浅析管理信息系统软件测试

乔昱霖　黄良经　李丹宁
山东英才学院，中国·山东 济南 250100

【摘　要】本文主要通过分析管理信息系统软件的测试内容，介绍当下的主流管理信息系统软件测试方法，希望通过有效的软件测试发放来提高软件质量，促进我国管理信息工程的发展。

【关键词】敏捷化；业务安全性

1　软件测试的内容

管理信息系统软件测试主要以单元测试、组装测试、确认测试和验收测试组成。源程序测试中发现的程序缺陷不一定是在编写过程中产生的。 有相关公司统计记载：需求阶段产生的缺陷最多（大概产生54%左右的缺陷），在设计阶段产生的缺陷排在第二（大概26%左右的缺陷），产生缺陷最少的却是编码阶段（大概产生8%左右），额外还有12%左右的缺陷是由软件的兼容性和配置产生的。

1.1单元测试

单元测试和程序调试即有联系，也存在着差异。如果选用一些成熟模块搭建软件，底层单元模块已经千锤百炼，测试的工作量可部分简化。

错误类型	常见表现或原因
数据引用错误	引用的变量未赋值或未初始化，数组引用下表值超界
组装测试	数据定义或属性不匹配，默认属性错误，数据长度或类型不当
运算错误	变量值超限，无效值参与了运算，中间值溢出，运算的优先顺序不正确
控制流程错误	循环越界，有额外的分支路径，程序被不当绕过，判断无法穷尽，文字或语法错误
输入输出错误	文件未及时打开或关闭，处理记录的缓冲区不足
接口错误	参数间的数量、属性或量纲不匹配，全局变量的定义不一致，参数被漏传

单元测试主要强调被测试对象的独立性，也就是为了避免其他单元对本单元的影响，已获得被测试单元的实际状态。如果某个组件比较大，可以进一步分离某些部分，直至分离到一个可接受的程度，这取决与可测试性和要求测试的粒度。单元测试更加强调质量管理的思想。单元是构造软件的基础，只有使每个单元得到足够的测试，软件的质量才有可靠的保证，后续的测试才能顺利的进行。

1.2组装测试

只要有组装后，才会出现一些常见或不常见的问题。组装测试常用于检验一些独立性较强的软件和模块，在其独立运行时可以保证正常工作，但在于其他模块进行交互时，变会产生问题，最常见的是兼容性。

1.3确认测试

确此时尽量采用真实场景和真实数据，并在终端用户参与下完成测试，全面检测并确认系统的质量，看信息系统是否满足了用户当前的需求。

1.4验收测试

验收测试是对软硬件的协调性，新软件平台上业务的流畅性和准确性，用户操作的水平等进行全面检测。检查开发者使用开发工具的合法性，检查开发者使用的第三方软件提供的函数、组件及DLL的合法性。对《需求分析说明书》、《概要设计说明》、《测试计划与报告底稿》、《开发手册》等一些列文档进行完备性、正确性、规范性检验，以及是否按照之前已经定义好的软件编码规范及软件产品说明书对其进行测试。

2　软件测试的分类

2.1软件测试的前的准备工作

软件测试制定一个标准的测试规程是十分重要的，在实际工作中也应遵循。测试过程不可能在真空中进行，如果软件开发人员不说明编写代码的用途和工作原理、何时工作，这对于测试任务是致命的

2.2软件测试的分类

2.2.1配置测试。一般的测试基本可分为：个人计算机、部件（系统主板、部件板卡之类）、外设（鼠标、键盘、打印机等）、接口（ISA、PCI、USB等）、可选项和内存、设备驱动程序。配置测试工作基本上分为两个主要模块，分离配置缺失和计算工作量。

2.2.2易用性测试。软件编写出了是为了使用，这是不言而喻的道理。但是很多时候，在忙于设计、开发和测试复杂产品的时候，软件开发人员和软件的测试人员会忽视这一点。开发小组在编写代码的技术方面投入了太多的时间和精力，然而忽视了软件的最重要的方面，即最终的使用者。

2.2.3文档测试。在过去，软件文档最多是拷贝到软件安装软盘中的readme文件，或者是塞进包装箱的一张小纸，随着信息技术的不断发展，所需内存的不断扩张，现在的软件文档变的越来越大，有时甚至需要投入比制作软件本身还要多的时间和精力。

2.2.4软件的安全性测试。对于软件的安全性评估，可以通过Michael Howard的威胁模式分析（threat modeling）模型，基本步骤如下：构建威胁模型分析小组：对于一个小规模的公司来说，方式上可能是在设计阶段让外部的咨询人员介入，对于一个大公司来说，这类人往往来自于从一个项目转到另一个项目、为项目提供专业咨询的一群专家人士。创建一个体系结构总体图：确认在不同技术和其证明之间的信任边界以及未来访问数据必须进行的授权。确认价值：考虑系统所有的东西对于一个入侵者来说有多大的价值。确认威胁：确认每一部分是否能被修改？黑客是否能阻止授权用户使用系统？是否有人能获得系统的访问权限并控制系统？分解应用程序：这是一个格式化的过程，用来确认数据所在位置以及如何通过系统。记录威胁：每个威胁都必须用文档记录，并且应进行跟踪以确保其被解决，文档是一种简单方式，用于描述威胁（用一句话或者用符号表示）、目标、攻击可能采取的方式、系统对于防御攻击有哪些手段。威胁等级评定：具体参照以下几个方面：潜在的损害、可反复性、可利用性、受影响的用户、可发现性。

参考文献：

[1]Tamfon Brian Bongwong,Bilounga Ndongo Chanceline, assessing the gaps for strengthening.BMC Medical Informatics and Decision Making[J].2020, 20(1).

[2]Jiang Wei Xi,Huang improvements, challenges and implications for China’s National Health Information System.Infectious Diseases of Poverty[J].2021, 10(1).

[3]吴永欢,孙煜华,廖嘉炜.信息系统实用化及数据质量管理研究.信息与电脑(理论版)[J].2017(18).

[4]李文涛,陈华君.大数据时代的信息管理与信息系统研究.中国管理信息化[J].2019(24).