是同步进行，相当于两个V是并列、同步进行的，测试在一定程度上是随着开发的进展而不断向前进行。

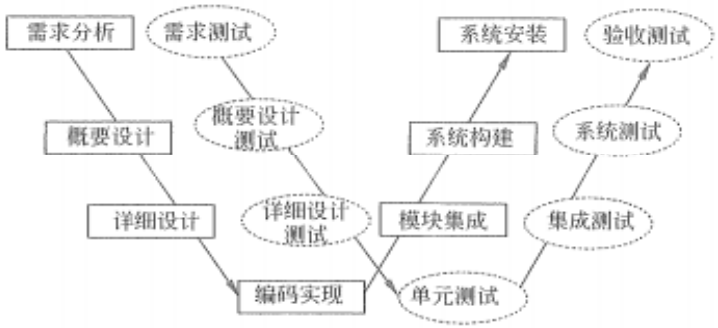


图 23-3 软件测试 W 模型

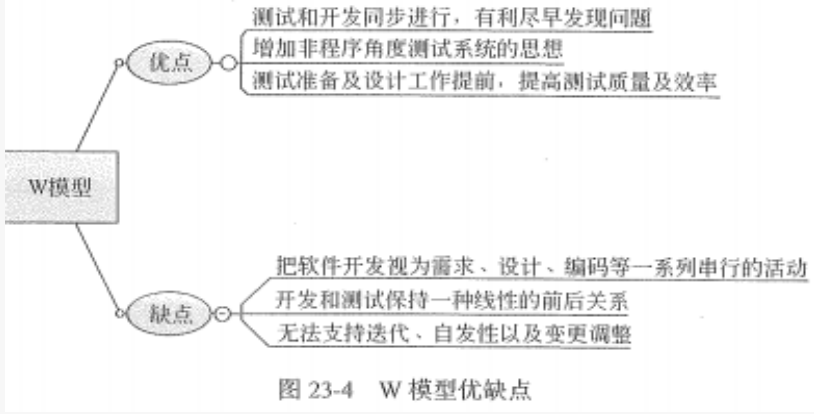


图 23-4 W 模型优缺点

8、在V模型和W模型中都存在一定的局限性，它们都把软件的开发过程视为需求、设计、编码等一系列串行的活动，但实际上，这些串行活动之间存在着相互牵制的关系，并且在大部分时间内，他们是可以交叉进行的。

9、H模型将测试活动完全独立出来，形成一个完全独立的流程

10、H模型图仅仅演示了在整个生存周期中某个层次上的一次“测试循环”。图中的其他流程可以是任意开发流程，如设计流程和编码流程。也可以是其他非开发流程，如SQA 流程，甚至是测试流程。也就是说，只要测试条件成熟了，测试准备活动完成了，测试执行活动就可以进行了

11、H模型揭示了一个原理：软件测试模型是一个独立的流程，贯穿于整个软件产品的周期，与其他流程并发地进行。

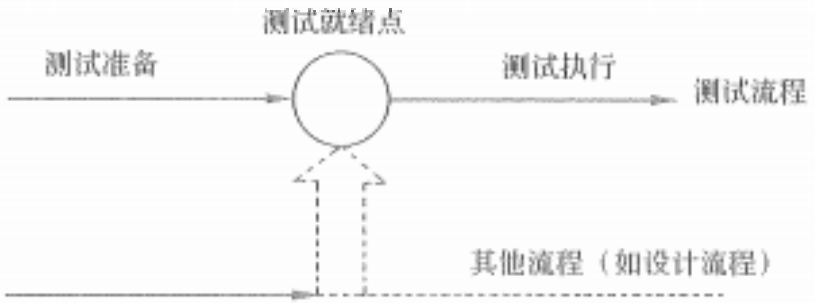


图 23-5 软件测试 H 模型

图 23-6 H 模型优缺点

12、对V模型的最主要批评是V模型无法引导项目的全部过程。X模型也是对V模型的改进，X模型提出针对单独的程序片段进行相互分离的编码和测试，此后通过频繁的交接和集成最终合成为可执行的程序。

13、X模型的左边描述的是针对单独程序片段进行的相互分离的编码和测试

14、X模型还定位了探索性测试,这是不进行事先计划的特殊类型的测试

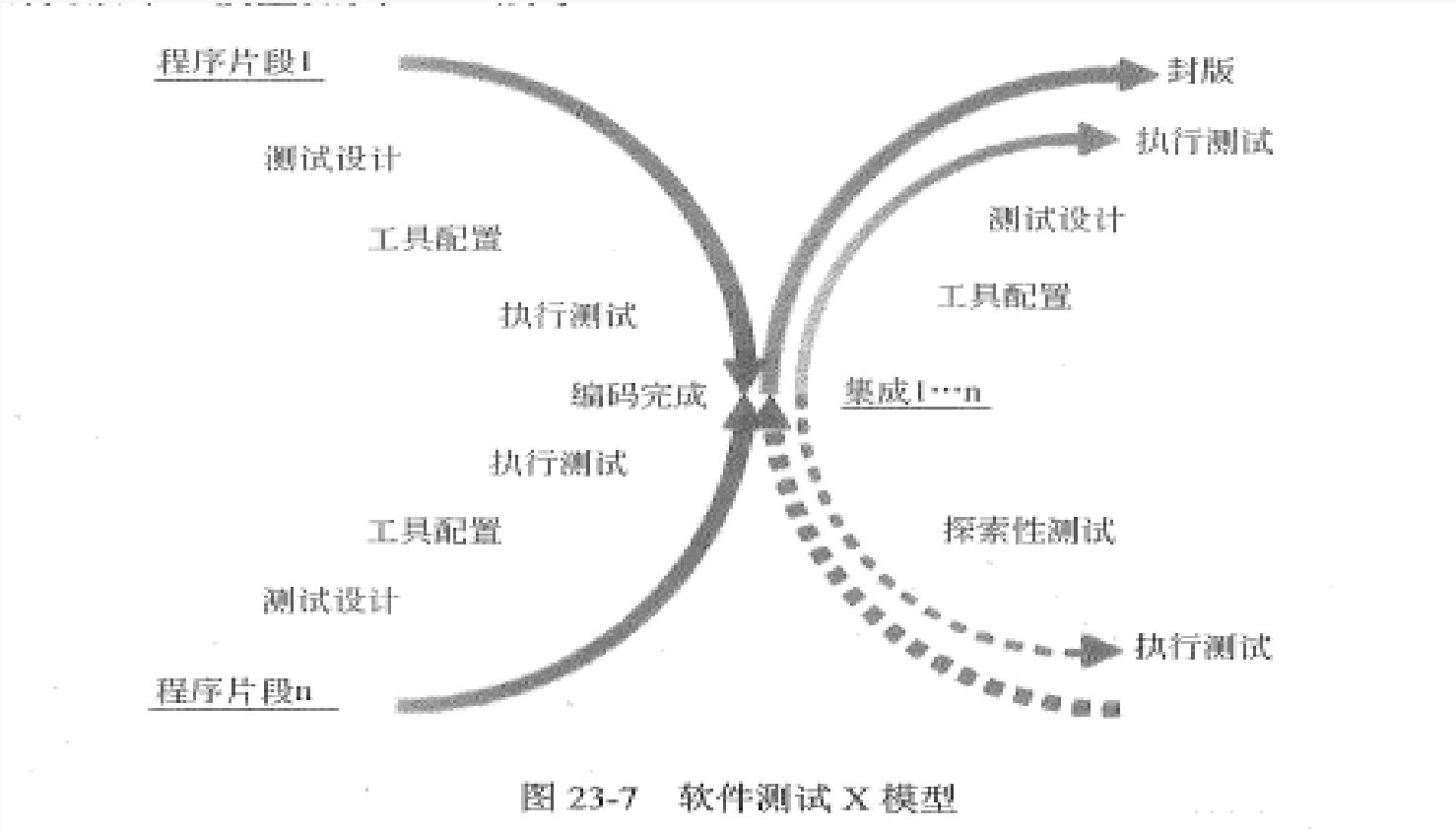


图 23-7 软件测试 X 模型

15、前置测试模型将测试和开发紧密结合，提供了一种轻松的方式，可以使你的项目加快速度。
16、前置测试模型将开发和测试的生命周期整合在一起，标识了项目生命周期从开始到结束之间的关键行为。
17、前置测试将测试执行和开发结合在一起，并在开发阶段以“编码一测试一编码一测试”的方式来体现。当程序片段一旦编写完成，就会立即进行测试。一般情况下，先进行的测试是单元测试，因为开发人员认为通过测试来发现错误是最经济的方式。
18、与V模型不同的是，前置测试模型认识到验收测试中所包含的3个要素：基于测试的需求、验收标准和验收测试计划，其中基于测试的需求和验收标准都与业务需求定义相联系，但是，验收测试计划则需要等到系统设计完成，因为验收测试计划是由针对按设计实现的系统来进行的一些明确操作定义所组成。
19、前置测试模型用较低的成本来及早发现错误，并且充分强调了测试对确保系统的高质量的重要意义。在整个开发过程中，反复使用了各种测试技术以使开发人员、经理和用户节省其时间，简化其工作。

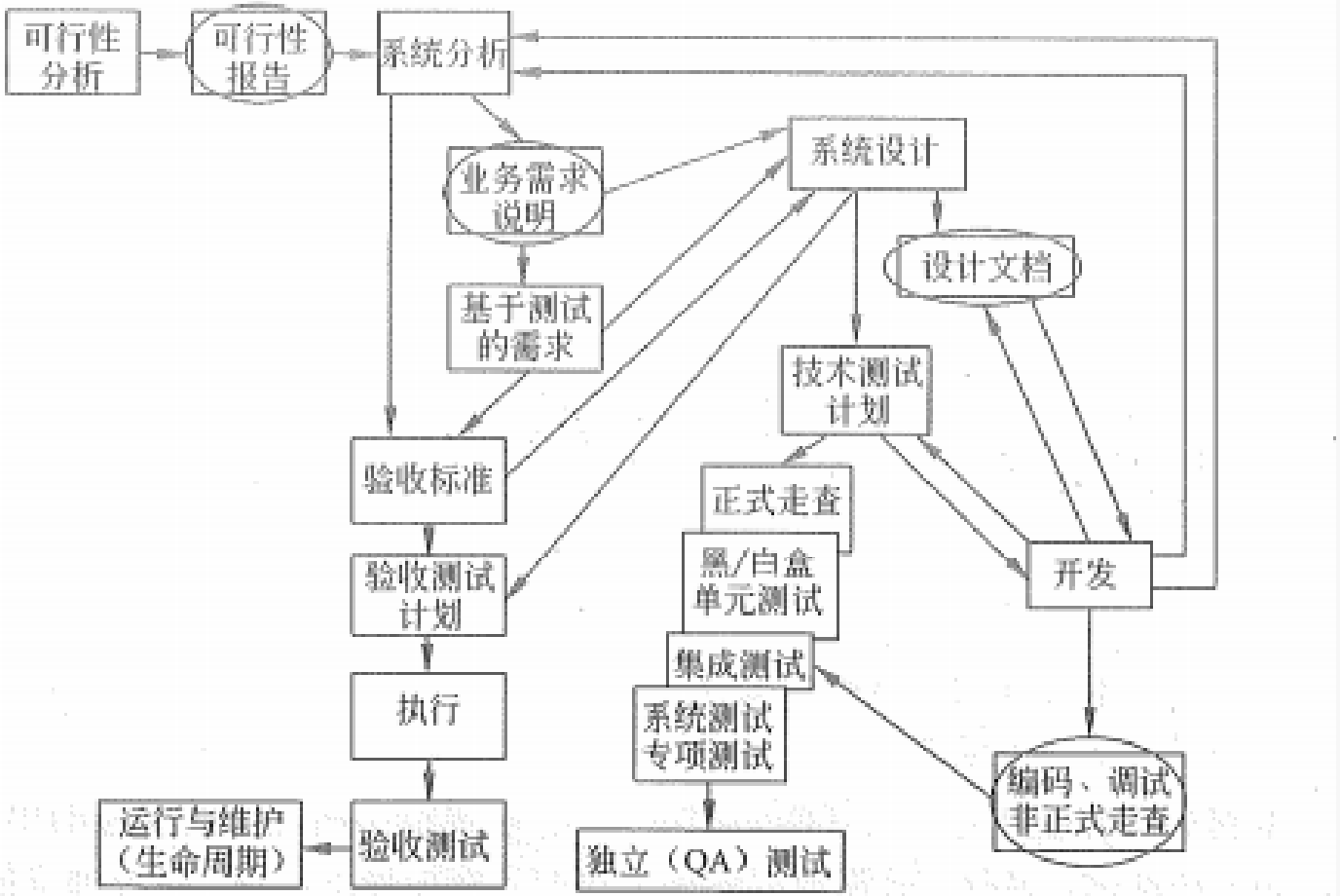

可行性分析
可行性报告
系统分析
业务需求说明
基于测试的需求
系统设计
设计文档
技术测试计划
验收标准
验收测试计划
执行
运行与维护（生命周期）
验收测试
正式走查
黑/白盒单元测试
集成测试
系统测试专项测试
独立（QA）测试
开发
编码、调试非正式走查

图 23-9　前置测试模型

23.1.2 软件测试类型

1、按照不同的划分方式，软件测试分为不同的类型。当按照开发阶段划分时，软件测试类型分为单元测试、集成测试、系统测试和验收测试。当按照测试实施组织划分时，软件测试类型分为开发方测试、用户测试、第三方测试。当按照测试技术划分时，软件测试类型分为黑盒测试、白盒测试和灰盒测试。当按照测试执行方式划分时，软件测试类型分为静态测试和动态测试。当按照测试对象 类型划分时，软件测试类型分为功能测试、界面测试、流程测试、接口测试、安装测试、文档测试、源代码测试、数据库测试、网络测试和性能测试。当按照质量属性划分时；软件测试类型分为容错性测试、兼容性测试、安全性测试、可靠性测试、维护性测试、可移植性测试和易用性测试。当按照测试地域划分时,软件测试类型分为本地化测试和国际化测试。

2、按开发阶段划分，如图

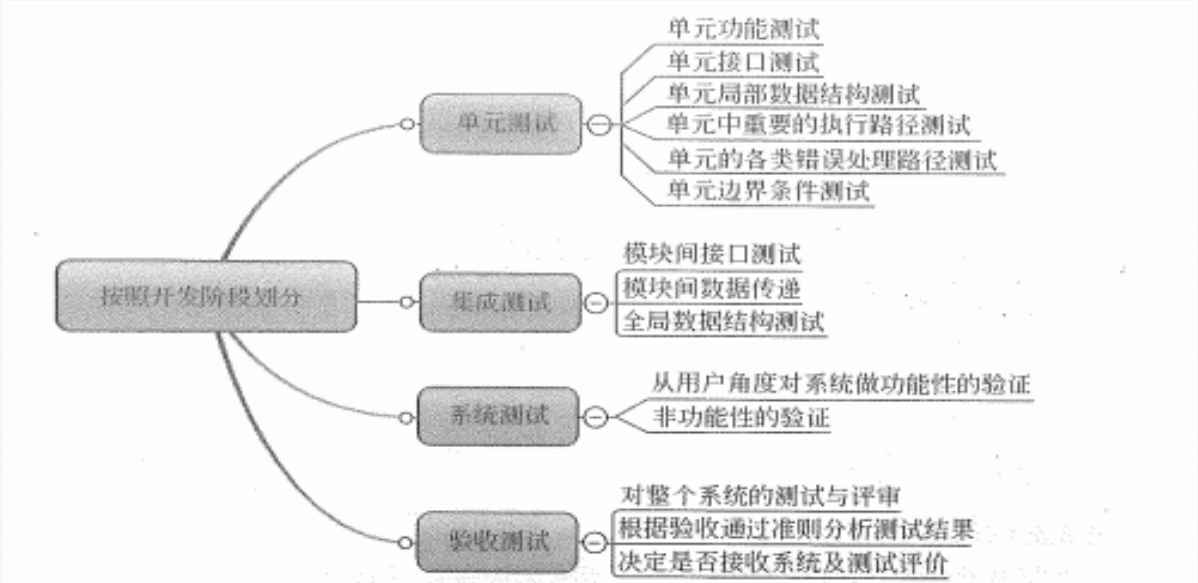


图 23-10 软件测试类型-按开发阶段划分

3、单元测试又称模块测试，是针对软件设计的最小单元（即程序模块）进行正确性检验的工作。单元测试的原则如下。

（1）应该尽早进行软件单元测试。

（2）应该保证单元测试的可重复性。

（3）尽可能采用测试自动化的手段来支持单元测试活动。

4、集成测试又称组装测试、联合测试、子系统测试或部件测试。集成测试是在单元测试的基础上，将所有模块按照设计要求（如根据结构图）组装成子系统或系统进行的测试活动。

5、系统测试是对已经集成好的软件系统进行彻底的测试，以验证软件系统的正确性和性能等是否满足其规约所指定的要求。系统测试的对象不仅仅包括需要测试的产品系统的软件，还要包含软件所依赖的硬件、外设甚至包括某些数据、某些支持软件及其接口等。系统测试的目的是在真实系统工作环境下通过与系统的需求定义作比较，检验完整的软件配置项能否和系统正确连接，发现软件与系统设计文档或软件开发合同规定不符合或与之矛盾的地方

6、验收测试：验收测试是在软件产品完成了功能测试和系统测试之后、产品发布之前所进行的软件测试活动，它是技术测试的最后一个阶段，也称为交付测试、发布测试或确认测试。

通常会有四种情况。

（1）测试项目通过。

（2）测试项目没有通过，并且不存在变通方法，需要作很大的修改。

（3）测试项目没有通过，但存在变通方法，在维护后期或下一个版本改进。

（4）测试项目无法评估或者无法给出完整的评估。此时必须给出原因。如果是因为该测试项目没有说清楚，应该修改测试计划。

按照测试执行者的不同，对不同项目的验收测试的称呼也不同。当测试的执行者是测试内部人员，且待测系统为公司内部产品时，我们称为发布测试或确认测试。当测试的执行者是客户或用户，且待测系统为交付客户的项目时，我们称为验收测试或交付测试。

7、按照测试实施组织划分

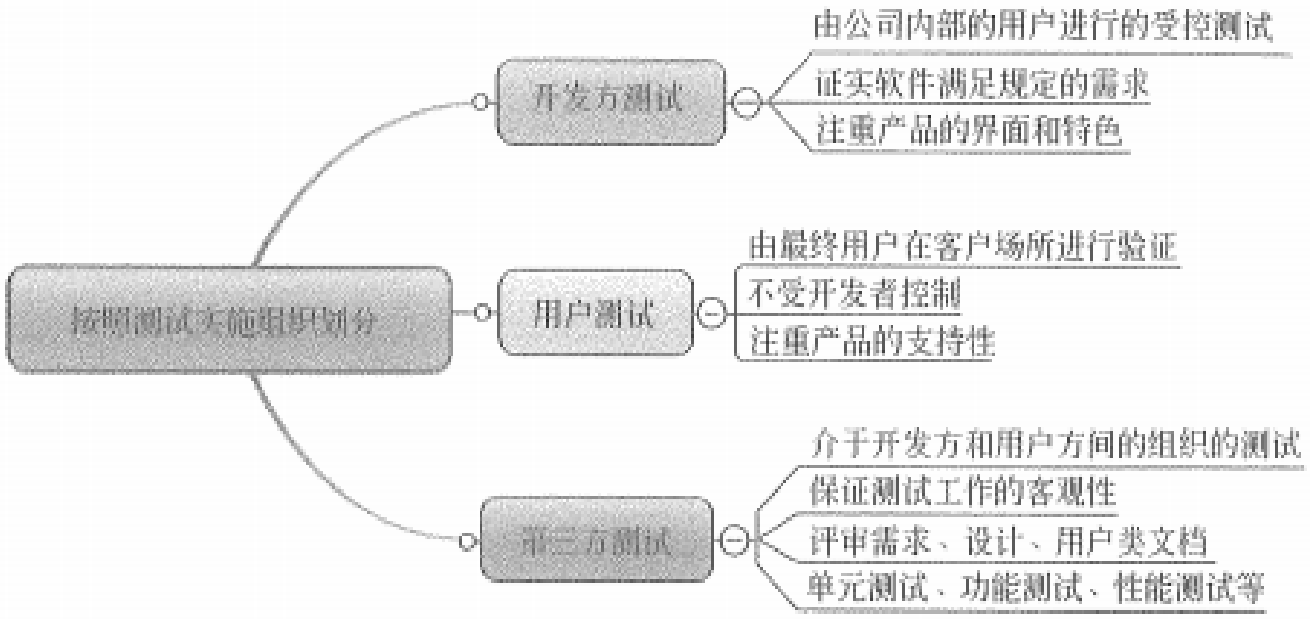


图 23-11 软件测试类型-按测试实施组织划分

8、开发方测试通常也叫“验证测试”或“α测试”。Alpha测试是由一个用户在开发环境下进行的测试，不能由程序员或测试员（有的地方又说可以让测试人员进行）完成。测试发现的错误，可以在测试现场立刻反馈给开发人员，由开发人员及时分析和处理。

9、用户测试是在用户的应用环境下，用户通过运行和使用软件，检测与核实软件实现是否符合自己预期的要求。通常情况下用户测试不是指用户的“验收测试”，而是指用户的使用性测试。Beta测试（即β测试）通过被看成是一种“用户测试”。Beta测试由软件的最终用户们在一个或多个客户场所进行。与Alpha测试不同的是开发者通常不在Beta测试的现场，Beta测试不能由程序员或测试员完成。因而，Beta 测试是在开发者无法控制的环境下进行的软件现场应用。

10、α、β、γ常用来表示软件测试过程中的三个阶段：α是第一阶段，一般只供内部测试使用；β是第二个阶段，已经消除了软件中大部分的不完善之处，但仍有可能还存在缺陷和漏洞，一般只提供给特定的用户群来测试使用；γ是第三个阶段，此时产品已经相当成熟，只需在个别地方再做进一步的优化处理即可上市发行。

11、第三方测试也称为独立测试，是介于软件开发方和用户方之间的测试组织的测试。一般情况下是在模拟用户真实应用环境下，进行软件确认测试。第三方测试有别于开发人员或用户进行的测试，其目的是为了保证测试工作的客观性。从国外的经验来看，测试逐渐由专业的第三方承担。同时第三方测试还可适当兼顾初级监理的功能，第三方测试以合同的形式制约了测试方，使得它与开发方存在某种“对立”的关系，所以它不会刻意维护开发方的利益，保证了测试工作在一开始就具有客观性。

12、按照测试技术划分

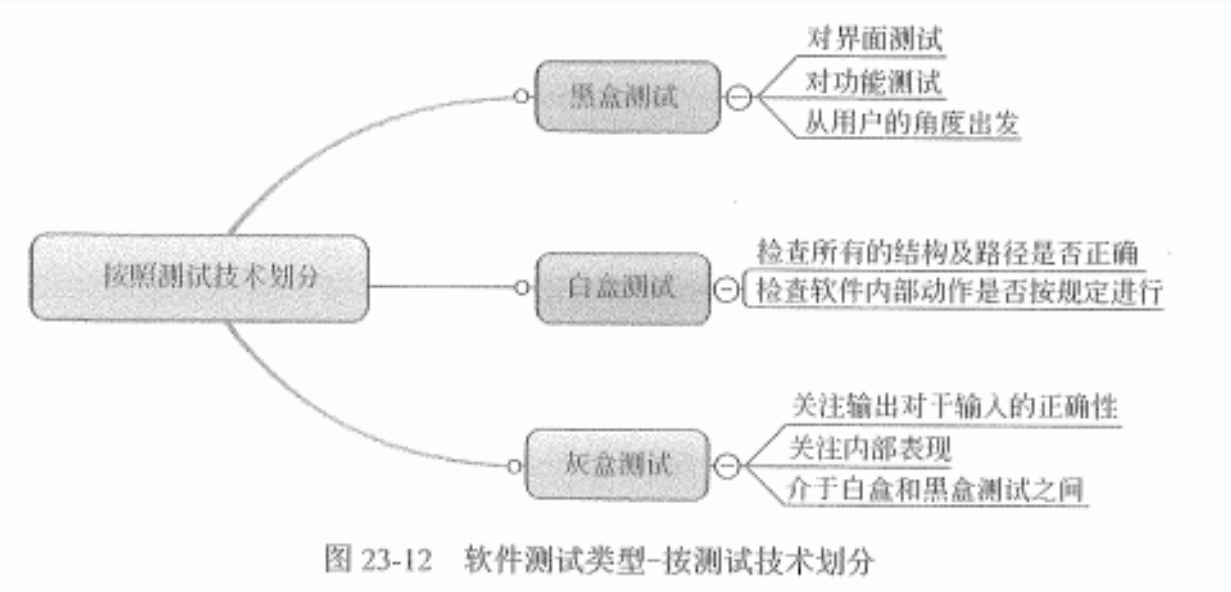


图 23-12 软件测试类型-按测试技术划分

13、黑盒测试也称功能测试，它是通过测试来检测每个功能是否都能正常使用。黑盒测试着眼于程序外部结构，不考虑内部逻辑结构，主要针对软件界面和软件功能进行测试。黑盒测试是以用户的角度，从输入数据与输出数据的对应关系出发进行测试的。从理论上讲，黑盒测试只有采用穷举输入测试，把所有可能的输入都作为测试情况考虑，才能查出程序中所有的错误。具体的黑盒测试用例设计方法包括等价类划分法、边界值分析法、错误推测法、因果图法、判定表法、正交试验设计法、功能图法、场景分析法等。

14、白盒测试又称结构测试其目的是通过检查软件内部的逻辑结构，对软件中逻辑路径进行覆盖的测试，可以覆盖全部代码、分支、路径和条件。

15、白盒测试和黑盒测试的联系如下。

（1）用白盒测试验证单元的基本功能；用黑盒测试的思考方法设计测试用例。

（2）黑盒测试中使用白盒测试的手段，常称为“灰盒测试”。

（3）白盒测试需要对程序的内部实现十分熟悉，黑盒测试是完全基于对系统需求的了解。

（4）仅仅使用白盒测试，或者仅仅使用黑盒测试都不能系统地全面测试一个软件。

16、灰盒测试是介于白盒测试与黑盒测试之间的测试。灰盒测试关注输出对于输入的正确性，同时也关注内部表现，但这种关注不像白盒测试详细、完整，只是通过一些表征的现象、事 件、标志来判断内部的运行状态。灰盒测试是基于程序运行时的外部表现同时又结合程序内部逻辑结构来设计用例，执行程序并采集程序路径执行信息和外部用户接口结果的测试技术。

其缺点：

（1）投入的时间比黑盒测试大概多20%～40%的时间。

（2）对测试人员的要求比黑盒测试高；灰盒测试要求测试人员清楚系统内部由哪些模块构成，模块之间如何协作。

（3）不如白盒测试深入。

（4）不适用于简单的系统。所谓的简单系统，就是简单到总共只有一个模块。由于灰盒测试关注于系统内部模块之间的交互。如果某个系统简单到只有一个模块；那就没必要进行灰盒测试了。

16、按测试执行方式划分

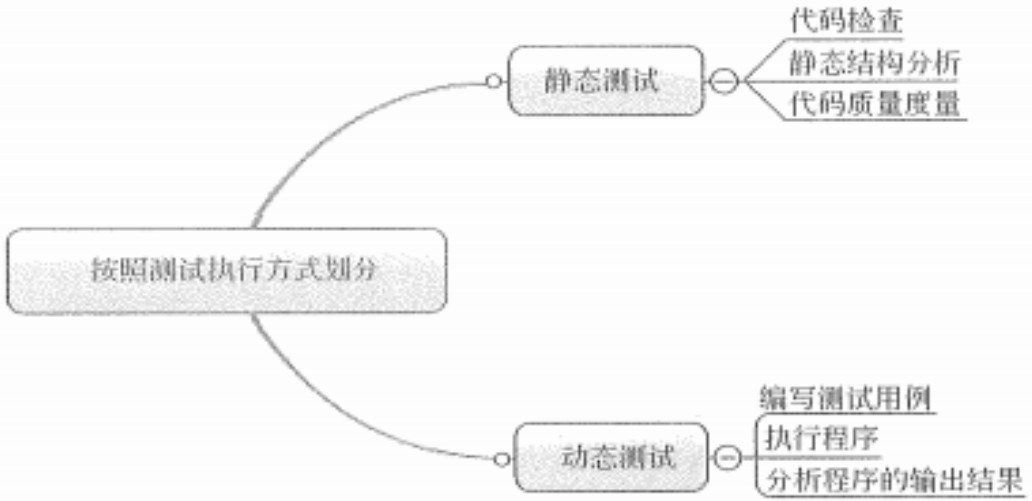


图 23-13 软件测试类型-按测试执行方式划分

17、静态测试是指不运行程序，通过人工对程序和文档进行分析与检查；静态测试技术又称为静态分析技术，静态测试实际上是对软件中的需求说明书、设计说明书、程序源代码、用户手册等进行非运行的检查。静态测试包括代码检查、静态结构分析、代码质量度量等。它可以由人工进行，也可以借助软件工具自动进行。

18、动态测试是指通过人工或使用工具运行程序进行检查、分析程序的执行状态和程序的外部表现。动态方法指通过运行被测程序，检查运行结果与预期结果的差异，并分析运行效率 结果与预期结果的差异，并分析运行效率和健壮性等性能，这种方法由三部分组成：编写测试用例，执行程序，分析程序的输出结果。静态测试与动态测试的区别如下。

（1）静态测试是用于预防的，动态测试是用于校正。

（2）多次的静态测试比动态测试要效率高。

（3）静态测试综合测试程序代码。

（4）在相当短的时间里，静态测试的覆盖率能达到100%,而动态测试经常是只能达到50%左右。

（5）动态测试比静态测试更花时间。

（6）静态测试比动态测试更能发现Bug。

（7）静态测试的执行可以在程序编码编译前，动态测试只能在编译后才能执行。

19、按测试对象类型划分

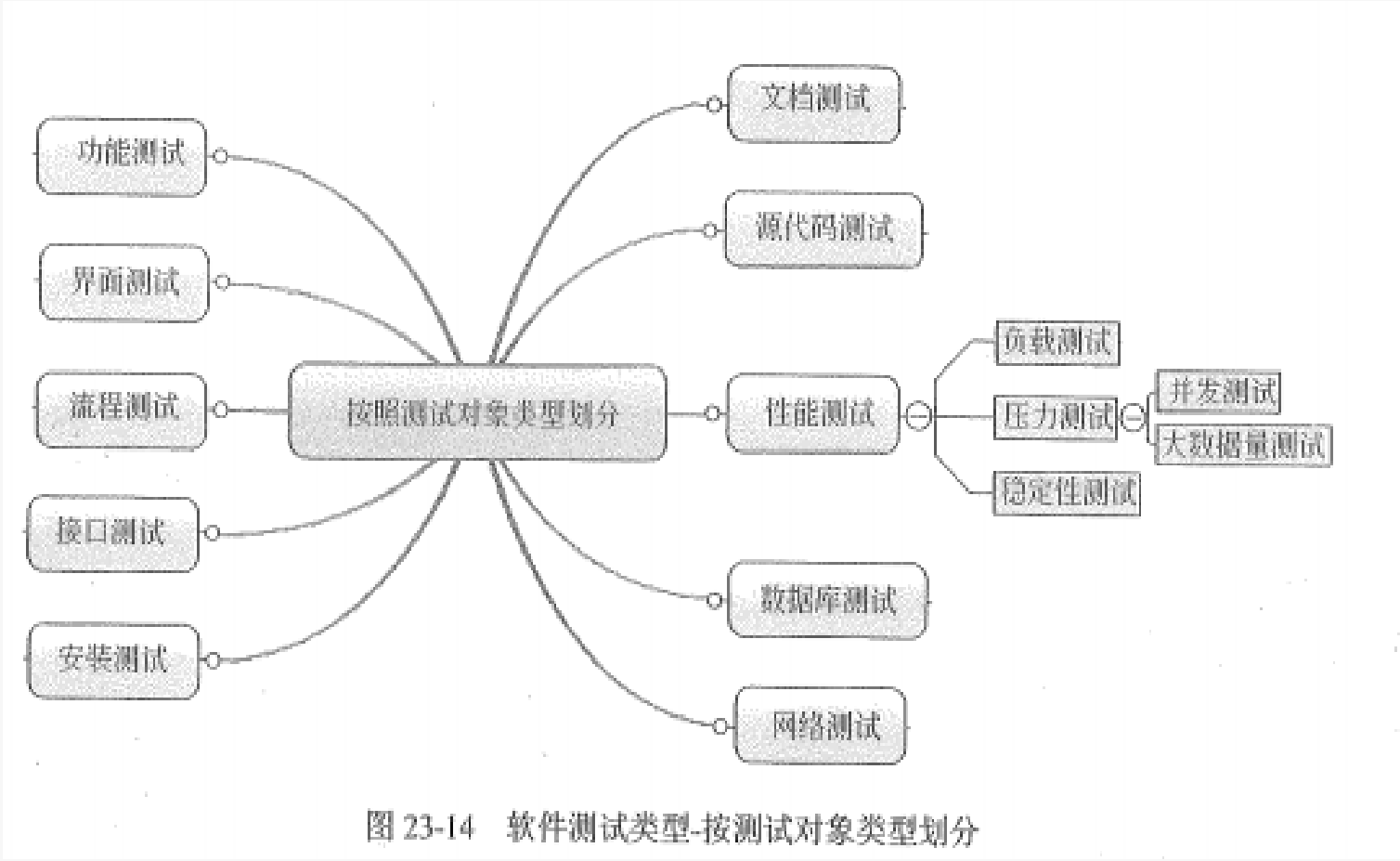


图 23-14 软件测试类型-按测试对象类型划分

20、功能测试：对软件功能进行的测试，主要检查软件功能是否实现了软件功能说明书（软件需求）上的功能要求。
21、界面测试：对软件的用户界面进行的测试，主要检查用户界面的美观度、统一性、易用性等方面的内容
22、流程测试：按操作流程进行的测试，主要有业务流程、数据流程、逻辑流程，其目的是检查软件在按流程操作时是否能够正确处理。
23、接口测试是测试系统组件间接口的一种测试。接口测试主要用于检测外部系统与系统之间以及内部各个子系统之间的交互点。测试的重点是要检查数据的交换，传递和控制管理过程，以及系统间的相互逻辑依赖关系等。
24、安装测试包括测试安装代码以及安装手册,安装手册提供如何进行安装，安装代码提供安装一些程序能够运行的基础数据。
25、文档测试

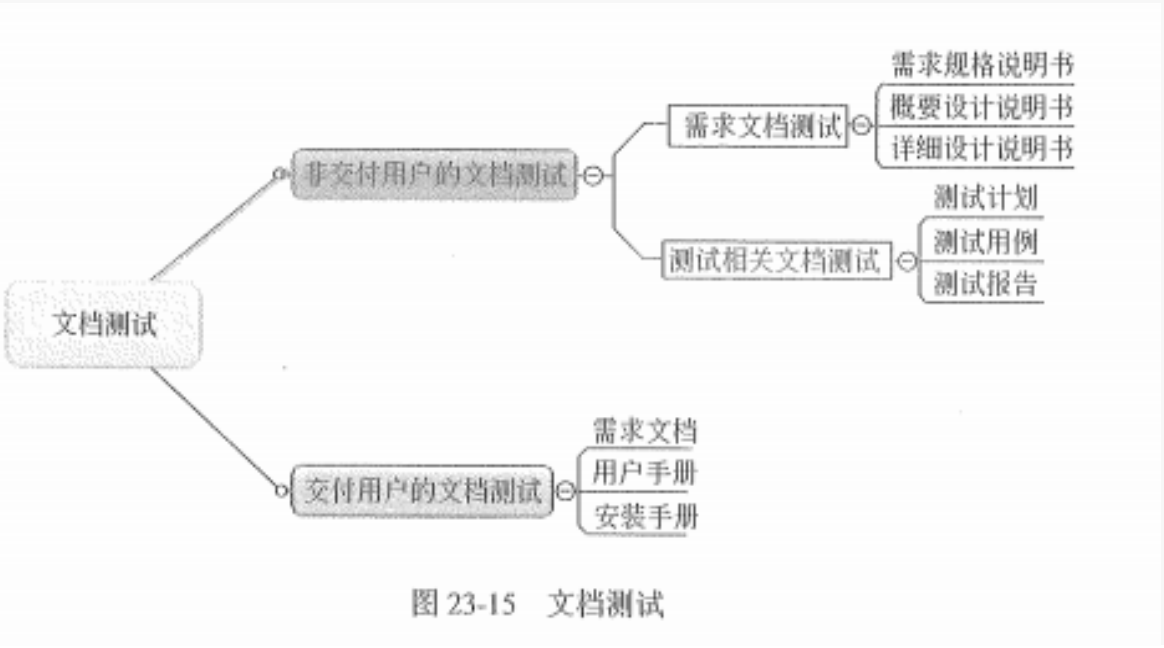
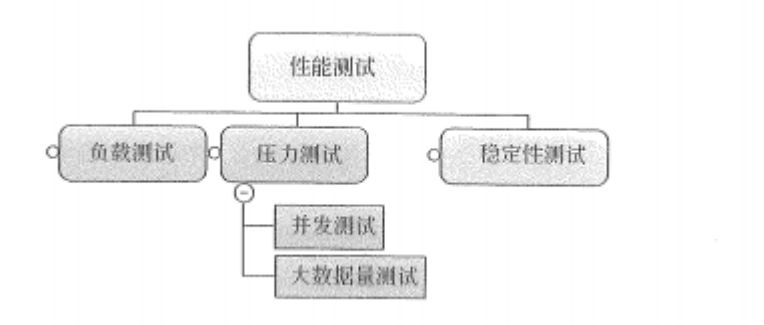


图 23-15 文档测试

26、源代码测试：通过本类型的测评发现应用程序、源代码中包括OWASP十大Web漏洞在内的安全漏洞，识别、定位存在的安全漏洞，并分析漏洞风险，提出整改建议，提高系统的安全性。
27、数据库测试的主要因素有：数据完整性、数据有效性和数据操作和更新。
28、网络测试主要是验证以下几个方面：链路连接情况、错包率、连通性、网络质量、路由策略、备份路由、网管等
29、性能测试



（1）负载测试，又叫强度测试，是通过逐步增加系统负载，测试系统性能的变化，并最终确定在满足性能指标的情况下，系统所能承受的最大负载量的测试。负载测试的目标是确定并确保系统在超出最大预期工作量的情况下仍能正常运行。此外，负载测试还要评估性能特征，例如，响应时间、事务处理速率和其他与时间相关的方面。
（2）压力测试：对系统逐渐增加压力的测试，来获得系统能提供的最大的服务级别的测试或者不能接收用户请求的性能点。通俗地讲，压力测试是为了发现在什么条件下应用程序的性能会变得不可接受。压力测试包括并发测试和大数据量测试。
①并发测试：主要指当测试多用户并发访问同一个应用、模块、数据时是否产生隐藏的并发问题，如内存泄漏、线程锁、资源争用等问题，几乎所有的性能测试都会涉及并发测试。并发测试目的不是为了获得性能指标，而是为了发现并发引起的问题。

②大数据量测试。大数据量测试包括独立的数据量测试和综合数据量测试两类。独立的数据量测试指针对某些系统存储、传输、统计、查询等业务进行的大数据量测试。综合数据量测试指和压力性能测试、负载性能测试、稳定性性能测试相结合的综合测试。

（3）稳定性测试。也叫疲劳强度测试。通常是采用系统稳定运行情况下的并发用户数，或者日常运行用户数，持续运行较长一段时间，保证达到系统疲劳强度需求的业务量，通过综合分析交易执行指标和资源监控指标，来确定系统处理最大工作量强度性能的过 程。

稳定性测试是概率性的测试，也就是说即使稳定性测试通过，也不能保证系统实际运行的时候不出问题。所以要尽可能提高测试的可靠性。可以通过多次测试，延长测试时间，增大测试压力来提高测试的可靠性。

30、按照质量属性划分

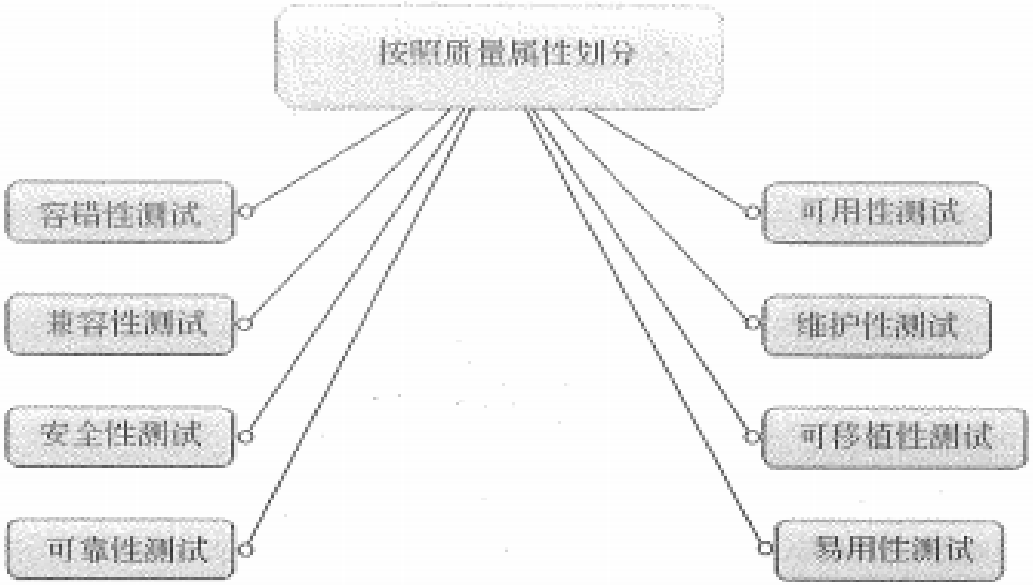


图 23-17 软件测试类型-按质量属性划分

31、容错性测试主要检查系统的容错能力，检查软件在异常条件下自身是否具有防护性的措施或者某种灾难性恢复的手段。

32、兼容性测试是指测试软件在特定的硬件平台上、不同的应用软件之间、不同的操作系统平台上、不同的网络等环境中是否能够很友好的运行的测试。

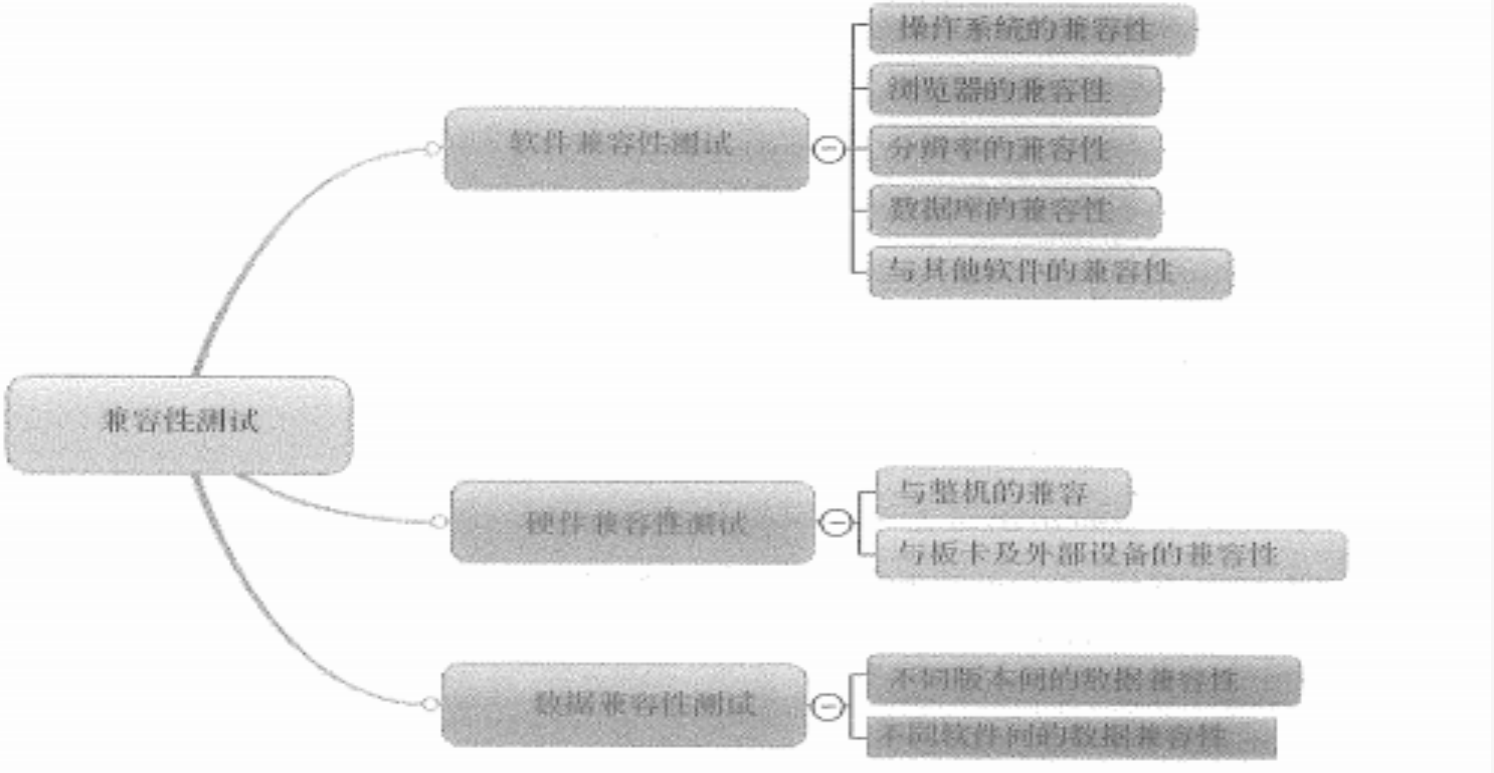


图 23-18 兼容性测试

33、安全测试是在IT软件产品的生命周期中，特别是产品开发基本完成到发布阶段，对产品进行检验以验证产品符合安全需求定义和产品质量标准的过程。
34、软件可靠性测试是指在预期的使用环境中，为检测出软件缺陷，验证和评估是否达到用户对软件可靠性需求而组织实施的一种软件测试。
35、可用性测试，是评估（测试）设计方案或者产品的可用性水平。
36、维护性测试，可维护性是衡量对已经完成的软件进行调整需要多大的努力。
37、可移植性测试：可移植性指未经修改或修改部分源代码后，应用程序或系统从一种环境移植到另一种环境中还能正常工作的难易程度。根据可移植性测试类型与指标体系结构的对应关系，可移植性测试类型包括代码变更测试、安装测试、用户界面测试和功能测试。
38、易用性测试主要考察评定软件的易学易用性、各个功能是否易于完成、软件界面是否友好等

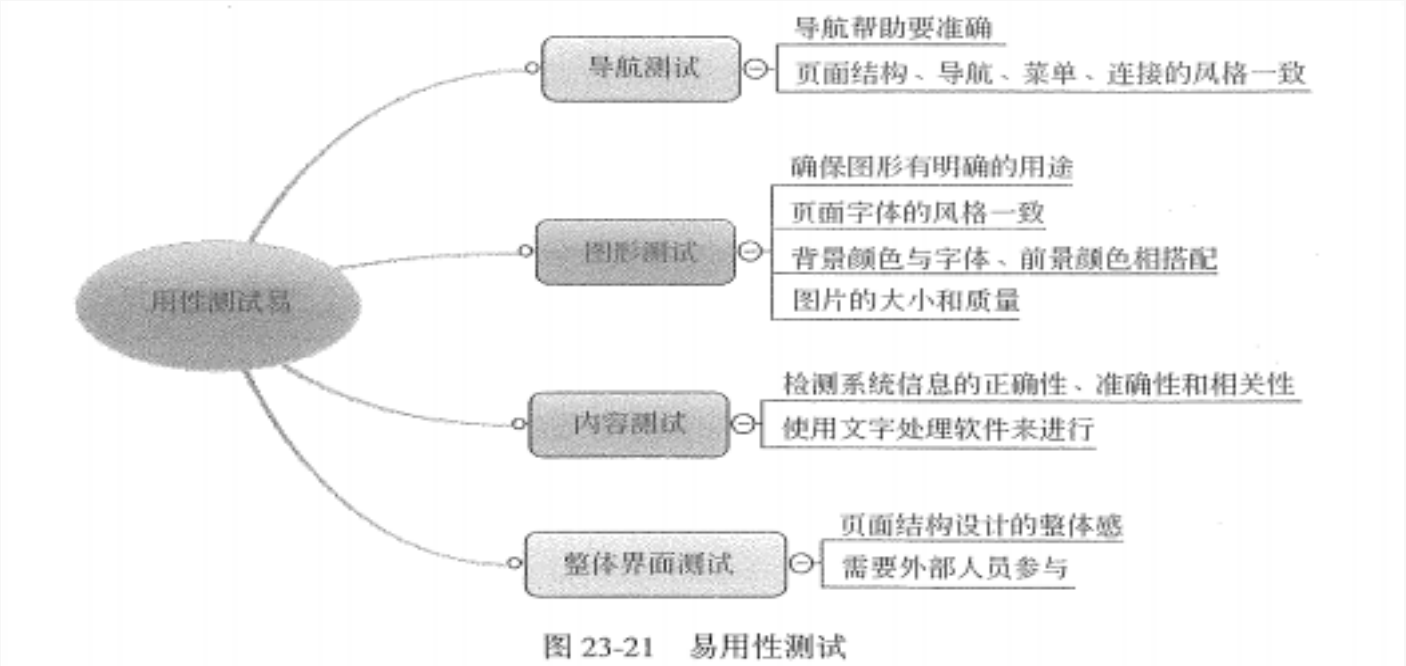


图 23-21 易用性测试

39、按照测试地域划分

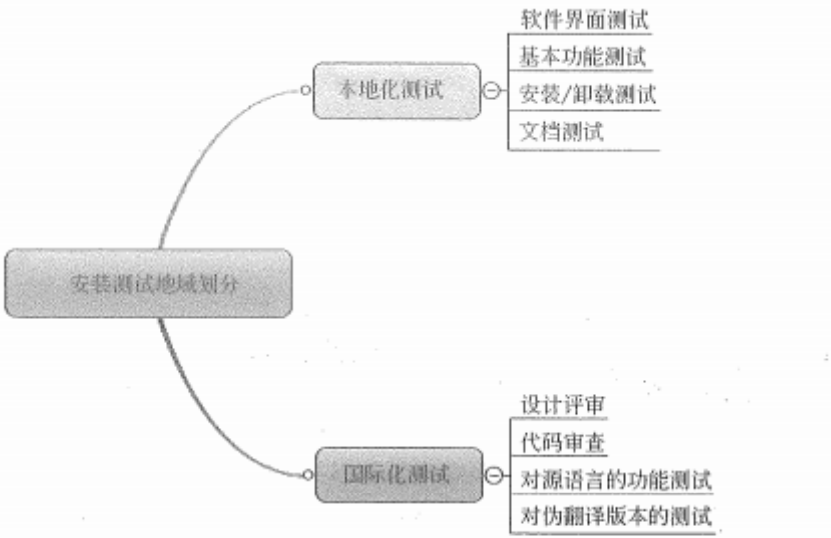


图 23-22 软件测试类型-按测试地域划分

40、本地化测试的对象是软件的本地化版本。本地化测试的目的是测试特定目标区域设置的软件本地化质量。

41、软件国际化的测试就是验证软件产品是否支持一些特性，包括多字节字符集的支持、区域设置、时区设置、界面定制性、内嵌字符串编码和字符串扩展等。设计评审和代码审查是国际化测试中最有效的方法

23.2 软件测试技术

软件测试技术主要包括白盒测试技术和黑盒测试技术，然而随着近些年测试技术的不断应用及实践，功能自动化测试技术、接口测试技术、性能测试技术以及探索式测试技术都被人们越来越重视

23.2.1 黑盒测试法

1、黑盒测试主要检查程序外部结构，不考虑内部逻辑结构。
2、黑盒测试的优点主要有以下几点。
（1）比较简单，不需要了解程序内部的代码及实现。
（2）与软件的内部实现无关。
（3）从用户角度出发，能很容易地知道用户会用到哪些功能，会遇到哪些问题
（4）基于软件开发文档，所以也能知道软件实现了文档中的哪些功能。
（5）在做软件自动化测试时较为方便。
3、黑盒测试的缺点主要有以下两点。
（1）不可能覆盖所有的代码，覆盖率较低，大概只能达到总代码量的30%。
（2）自动化测试的复用性较低。
4、黑盒测试的测试用例设计方法主要有：测试区域确定法、数据覆盖法、逻辑推断法、业务路径覆盖法等等。
5、测试区域确定法分为等价类划分法和边界值分析法
6、等价类划分法是把所有可能的输入数据，即程序的输入域划分为若干部分（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。每一类的代表性数据在测试中的作用等价于这一类中的其他值。

7、边界值分析法就是对输入或输出的边界值进行测试的一种黑盒测试方法。通常边界值分析法是作为对等价类划分法的补充，这种情况下，其测试用例来自等价类的边界。长期的测试工作经验告诉我们，大量的错误是发生在输入或输出范围的边界上，而不是发生在输入输出范围的内部，因此针对各种边界情况设计测试用例，可以查出更多的错误。

8、边界值分析法与等价类划分法的区别在于：

（1）边界值分析不是从某等价类中随便挑一个作为代表，而是使这个等价类的每个边界都要作为测试条件。

（2）边界值分析不仅考虑输入条件，还要考虑输出空间产生的测试情况。

9、组合覆盖是设计尽可能少的测试用例；使各个被测元素的中的各类测试数据组合都被至少执行一次。组合覆盖是覆盖率很高的覆盖法。组合覆盖测试技术是一种设计测试用例的方法，它利用组合产生能够覆盖规定组合的测试用例。根据覆盖程度的不同，可以分为全组合覆盖、成对组合覆盖、正交实验设计法、数据覆盖法等。这种方法力求用尽可能少的测试用例，覆盖尽可能多的影响因素

10、逻辑推断法包括因果图法、判定表法和大纲法等

11、业务路径覆盖法包括场景分析法和功能图法

12、场景主要包括4种主要的类型：正常的用例场景，备选的用例场景，异常的用例场景,假定推测的场景。

23.2.2 白盒测试法

1、白盒测试又称为结构测试或逻辑驱动测试。

2、采用白盒测试方法必须遵循以下几条原则，才能达到测试的目的。

（1）保证一个模块中的所有独立路径至少被测试一次。

（2）所有逻辑值均需测试真和假两种情况。

（3）检查程序的内部数据结构，保证其结构的有效性。

（4）在上下边界及可操作范围内运行所有循环。

3、白盒测试方法

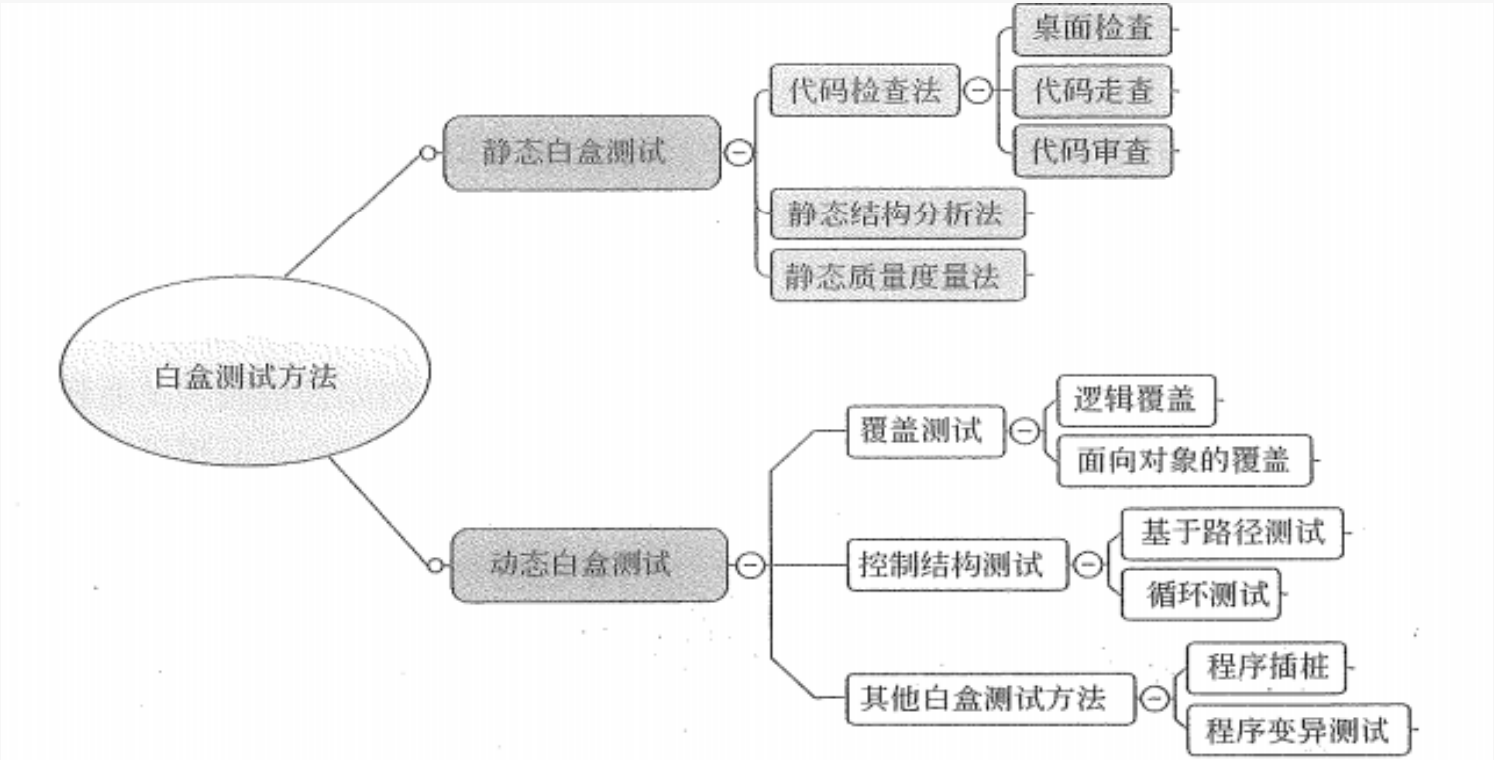


图 23-38　白盒测试方法

4、静态白盒测试是在不执行的条件下，有条理地仔细审查软件设计、体系结构和代码从而找出软件缺陷的过程。静态白盒测试的优点：

（1）尽早发现软件缺陷。

（2）为黑盒测试员在接受软件进行测试时设计和应用测试用例提供思路。

5、动态白盒测试又称结构测试，因为软件测试员可以查看并使用代码的内部结构，从而设计和执行测试。

23.3 信息系统测试管理

23.3.1 测试管理概述

1、测试管理是为了实现测试工作预期目标，以测试人员为中心，对测试生命周期及其所涉及的相应资源进行有效的计划、组织、领导和控制的协调活动。

2、测试管理的主要因素包括测试策略的制定、测试项目进度跟进、项目风险的评估、测试文档的评审、测试内部和外部的协调沟通、测试人员的培养等。

23.3.2 测试管理内容

测试管理的内容按照管理范围和对象，一般可分为测试部门管理和测试项目管理两种。测试部门管理包含部门日常事务、部门人员、部门下属项目、部门资产等的跟赊及管理工作。测试项目管理包含测试人员管理、测试计划及测试策略的编写、测试评审的组织、测试过程的跟进、测试内部和外部的沟通协调、缺陷跟踪等。

23.3.3测试监控管理

测试监控的目的是为测试活动提供反馈信息和可视性。测试监控的内容如下。

（1）测试用例执行的进度。

（2）缺陷的存活时间

（3）缺陷的趋势分析。

（4）缺陷分布密度。

（5）缺陷修改质量。

23.3.4 配置管理

测试过程中的配置管理不仅包括搭建满足要求的测试环境，还包括获取正确的测试、发布版本。

23.3.5 测试风险管理

回归测试风险：回归测试一般不运行全部测试用例，可能存在测试不完全。

23.3.6 测试人员绩效考核

无重要考点，大家有兴趣的话可以读下。

上节考点回顾：

1、（16）不是对称加密算法的优点。

A、加/解密速度快　　B、密钥管理简单

C、加密算法复杂、加密强度高　　D、适宜一对一的信息加密传输过程

2、OSI 安全体系结构定义了五种安全服务，其中（16）用于识别对象的身份并对身份证实。（17）用于防止对资源的非授权访问，确保只有经过授权的实体才能访问受保护的资源

（16）A. 安全认证服务　　B. 访问控制安全服务

C. 数据保密性安全服务　　D. 数据完整性安全服务

（17）A. 安全认证服务　　B. 访问控制安全服务

C. 数据保密性安全服务　　D. 数据完整性安全服务

3、以下关于入侵检测系统功能的叙述中，（18）是不正确的。

A. 保护内部网络免受非法用户的侵入

B. 评估系统关键资源和数据文件的完整性

C. 识别已知的攻击行为

D. 统计分析异常行为

4、信息的（12）要求采用的安全技术保证信息接收者能够验证在传送过程中信息没有被修改，并能防范入侵者用假信息代替合法信息。

A、隐蔽性　　B、机密性　　C、完整性　　D、可靠性

上节考点回顾：

5、在信息系统安全保护中，信息安全策略控制用户对文件、数据库表等客体的访问属于（16）安全管理

A、安全审计　　B、入侵检测　　C、访问控制　　D、人员行为

6、IDS发现网络接口收到来自特定IP地址的大量无效的非正常生成的数据包，使服务器过于繁忙以至于不能应答请求，IDS会将本次攻击方式定义为（17）

A、拒绝服务攻击　　B、地址欺骗攻击　　C、会话劫持　　D、信号包探测程序攻击

7、通过收集和分析计算机系统或网络的关键节点信息，以发现网络或系统中是否有违反安全策略的行为和被攻击的迹象的技术被称为（18）

A、系统检测　　B、系统分析　　C、系统审计　　D、入侵检测

8、为了保护网络系统的硬件、软件及其系统中的数据，需要相应的网络安全工具，以下安全工具中（16）被比喻为网络安全的大门，用来鉴别什么样的数据包可以进入企业内部同。

A. 杀毒软件　　B. 入侵检测系统　　C. 安全审计系统　　D. 防火墙

9、信息系统访问控制机制中，（17）是指对所有主题和客体部分分配安全标签用来标识所属的安全级别，然后在访问控制执行时对主题和客体的安全级别进行比较，确定本次访问是否合法性的技术或方法

A. 自主访问控制　　B. 强制访问控制　　C. 基于角色的访问控制　　D. 基于组的访问控制

感谢您的聆听