软件失效原因分析

谢瑞生

（中国电子科技集团公司第二十八研究所，江苏 南京 210007）

摘 要：从软件与硬件的比较、失效的内外原因、失效的主客观原因等方向出发，通过分析软件生命周期各阶段差错的因果联系，研究软件失效的原因。

关键词：软件可靠性；软件失效；原因分析

中图分类号：TP311 **文献标识码**：A **文章编号**：1672-5468（2009）03-0013-07

Analysis of Software Failure Cause

XIE Rui-sheng

（1. The 28th Research Institute of CETC, Nanjing 210007, China）

Abstract: By comparing software and hardware, the intrinsic and extrinsic factors, and the subjective and objective factors of software failures, the main cause of a software failure was concluded by analyzing the causality of errors in various stages of the software lifecycle.

Key words: software reliability; software failure; cause analysis

1 引言

1.1 问题的提出

当系统功能和性能主要通过软件实现时，系统的研制需要开展软件可靠性设计、软件可靠性保证、软件可靠性测评等工作。目前国内的可靠性工作主要针对基于硬件设备或以硬件设备为主的系统，对于以软件为主的系统，工作开展得很少。在工作中我们发现造成软件失效的原因很多，要开展好软件可靠性工作，必须找到造成软件不可靠的原因即软件失效的原因。

所谓软件失效（software failure），就是指软件出现如下3种情况：1）功能部件执行其功能的能力丧失；2）系统或系统部件丧失了在规定的限度内执行所要求功能的能力；3）程序操作背离了程序要求。

在实际的应用中，软件失效表现为：

1）死机：软件停止输出或软件对输入不发生响应；

2）运行速度不匹配：数据接受（输入）或输出的速度与系统的需求不符；

3）计算精度不够：某一或某些输出参数值的计算精度不合要求；

4）输出项缺损：缺少某些必要的输出值；

5）输出项多余：软件输出了系统不期望的数据/指令。

1.2 软件与硬件的比较

我们对于硬件的可靠性相关问题已经有了一个比较清晰的理解，所以为了分析软件失效的原因，将软件、硬件及其可靠性作一个对比（如表1所示），将有助于问题的解决。

收稿日期：2009-01-07 修回日期：2009-05-11

作者简介：谢瑞生（1965-），男，江西吉安人，中国电子科技集团公司第二十八研究所高级工程师，从事软件开发工作。

表 1 软件与硬件的对比

序号	项目	软件	硬件
1	可变性	是逻辑实体，始终不会自然变化，只是其载体可变。	是物理实体，每件同规格产品的质量特性之间有散布，会随时间和使用而老化、磨损以致失效。
2	可测控性	研制主要是紧张的脑力劳动，本质上无形，看不见，难测控。	不只是脑力劳动，过程有形，便于测控。
3	缺陷形成	不可靠问题基本上是开发过程中人为差错造成的缺陷所引起的。	不可靠问题不只是设计问题，在生产和使用过程中也会产生新的故障。
4	失效形成	程序是指令序列，即使每条指令本身都正确，但在执行时其逻辑组合状态变化万千，不一定完全正确。	硬件失效总是由其零部件或其组合的故障所引起。
5	故障前兆	系统的数学模型是离散的，其输入在合理范围内的微小变化可能引起输出的巨大变化，故障的形成无物理原因，失效的发展取决于输入值和运行状态的组合，无前兆。	系统在正常工作条件下其行为是渐变的，故障的形成和失效的发生一般都有物理原因，有前兆。
6	故障定位	故障难以定位，失效现象往往不在失效部件显现。	故障较易定位，失效部件的物理参数常常发生明显变化。
7	故障排除	惟有重新设计、编码或通过检测排错，才可提高可靠性。	维修可提高系统的功能或提高使用可靠性。
8	失效率分布	失效率随错误排除而下降。	失效率变化如浴盆曲线。
9	可靠性提高	只能通过不同软件冗余来提高软件可靠性，相同冗余不会提高可靠性。	可通过冗余提高系统的可靠性。
10	报废原因	软件报废的主要原因是软件版本的功能已不能满足用户新的需求。	硬件报废的主要原因则是产品经过长时间的使用，已经进入损耗是小气，无法继续正常工作。

由上表可看出，软硬件实效的原因、表现均不相同，下面将具体分析造成软件失效的内外原因与主客原因。

2 失效原因分析

2.1 内在原因

2.1.1 软件生命周期各阶段可能产生的错误

软件生命周期包括需求分析、设计与编码、测试与系统集成、运行维护等阶段。在运行维护阶段软件产品的品质已经形成，造成其失效的原因属于外部原因。

2.1.1.1 需求差错

需求阶段造成的错误叫做需求差错。可能产生的需求差错有：

a）完整性差错

1）使用方提出的用户需求不完整，有遗漏；

2）对需求分析不充分，未完全考虑使用方需求。

b）一致性差错

用户的需求频繁改动以至于无法有效地控制其一致性。

c）理解性差错

需求分析人员误解了使用方的用户需求。

d）潜在性差错

分析人员未能根据用户提出的需求，分析出其潜在的需求。

e）超越性差错

用户提出超过实现能力的需求，分析人员未分析出其不合理性。

需求差错还可能发生在其它阶段，它们是：

1）概要设计没有完全实现需求规范；

2）详细设计没有完全实现概要设计规范；

3）编码没有完全实现详细设计规范；

4）集成测试没有覆盖需求规范。

这些错误虽然不是发生在需求分析阶段，但其实质还是属于需求差错，且大部分属完整性差错。

2.1.1.2 设计差错

需求分析是正确的，也完全遵守了其形成的规格说明，但由于设计上的错误，也有可能造成错误，设计阶段造成的差错叫做设计差错。可能产生的设计差错有：

a）体系结构

软件系统的体系结构不合理。

b）数学模型

错误的数学模型、错误的或不完备的算法。

c）复杂程度

程序的结构化程度不好，程序模块的圈复杂度过大。

d）技术成熟

1）选择了不可靠的模块，如调用的库函数自身存在问题；

2）使用了不成熟、不可靠的软件技术。

e）流程设计

1）逻辑判断错误，如逻辑不完善、判据不当、转移方向错、死循环；

2）调度错误，如控制时序混乱、指挥法则错误、控制方法错误。

f）冗余设计

1）没有容错设计或容错设计不够，缺少异常处理；

2）软件适应性考虑不足，没有留足够的余量，对外部环境要求过于苛刻，如要求时钟频率、与外界交互频度在一定的范围。

2.1.1.3 编码差错

在软件编码阶段产生的差错叫做编码差错，许多编码差错在编译、调试过程中就被发现从而得到解决，以下差错在编译、调试过程中不易被发现：

a）符号错误

1）键入错代码，如用错相同类型、名称相近的变量；

2）键入数值错误，包括常数值错、参数值错，如误将“3.14”写成“31.4”；

3）丢失代码，如少括号、将“==”误写成“=”；

4）使用相同的全程变量名或相同的全程函数名，如两个模块都使用全程变量“int a;”。

b）计算错误

键入错误的表达式，如“(a+b) *c”误写成“a+b*c”。

c）逻辑错误

1）错误的判断条件，如“if (a>b)”误写成“if (a<b)”；

2）错误的循环条件，如“for (int i=0; i<10; i++)”误写成“for (int i=0; i<=10; i++)”；

3）死循环，如“while (a==a)　{…}”。

d）初始化错误

1）变量使用前未初始化；

2）使用未分配内存的空指针。

e）内存操作错误

1）数组读写越界，如“int a [6]; a [8] = 123;”；

2）在某些运行分支，未释放已分配的无用内存。

f）输入输出错误

1）输入输出界面错误，如该用列表框却用了组合框；

2）缺少输入输出完备性检查，或完备性检查错，如编辑框未限制字符长度。

g）接口错误

1）调用模块接口前，没有进行输入参数检查，或检查不完备；

2）调用模块返回后，没有进行输出值检查，或检查不完备。

h）不确定性错误

1）用了可能被零除这样不定值的表达式，如“a=2; b=8/(a-2);”；

2）含有不该有的语句。

2.1.1.4 测试差错

测试期间发生的差错有：

a）错误用例

测试用例过于局限甚至错误，如有 3 项功能，而用例只覆盖其中两项功能。

b）错误数据

测试数据不能反映软件使用的真实环境。

c）错误分析

测试人员对测试结果的错误分析。

2.1.1.5 文档差错

在软件生命周期的各个阶段，都要生成各种技术文档，由于文档问题而导致的软件缺陷叫做文档差错，可能直接导致软件失效的文档差错存在于操作维护手册中，文档差错包括如下情形：

a）完整性差错

文档没有完整地反映应有的内容，有缺项。

b）可操作性差错

文档没有准确地反映应有的内容，过于抽象而不具体、过于具体而没有通用性、文字有偏颇。

c）精确性差错

内容具有二义性，不同的人对文档内容的理解也不同。

2.1.2 软件开发工具对可靠性的影响

软件开发工具的选择对开发出来的软件可靠性影响很大，如 VB、Delphi 等工具是快速应用开发工具，能快速形成软件原型，但其内部包含不可靠

模块，用这些工具开发的软件可靠性相对差，且出错信息多为英文，反之 VC、Java、Ada 等开发工具开发出来的软件，可靠性相对较高。

由于软件开发工具而形成的软件失效，是因为选择了不可靠的模块、使用了不成熟、不可靠的技术，属于软件设计差错。

以上分析了造成软件失效的内部原因，内因对软件的失效起决定性的作用，但是也不能忽视造成软件失效的外部原因，下面将分析引起软件失效的外部原因。

2.2 外在原因

软件失效的外在原因包括安装培训、运行环境、软件使用、软件维护管理等。

2.2.1 安装培训

软件开发方法经历了非结构化程序设计、结构化程序设计、面向对象程序设计、构件化程序设计的发展过程，构件化程序设计方法形成的模块在安装时动态生成用户需要的软件，往往因为如下错误导致软件不能可靠地运行：

a）少装

缺少依赖的软件模块。

b）多装

安装了不必要软件或软件模块，或挤占资源或相互冲突。

c）错装

依赖的软件模块版本不对。

d）错配

软件配置与设置错误。

软件培训时往往因为下述几个方面不到位，可能导致用户不能正确地使用软件，从而造成软件失效。

a）基本概念不明

用户基本概念不对，在使用过程中会造成操作行为与操作目的不符，最终导致软件失效。

b）基本流程不清

基本流程不清，导致错误的操作顺序，最终导致软件失效。

c）注意事项不清

在某种场合不能做或者必须做的操作不清楚，可能导致软件实效。

d）事件不知处置

在软件出现某些状况时，不知道如何正确处置，最终可能导致软件实效。

e）实际训练欠缺

实际操作训练不足，无法将培训知识转化成操作技能，前面四项培训很难达到预定的效果。

2.2.2 运行环境

运行环境是导致软件运行失效的重要外部原因，包括：

a）运行资源欠缺

软件运行资源不满足，如硬盘存储空间、内存、CPU 处理速度不够。

b）运行伙伴竞争

同时运行多个软件，造成运行资源竞争，瓜分了系统的硬盘存储空间、内存、CPU 时间等资源，资源申请失败或延时造成软件失效。

c）运行硬件失效

硬件失效，如由于外界辐射造成造成内存状态改变、CPU 或内存条烧坏；时钟频率、中断频度过高或过低，将诱发适应性差的软件失效。

d）软件环境缺损

操作系统环境遭到破坏，如某些动态库、运行需要的数据被误删。

e）运行数据有误

软件运行使用的数据库或数据文件中的数据错误，导致软件失效。

f）恶意软件破坏

病毒或其它恶意软件，可能破坏软件的运行环境也可能直接破化软件从而造成软件失效。

2.2.3 操作维护

操作导致的软件失效包括：

a）时机错

不该动作时动作，该动作时不动作。

b）操作错

动作时机正确，但动作本身错误。

软件使用过程中，不进行定期维护或没有正确的维护，也可能造成软件失效，具体的情形有以下几种：

a）定时清理不够

软件运行常产生运行状态信息、日志信息、其它过期数据，如不定时清理，将挤占硬盘空间，最

后可能导致软件失效。

b）定时检查不够

软件操作过程中，由于某些误操作，可能改变软件状态或其运行环境，定时检查软件状态和运行环境，可避免由此造成的软件失效。

c）软件配置有误

软件运行过程中，有时可能要重新配置软件，配置修改不当将造成软件失效。

2.3 主观原因

在软件生命周期中，涉及需求人员、设计人员、编程人员、测试人员、维护人员、使用人员，下面分别说明各类人员对软件可靠性的影响。

2.3.1 需求人员

需求人员包括需求提出人员和需求分析人员，需求提出人员一般属于用户方或其委托单位，由于需求提出人员的需求差错，需求提出人员主观上因如下情况产生需求差错：

a）知识能力欠缺

基于知识结构的原因，对软件功能性能产生过多美好愿望，提出不切实际的需求。

b）部门利益考虑

基于自己部门利益考虑，不考虑或少考虑其它部门的需求。

c）表达方式不妥

所使用的专业词汇太多，软件技术人员无法理解。

需求分析人员导致软件失效有如下情形：

a）知识能力欠缺

基于知识结构的原因，不能很好地理解甲方提出的需求。

b）部门利益考虑

怕影响与用户方的关系，不敢拒绝不合理的需求。

c）工作浮躁冒进

急于完成任务，没有对需求进行深入分析。

2.3.2 设计人员

设计人员主观上因为下述原因而导致软件产生缺陷：

a）知识能力欠缺

1）知识陈旧，不敢采用新技术或贸然采用不成熟技术；

2）没用编程经验，“拍脑袋”进行设计，导致设计方案无法实现。

b）工作浮躁冒进

关键技术细节没有解决，就让编程人员开始编程，导致技术状态不稳定。

2.3.3 编程人员

对软件内在品质影响最大的是编程人员，而编程人员出现的差错是隐性的，往往一个模块出现差错，要在另外的模块中得到反映。编程人员造成的差错属于编码差错，主观原因如下：

a）知识能力欠缺

对软件开发工具、需调用的库函数不熟悉。

b）工作浮躁冒进

没有准确理解需求、设计的要求就贸然投入编程。

d）工作不够认真

程序编完后不进行代码走查，只要编译能通过就行；模块编译完后，没有自我进行单元测试就交出去，造成问题隐性累积。

e）生理心理状态

身体疲劳或社会环境造成的心理不稳定因素，导致错误输入。

2.3.4 测试人员

测试因如下主观原因导致软件产生测试差错：

a）工作浮躁冒进

急于短期内完成测试，造成测试工作全面“缩水”。

b）认识程度不够

没有深入了解软件，仅测试软件界面就算完成任务。

c）工作不够认真

不经过测试，就相信编程人员对软件的“理论说明”。

2.3.5 维护人员

软件维护人员往往因为如下原因，导致软件失效：

a）认识程度不够

认为软件是智能化，一切维护都应该能自动进行。

b）知识能力欠缺

未经过操作维护培训，不知道需要哪些维护、如何维护。

c）工作责任欠缺

认为软件维护是软件提供方的工作，有事找软件提供方就行。

2.3.6 操作人员

软件操作人员往往因为如下原因，导致软件失效：

a）认识程度不够

认为软件是智能化，一切错误操作都应该能自动识别而得到处理。

b）知识能力欠缺

未经过操作维护培训，导致错误操作。

c）生理心理状态

身体疲劳或社会环境造成的心理不稳定因素，导致错误操作。

2.4 客观原因

造成软件失效除了人的主观原因外，还有如下客观原因：

a）时间进度紧

有的软件是为应付某种“应急”任务而提出的，没有经过严格的科研程序，在软件生命周期的各个阶段工作都不到位的情况下进入下一个阶段，结果欲速则不达。

b）研制经费少

由于各种原因，有的软件研制经费过少，造成投入的研发力量太小，软件生命周期各阶段的工作也就不能得到有效的保证。

c）问题复杂性

有的软件要解决的问题本身很复杂，难以量化解决，必须在某种假设条件下，对问题进行简化。问题的数学模型往往是连续、非线性、分布参数、非稳态分布，但实际处理时将其简化成离散、线性、集中参数、稳态概率分布的数学模型，在对数学模型求解时也往往是用数值逼近解代替解析解。这些都有可能造成软件在某种状态下的失效。

2.5 因果分析

事物发生变化的根据是事物的内在因素，事物发生变化的条件是事物的外在因素。软件失效的根据是软件的内在因素即软件的品质，软件失效的条件是是软件运行的外在因素即软件的使用和运行环境。软件自身的缺陷是因，是一个静态的概念，存在于软件之中，软件故障是果，是一个动态的概念，在软件的使用过程中表现出来。

a）需求差错因果分析

需求差错主观上在于需求提出和分析人员，客观上在于问题复杂性。其因果关系如图 1 所示。

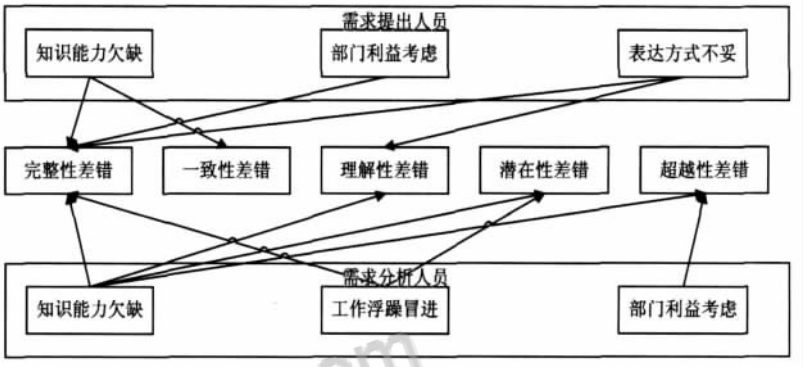

图 1 需求差错主观原因

b）设计差错因果分析

设计差错主观上在于设计人员，客观上在于问题复杂性。其因果关系如图 2 所示。

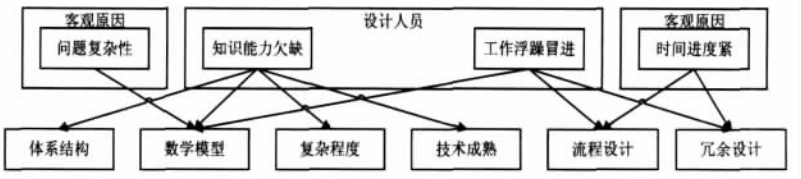

图 2 设计差错原因

c）编码差错因果分析

编码差错主观上在于编程人员，客观上在于研制经费和时间进度，其因果关系如图 3 所示：

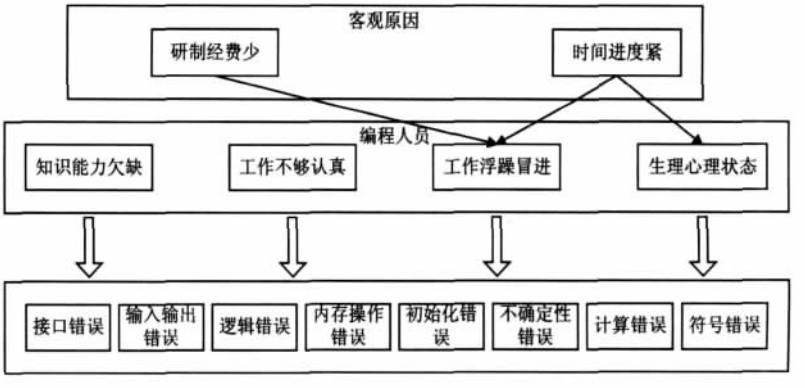

图 3 编码差错原因

d）测试差错因果分析

测试差错主观上在于测试人员，客观上在于问题复杂性、研制经费和时间进度，其因果关系如图 4 所示：

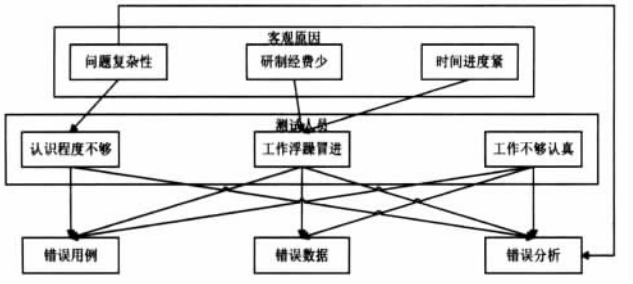

图 4　测试差错原因

f）文档差错因果分析

文档差错主观上在于需求分析人员、设计人员、编程人员，客观上在于研制经费和时间进度，其因果关系如图 5 所示：

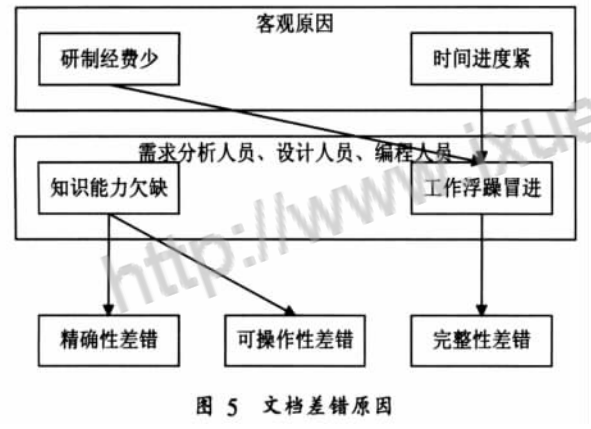

图 5　文档差错原因

g）软件失效因果分析

通过软件失效的内部原因分析，可以得出软件失效的因果关系如图 6 所示。

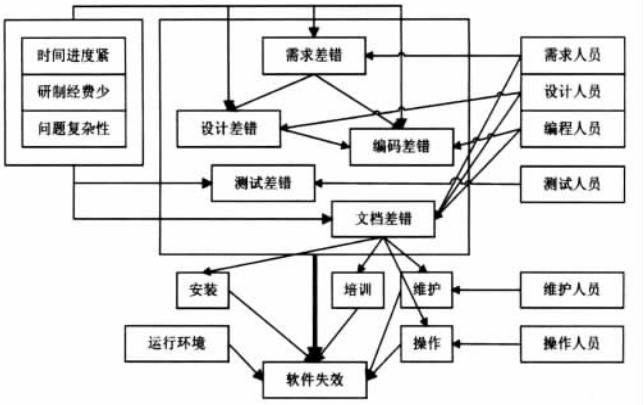

图 6　软件失效原因

3　结束语

从以上分析不难看出，软件是由人开发的，软件也是由人操作使用的，人不可避免地会犯各种错误，人所犯的各种错误造成了软件失效，人是软件失效的第一原因。

参考文献：

[1] 徐仁佐. 软件可靠性工程 [M] . 北京：清华大学出版社，2007.

[2] 黄锡滋. 软件可靠性、安全性与质量保证 [M] . 北京：电子工业出版社，2002.

[3] 何国伟，王玮. 软件可靠性 [M] . 北京：国防工业出版社，1998.

[4] 徐仁佐，谢旻，郑人杰. 软件可靠性模型及应用 [M] . 北京：清华大学出版社；南宁：广西科学技术出版社，1994.

[5] 赵晓华. 计算机软件可靠性与质量管理 [M] . 北京：中国经济出版社，1992.

信息与动态

Allegro Systems 公司发布一款全新宽输入电压 2 A 降压稳压器

2009 年 4 月 15 日，美国马萨诸塞州伍斯特市的 Allegro MicroSystems 公司发布一款 2 A 固定关断时间、电流模式控制型反向开关稳压器——A4447，进一步扩展了其当前的降压稳压器系列。该通用反向稳压器主要面向消费电子、办公自动化和工业市场，如消费设备功率、不间断电源、12 V 轻功率应用（便携 DVD 等），带高电压保护的汽车 12 V 或 24 V 输入应用，打印机应用和带 24 V 或 36 V 总线的工业应用。8~ 50 V 的输入范围使其在输入电压范围较宽的应用中成为理想之选。

该稳压器需要一个外部箝位二极管、感应器和滤波电容器。它的停机时间取决于外部电阻器，可在连续和间断模式下操作。由于外部箝位二极管的反向恢复，内部消隐电路将用于过滤瞬态电流。典型的消隐时间为 200 nS；基于电阻分配器和 0.8 V ±3 % 参考值，输出电压可在 0.8~ 24 V 的范围内调整。采用 eSOIC-8L 封装。

（本刊讯）

阅读此文的还阅读了：

1. 中国证券市场惩戒机制失效的具体表现与原因分析
2. 20000m~3外浮顶罐浮盘及支柱失效分析
3. 浅析断齿失效与混晶的产生原因
4. 螺杆泵采油井杆柱断脱机理及其对策
5. 斯蒂格利茨：市场引导创新的失效的原因
6. 高中政治课探究“失效”的原因及对策
7. 浅析企业内部会计监督制度
8. 高职高专医学院校医德教育失效的原因分析
9. 国产加压钢板治疗股骨干骨折失效原因及防治
10. 软件可靠性与硬件可靠性异同分析
11. 500kV输电线路铁塔横担变形材质检测及失效分析
12. 微机软磁盘失效的原因及其数据挽救
13. 12V240ZJ型柴油机凸轮轴承失效原因及解决措施
14. 浅析四_2区部分浅层稠油井酸化失效原因及防治措施
15. 中国证券市场的惩戒机制失效的具体表现与原因分析
16. 关于内燃机车高温部位螺纹连接失效的分析和改进的探讨

17. 中国证券市场惩戒机制失效的具体表现与原因分析

18. 高温过热器失效原因分析及处理

19. 渔药失效的原因分析

20. 油气管道的故障树分析

21. 油气管道的故障树分析

22. 对国家房价调控失效问题的探讨

23. 分注管柱失效原因分析及治理对策探讨

24. 浅析电梯限速器-安全钳联动试验失效

25. 往复式压缩机阀片弹簧失效原因分析与改进

26. 降膜蒸发器的失效分析与预防

27. “罗森塔尔效应”失效的原因

28. 一起紧急切断阀失效的原因分析

29. 股票期权激励失效的原因分析

30. 基于高效换热器换热管失效原因分析及预防措施

31. 乳化液泵曲轴连杆机构的失效分析

32. 连续油管故障树的建立与分析

33. 让对方看不见你的视频

34. 静态平面O形橡胶圈密封失效原因与选型设计

35. 内燃机车柴油机轴瓦失效的原因分析与预防措施

36. 锚索桩锚索失效原因分析及治理措施

37. 电梯超载保护装置失效原因分析及处理

38. 钢轨联接件鱼尾板的失效原因与分析

39. 不会失效的代理服务器Tor

40. 升级XP后媒体播放器全部失效

41. 可调限位板的分析与应用夹片式锚具锚固失效原因及对策分析

42. T检验失效的原因及处理

43. 试论我国企业激励机制失效的原因与对策分析

44. 软件失效原因分析

45. 砂岩油田部分油水井酸化失效的原因及防治

46. 降膜蒸发器的失效分析与预防

47. 不要只盯着离合器——引起离合器失效的外部原因

48. 轴类机械密封失效的原因与对策

49. φ95mm有杆抽油泵失效分析及预防措施

50. 液压启闭闸门失效事故原因分析总结