doi: 10.3969/j.issn.1671-1122.2009.12.003

金融信息系统软件二次开发安全问题研究

杨向东

（中国银行山西分行，山西太原 030001）

摘　要：文章从金融行业中遇到的突发性系统故障入手，深入分析了在信息化高速发展的背景下，金融信息系统软件二次开发中存在的风险，同时，结合工作实际，对如何提高软件开发的安全性提出了思路和方法。

关键词：金融信息化；软件开发；软件测试；信息安全

中图分类号：TP393.08　**文献标识码：**A

0 引言

2005 年 11 月 1 日，日本东京证券交易所股票系统发生大规模系统故障，导致所有股票交易全面告停，短短 2 个小时造成了上千亿的损失。这次事故的原因是不久前为增强系统处理能力而更新的交易软件程序存在缺陷。虽然在工程师的紧急抢救下系统得以恢复，但这次事件已经在整个金融界留下了挥之不去的阴影。

为了使金融信息系统中使用的软件更加符合安全需求，对原有软件程序进行改造是常有的事。而通过上述案例就不难看出，金融信息系统软件程序的改动牵一发而动全身，可以直接导致重大安全风险、事故的发生。

1 金融信息系统软件改造存在风险

耗费巨资进行信息系统的建设和改造，其原本目的是为了提高工作效率，更好地促进业务发展，创造更多的利润，然而“制胜的法宝”有时却会变成“要命的魔鬼”，如果软件质量不过关，有时甚至是“微不足道”的缺陷，都会给整个系统埋下严重隐患，特定条件下就会爆发，造成不堪设想的后果。

随着我国金融信息化建设的逐步深入，尤其是“入世”后面临与外资银行同场竞争的挑战，如何依托先进的计算机技术提升自己的综合竞争实力，为客户提供全方位的金融服务已成为我国各商业银行的共识和竞争的焦点。在这个背景下，计算机在金融行业中应用广度和深度都空前提高，已经渗透到了金融工作的各个方面，特别是金融行业实行数据大集中后，各种大规模的软件开发项目也日益增多，随之而来的问题就是如何保证软件的可靠性，如何降低软件开发的成本，如何提高软件的开发质量，这些都成为软件开发时必须重点考虑的内容，对那些大规模的软件工程来说尤其显得重要。

随着信息化系统建设的集中度和复杂度的提高，软件产品也愈发庞大，目前大多数软件产品都由几十万、上百万，甚至更多的程序代码组成，而任意一行代码，哪怕是一个字段都可能影响到整个程序进而影响到整个系统的正常运行，甚至造成系统的崩溃，这种情况在集中化程度越来越高的情况下是非常可怕的。

俗话说“金无足赤，人无完人”，在软件开发这样的系统工程中，通常有很多人及很多部门参与，一个人又可能要完成多项任务，再完善的软件计划和再熟练的开发人员也难免会出现错误和疏漏，所谓绝对周密和天衣无缝只是理想化的目标，比如系统分析员错误地理解了用户的要求，就会发生系统分析员与用户之间的“信息偏差”，系统分析员在书写需求规格说明书时不能正确表达自己的思维，发生了系统分析员思维到文档之间的“信息偏差”，开发过程中个人的思路、风格、水平各不相同，难免发生这样那样的“信息偏差”。总之，用户需求的不确定性、软件设计的不可预测性、客观条件的不确定性、开发人员的水平和个体差异、技术本身的缺陷（如曾经困扰全球计算机行业的 Y2K 问题、系统本身的其他漏洞等）以及软件开发项目管理等都会给软件开发带来不可预知的风险。

2 测试是消除风险的有效手段

由于，金融信息系统的二次开发存在诸多风险，因此对所开发的软件系统的测试就必不可少。测试的一个目的是对软件查错和修正，另一个目的是检验软件是否达到了用户的要求。国外优秀的软件开发机构的测试工作通常都占到整个开发工作量的 40%，而测试费用则占到了总费用的 30—50%，对一些要求高可靠性和高安全性的重要的软件如资金划拨、网络通讯、安全监控等软件的测试力度更大。测试是对需求分析、程序设计、编码的最后复审，从经验上看，测试应遵循下面一些基本原则：

1）设计测试用例时，不仅要给出输入数据，还要给出预期的结果，作到有的放矢。

2）开发组织和测试组织要分立。为保证测试的质量，一定要有非开发人员（用户方和第三方如管理人员、安全稽核人员等）参与测试，因为开发和测试二者在思想上和方法上截然不同，前者是建设性的而后者是破坏性的，就一般人的心理而言，要破坏自己亲手建立的东西是比较困难的。测试人员要有“鸡蛋里面挑骨头”的精神，

3）要设计非法输入的测试用例，要特别注意一个程序不仅能在合法输入时正确执行，而且在非法输入时能给出提

下转第 11 页

做到“可视、可控”，确实保障信息安全工作落到实处。

运维的主要工作就是按照规定的程序保证系统的正常运行。最重要的一是要保证有“规定的程序”，二是要保证能“按照程序去做”。信息中心首先要和有关合作单位制订好“规定的程序”，再制订如何检查落实的规定，进行检查、督促。三是要保障运维的技术水平，要有通用的安全操作规范来保障运维工作的一致性。

“规定的程序”一是每个系统（如网络、办公自动化系统等）的日常运行维护流程，包括：（1）每天、每周、每月要做的工作及检查、测试的内容；（2）所做工作、检查、测试的情况要有记录；（3）要规定日常一般情况如何处理；（4）要规定特殊、应急情况如何处理；（5）要规定需报告的事项和时间要求。支持日常运行维护流程工作，还要有相应的每个系统的操作手册，包括开关机、检查、一般操作所需的命令等。二是系统变更时所需流程：包括申请、变更方案、审批、实施、变更情况确认。三是应急预案，应急预案只需规定可能出现的主要情况，程序要简明、易实施，不需其他协助即可完成。

“检查落实”一是要通过一些控制手段来检查运维人员是否“按照规定”去做工作，如规定每日、每周汇报检查运维情况；每周汇报本周运维情况分析，下周重要运维工作，查看相关的报告，日志等。二是要承担相关的审核、检查工作。

“运维安全性控制”一是控制对系统操作的权限，避免特权用户的产生，将最高权限分散。二是提供技术保障：（1）要有必要的监控手段来监视系统运行情况，而不是依赖于运维人员的主观活动；（2）统一运维操作平台，减少运维人员进入机房操作，加强操作控制；（3）测试环境与运行环境分开：系统新上线或变更时测试可行性，进行应急演练，紧急情况下可代替原系统运行；（4）通过运维管理平台为规范管理流程、加强安全运维管理提供技术保障。

按照《烟草行业信息安全保障体系建设指南》的要求，结合行业实际，信息安全体系建设将围绕数据中心建设，加强技术体系建设，完善技术保障基础。围绕系统集成、信息共享，加强管理体系和运维体系建设，通过管理来保安全，通过运维来做到安全工作落地，使行业信息安全保障水平在近期内有较大提高，以适应“数字烟草”战略下行业信息化的安全保障需要，从而保障行业信息化的可持续和安全发展。（责编 杨晨）

作者简介：张雪峰（1961-），男，处长，高级工程师；王海清（1968-），女，副处长，高工。

上接第 6 页

示并拒绝执行，更不能潜伏其他隐患。

4）对程序修改之后要进行回归测试，对程序的任何修改都可能引入新的错误，所以必须用以前测试的用例进行回归测试，这有助于发现由于修改程序而带来新的错误。

5）在进行深入测试时，要集中测试容易出错的模块，例如，笔者在对 DACI 系统 Y2K 问题测试中发现，几乎所有的日期问题都与系统底层的日期函数有关。

6）设计测试用例时要注意科学合理选择数据，尽量保证程序中所有的语句至少要执行一次，每个判断至少要获得一次“真”和“假”的值，每个条件能获得各种不同的结果，各种判断中的各种条件的各种不同的组合都至少能出现一次，要特别注意对临界值的测试。

7）测试应包括单项测试（逐个模块分调）、整体测试（各功能模块组合在一起联调）、有效性测试（软件的功能与用户的需求是否一致）、系统测试（软件在与其他系统元素如硬件、网络、其他业务系统等结合在一起综合测试）。

8）基本测试完成后应加大程序的负载，进行压力测试，检测系统的承载能力。可采取试运行或试点的办法，试运行期间一定要作好“人机并行”或“双机并行”，并注意收集试运行中出现的各种问题。特别需要指出的是大型软件必须要经过压力测试才能正式投产，而现在有些软件开发项目为了赶进度，往往把这一步给忽略了，其实这一步是很重要的，尤其是对一些跨区域、采用大集中方式处理的软件系统来说更是如此。

在实际工作中可以将“白盒法”和“黑盒法”结合运用，选取测试一些数量有限的重要逻辑路径，并对一些重要的数据结构的正确性进行完全检查，以保证程序接口和内部逻辑的正确性。测试是一项非常复杂的、创造性的、需要高度智慧和丰富经验的工作，一个好的测试用例有可能发现至今尚未发现的错误，而一次成功的测试是发现了至今尚未发现的错误的测试。经过严格测试的软件系统要填写详细的测试报告，并经上级领导授权后方可交付使用。

3 结语

需要指出的是，所有的测试并不可能是完全测试，通常只能证明程序有错，而不能证明程序无错。金融系统中，很多软件系统都是在实际生产中不断发现问题而得到逐步完善的，这也是软件有不同版本和补丁的原因。另外，我国的软件测试业还存在着测试手段和测试工具匮乏、专业测试队伍特别是行业人才奇缺的问题，因此，对于已投入生产的软件系统，仍要进行版本跟踪，并结合业务的变更和技术的发展不断修改、排错、升级、扩充、完善，只有这样，我们的软件系统才经得起时间的考验，才能提高我国金融行业的信息安全保护水平。（责编 杨晨）

作者简介：杨向东（1971-），男，高级工程师，经济师，主要研究方向：信息安全。