计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2019,28(2):158−163 [doi: 10.15888/j.cnki.csa.006779]
©中国科学院软件研究所版权所有.
E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

SFMEA 安全性分析技术在软件安全性测试中的应用①

张　峰[1], 李亚伟[2]

[1](91404 部队, 秦皇岛 066001)
[2](北京赛迪软件测评工程技术中心有限公司, 北京 100048)
通讯作者: 李亚伟, E-mail: lyw@cstc.org.cn

摘　要: 随着软件在现代高可靠性装备中的比重和关键程度越来越高, 传统的软件安全性测试方法已经不能满足当前测试要求, 本文主要介绍一种新的安全性测试分析思路和方法——SFMEA 技术在软件安全性测试中的应用, 以弥补安全性测试需求分析和测试用例设计不足问题. 文章首先分析介绍了常规安全性测试内容和方法及其不足, 同时分析说明了引入新的安全性测试方法的必要性, 然后介绍了 SFMEA 安全性分析技术相关定义、方法以及流程等, 最后结合实例详细描述了基于 SFMEA 安全性分析技术的软件安全性测试方法与工作流程, 并对基于 SFMEA 安全性分析技术进行安全性测试工作优缺点以及重点关注内容进行了总结.

关键词: 软件测试; 安全性测试内容; 安全性测试方法; FMEA; SFMEA

引用格式: 张峰,李亚伟.SFMEA 安全性分析技术在软件安全性测试中的应用.计算机系统应用,2019,28(2):158–163. http://www.c-s-a.org.cn/1003-3254/6779.html

Application of SFMEA Safety Analysis Technology in Software Safety Testing

ZHANG Feng[1], LI Ya-Wei[2]

[1](No. 91404, Troops of PLA, Qinhuangdao 066001, China)
[2](Beijing CCID Software Test Engineering Technology Center Co. Ltd., Beijing 100048, China)

Abstract: With the increasing proportion and key degree of software in modern high reliability equipment, the traditional software safety testing methods cannot meet the requirement of current testing. This paper mainly introduces a new method of safety testing and analysis—the application of SFMEA technology in software safety testing, to make up for the deficiency of safety testing requirement analysis and test case design. The article first analyzes and introduces the contents, methods, and shortcomings of the conventional safety test. At the same time, it analyzes the necessity of introducing a new safety test method, and then introduces the definition, method, and process of SFMEA safety analysis technology. Finally, the software based on SFMEA safety analysis technology is described in detail. The safety testing method and workflow of the piece are introduced, and the merits and demerits of safety testing based on SFMEA safety analysis technology and the focus of attention are summarized.

Key words: software testing; safety testing content; safety testing methods; FMEA; SFMEA

1　引言

随着软件在高可靠性领域产品中的比重逐步提升, 因软件缺陷导致的安全事故也层出不穷, 例如 1999 年美国 NASA 制造的火星气候轨道探测器因为单位使用错误缺陷导致探测器坠毁, 2011 年 7·23 中国高铁甬温线因信号设备设计缺陷引发追尾重大事故, 2016 年日

① 收稿时间: 2018-08-02; 修改时间: 2018-08-30, 2018-09-18; 采用时间: 2018-09-26; csa 在线出版时间: 2019-01-28

© 中国科学院软件研究所 http://www.c-s-a.org.cn

本 X 射线天文卫星因底层软件飞行姿态失控状态调整缺陷导致卫星彻底失控等等. 为防止因为软件缺陷导致重大安全事故发生, 人们做了大量的安全防护工作, 包括研制阶段安全性需求分析设计论证工作以及研制测试阶段的安全性测试工作, 很多问题事后证明是软件设计缺陷, 但在测试阶段仍存在被发现的可能.

目前在各类型软件尤其航空航天、工业控制等高可靠性软件研制过程中, 软件安全性测试工作越来越受重视, 相关技术标准体系已经非常成熟, 安全性测试工作过程也受到了全过程监督审查, 可因为软件设计缺陷且测试不够充分而引发的安全事故频发, 损失惨重.

因此, 一方面当前社会要求加强软件安全性需求分析和设计工作, 另一方面也对软件安全性测试工作提出了更高要求. 本文旨在介绍一种新的安全性测试分析思路和方法, 以提高软件安全性测试质量.

2 常规软件安全性测试方法概述

2.1 常规软件安全性测试内容

安全性测试是检验软件中已存在的安全性、安全保密性措施是否有效的测试, 其一般包括内容见表 1[1].

表 1 常规安全性测试内容

序号	安全性测试内容
1	安全性功能验证测试, 测试软件的安全功能实现是否与安全需求一致.
2	异常处理能力测试, 从攻击/破坏者的角度, 以发现软件的安全缺陷. 包括对异常条件下系统/软件的处理和保护能力的测试、对输入故障模式的测试; 安全性关键的操作错误的测试; 对具有防止非法进入软件并保护软件的数据完整性能力的测试; 对重要数据的抗非法访问能力的测试等.

2.2 常规安全性测试方法不足

安全性测试目的是验证软件规定的安全性需求是否都实现, 安全保护措施是否有效, 是否具备因某部件或者功能失效而不引起系统发生事故的能力. 常规安全性测试方法在一定程度上可以对软件安全性进行检测, 但是也存在部分不足之处, 主要体现在以下几个方面:

(1) 一定程度上对软件安全性需求和设计的质量有很大依赖性;

(2) 测试的覆盖程度不能保证, 测试的样本有限, 从而不能保证测试的深度和广度;

(3) 对测试人员个人经验和能力要求很高, 测试质量不能保障;

(4) 对测试工具质量要求比较高, 工具在一定程度上无法保证对运行平台和业务逻辑的通用性, 因此不能保证测试充分性.

针对以上问题可以看出, 当前的安全性测试工作已经不能满足安全性我们需要更完善的方法体系来保证安全性测试的充分性, 以保障软件安全可靠性.

2.3 软件安全性测试引入安全性分析方法必要性

软件安全性测试仅是验证软件安全性需求和设计措施有效的过程和手段, 软件的安全可靠性需要由软件安全性设计来保障, 安全可靠性需求的质量一定程度上决定了软件安全性测试的质量. 然而实际现状是在很多高安全可靠性领域软件工程化生产管理方面, 对软件安全性分析重视程度较低, 普遍在需求和分析阶段没有进行更深入安全性分析, 因而在测试阶段也就无法有更充分的依据来进行安全性测试用例设计. 因此在当前阶段对软件安全性测试提出了更高要求, 在安全性需求无法保障情况下, 有必要在测试阶段, 基于被测软件的需求和设计进行安全性分析工作并进行安全性测试用例设计, 以提高软件安全性测试质量.

在软件安全性测试过程中, 引入 SFMEA(软件潜在失效模式及后果分析) 技术进行安全性测试需求分析, 可以提高软件安全性测试充分性.

3 SFMEA 安全性分析方法

3.1 SFMEA 安全性分析定义

FMEA 全称“Failure Mode and Effects Analysis”, 即“潜在失效模式及后果分析”, FMEA 方法主要应用于一般工业产品过程设计阶段, 对产品构成的部件或零件在过程阶段的各个工序逐一进行分析, 找出所有可能的失效模式, 并分析因为失效带来的后果, 从而采取必要的预防措施, 以保证产品的质量和可靠性. SFMEA(软件潜在失效模式及后果分析) 安全性分析技术是 FMEA 的扩展, 用于软件安全可靠性分析与设计的一种自底向上的分析方法, 以失效模式为基础, 以软件失效对系统或者软件的影响或后果为核心, 分析系统或者软件设计架构层次, 进行因果关系推理和归纳

© 中国科学院软件研究所 http://www.c-s-a.org.cn

总结, 以识别软件设计的薄弱环节, 提出改进措施和建议, 以保障软件产品的质量[2–4].

目前 SFMEA 安全性分析方法广泛应用于高可靠性领域的软件研发设计阶段, 也有学者提出在可靠性测试领域以 SFMEA 故障模型推动软件测试用例设计.

3.2 SFMEA 安全分析工作内容与方法

SFMEA 分析方法与一般产品设计 FMEA 基本相同, 如图 1 所示.

(1) 首先确定系统分析对象级别和分范围. 通常根据软件需求规格等相关文档, 分解系统或者软件需求, 确定分析级别和对象.

(2) 确定分析对象的失效模式及其原因. 针对分解后的分析对象, 分析其所有可能的失效模式. 软件失效模式包括功能失效模式和性能失效模式, 一般功能失效模式为主, 找出关键软件缺陷, 形成软件关键功能失效模式集合, 并针对每一种失效模式分析其可能的失效原因.

(3) 分析失效影响及其严重性. 根据软件失效可能带来的风险进行分析, 并根据风险严重程度确定失效严重等级. 严重程度一般分为严重、一般和建议三个级别.

(4) 提出预防措施建议. 对每一个失效模式产生的影响和失效原因, 提出相应预防措施及修改建议, 形成完整的 SFMEA 表[2–4], 见图 1.

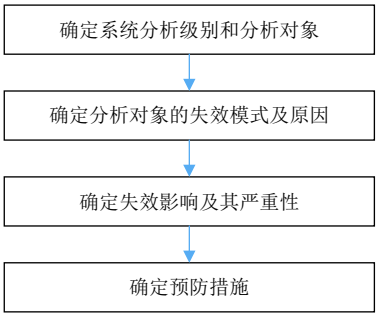

图 1 SFMEA 分析流程

如对某制冷设备进行 SFMEA 安全性分析结果如表 2.

表 2 SFMEA 安全性分析结果表

编号	需求	失效模式	失效原因	失效影响	严重性	预防措施
1	温度控制功能	软件遗漏了当输入温度>500 时相应处理	输入温度取值为 600 时, 软件输出值–1, 不进行制冷	将可能导致系统超温	严重	补充需求:输入温度>500 时进行制冷处理, 并进行告警
2	温度控制功能	软件遗漏了当输入温度从正常值变化到小于下限时相应处理	当输入温度从>=0 变化到<0 时, 软件仍输出为进行制冷	违法逻辑, 将可能导致造成设备磨损和浪费	一般	补充需求: 当输入温度<0 时, 输出为–1, 不进行制冷

4 基于 SFMEA 安全性分析技术进行软件安全性测试分析方法

4.1 基于 SFMEA 安全性分析方法进行安全性测试工作步骤

依据软件测试的常规测试流程, 基于 SFMEA 安全性分析方法进行软件安全性测试工作流程如图 2 所示.

(1) 安全性测试需求分析. 在软件测试需求分析和策划阶段, 依据 SFMEA 安全性分析方法, 按照图 1 安全性分析流程进行安全性测试需求分析, 对被测系统和软件安全关键业务和模块生成 FMEA 失效模式表, 明确安全性测试内容;

(2) 安全性测试用例设计. 基于安全性分析 FMEA 失效模式表进行测试用例设计;

(3) 安全性测试执行. 依据安全性测试用例执行测试, 在测试过程中根据需要调整或者补充 FMEA 表及测试用例, 对测试发现的安全性问题分析原因并提出改进建议, 并进行回归测试;

(4) 安全性测试总结. 在测试执行完毕后对测试过程和测试结果进行总结, 对安全性问题进行分析, 对软件安全性进行评估[5].

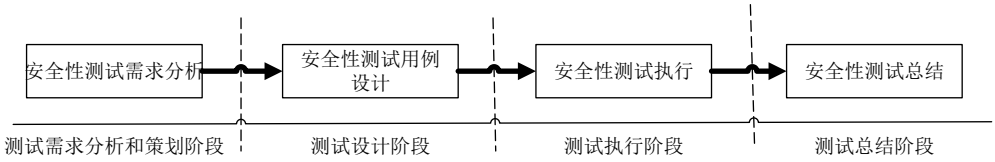

图 2 基于 SFMEA 安全性分析技术进行安全性测试步骤

© 中国科学院软件研究所 http://www.c-s-a.org.cn

4.2 基于 SFMEA 分析方法的安全性测试重点关注内容

测试重点关注内容如表 3.

表 3 基于 SFMEA 分析方法的安全性测试重点关注内容

编号	重点关注内容
1	重点关注系统、子系统和低一级功能级所执行功能和相联系的潜在失效上
2	重点关注系统之间、子系统之间信息交换接口失效情况
3	将测试对象系统结构化, 并分解成系统单元, 并说明各单元间的功能关系
4	从已描述的功能中分析每一系统单元的可想象的失效功能(潜在缺陷)
5	确定不同系统单元失效功能间的逻辑关系, 以便能在系统 SFMEA 中分析潜在的缺陷、缺陷后果和缺陷原因
6	当设计发生重大更改时应对涉及的单元重新进行系统 SFMEA

5 SFMEA 安全性分析技术的在安全性测试中的应用实例

据媒体报道: 2018 年 1 月 1 号刚开通三天的北京有轨电车西郊线发生重大事故. 事故原因是车辆发生故障后未按规定摘挡, 动力手柄未按规定回位, 仍位于前进动力位置, 导致故障恢复后, 车辆突然窜出并脱轨. 之后调了大型起重机到达现场把列车吊回了轨道. 列车成功被吊回轨道. 结果还是没有人想到要摘挡, 列车在车内无司机, 手柄位于前进动力的情况下, 直接从香山加速下山放飏, 溜车 6 公里后, 由于电流过大启动过热保护, 车辆在隧道内自动停车. 本文以此事故为例进行安全性测试分析工作, 分析基于 SFMEA 安全性分析方法进行安全性测试可以检测并发现哪些安全问题, 是否可以避免事故的发生.

5.1 软件需求

根据案例分析, 假设车辆控制系统在车辆动力控制方面有如下需求 (不考虑刹车控制):

(1) 输入:

1) 动力手柄信号: 无动力 (00), 前进动力 (01), 后退动力 (10), 故障 (11).

2) 车辆运行状态: 停止 (00)、前进 (01)、后退 (10) 故障停车 (11).

(2) 输出: “动力控制电流”: 无输出 (0), 有输出 (100).

(3) 软件处理需求:

1)“状态字”=前进状态 (01) 或后退状态 (10), 且“动力手柄信号”=01 时, 输出“动力控制电流”=100; 车辆开始前进.

2)“状态字”=前进状态 (01) 或后退状态 (10), 且“动力手柄信号”=10 时, 输出“动力控制电流”=100; 车辆开始后退.

3)“状态字”=前进状态 (01) 或后退状态 (10), 且“动力手柄信号”=11 时, 输出“动力控制电流”=0; 车辆故障停车.

4)“状态字”=故障停车 (10) 时, 输出“动力控制电流”=0; 即车辆保持停止.

5)“状态字”=停止状态 (00), 输出“动力控制电流”=0; 即车辆保持停止.

5.2 测试需求分析

根据以上需求, 对软件运行状态进行分析, 软件运行状态转换图如图 3 所示.

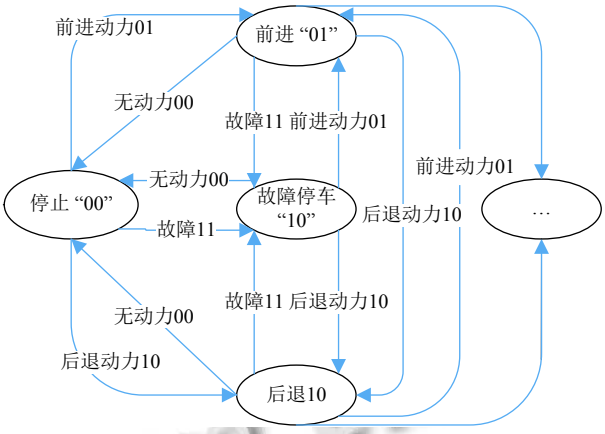

图 3 车辆运行状态转换图

根据车辆动力控制部分需求和以上运行状态图, 按照 SFMEA 安全分析方法, 对其在状态转换期间的可能存在的失效模式进行分析, 如表 4 所示.

以上仅分析在车辆动力控制部分可能失效情况, 读者可以依据此方法进行更深入分析. 在实际情况中, 根据系统复杂程度, 可能存在的失效情况比该实例多很多.

5.3 测试用例设计

根据表 3 安全性分析表, 针对以上安全性分析设计相应测试用例. 以表 4 中第 6、7 种失效模式为例设计测试用例, 设计安全性测试用例如表 5.

同理, 根据表 3 安全性分析结果可以设计其它 8 种失效模式的安全性测试用例, 分别进行相关安全性测试.

© 中国科学院软件研究所 http://www.c-s-a.org.cn

表 4 车辆状态控制失效模式分析表

编号	状态转换	失效模式	失效可能原因	失效影响	严重性	预防措施
1	正常停车->上电	正常停车状态上电失败	硬件故障, 加电失败软件初始化失败, 上电失败	车辆不能正常上电, 无法启动运行	一般	实时监测系统硬件故障并告警, 软件初始化过程中监测异常并报警
2	正常停车->上电	上电后车辆异常前进	动力手柄处于前进动力位置, 软件初始化功能失效, 未判断当前动力手柄信号是否处于无动力状态并作出启动限制	车辆异常前进, 可能造成重大事故	严重	软件初始化时检测动力手柄信号是否为无动力状态并作出限制处理
3	正常停车->上电	上电后车辆异常后退	动力手柄处于后退动力位置, 软件初始化功能失效, 未判断当前动力手柄信号是否处于无动力状态并作出启动限制	车辆异常后退, 可能造成重大事故	严重	软件初始化时检测动力手柄信号是否为无动力状态并作出限制处理
4	故障停车->上电	车辆故障停车状态下上电后异常前进	动力手柄处于前进动力位置, 软件初始化功能失效, 未判断当前动力手柄信号是否处于无动力状态并作出启动限制	车辆异常前进, 可能造成重大事故	严重	软件初始化时检测动力手柄信号是否为无动力状态并作出限制处理
5	故障停车->上电	车辆故障停车状态下上电后异常后退	动力手柄处于前进动力位置, 软件初始化功能失效, 未判断当前动力手柄信号是否处于无动力状态并作出启动限制	车辆异常后退, 可能造成重大事故	严重	软件初始化时检测动力手柄信号是否为无动力状态并作出限制处理
6	停车上电->启正	正常停车上电后启动前进失败	1、硬件故障, 获取软件前进动力信号后启动失败 2、软件输出前进动力信号失效	车辆前进失败, 处于停车状态	严重	实时监测系统硬件故障并告警, 软件根据设备状态进行状态监测并告警
7	停车上电->启动	正常停车上电后启动后退失败	1、硬件故障, 获取后退动力信号后启动失败 2、软件输出后退动力信号失效	车辆后退失败, 处于停车状态	严重	实时监测系统硬件故障并告警, 软件根据设备状态进行状态监测并告警
8	停车上电->启动	正常停车上电启动运动方向错误	硬件故障, 获取正确启动方向信号后运动方向错误软件输出运动方向控制指令错误	车辆运行方向错误	严重	实时监测系统硬件故障并告警, 软件根据设备状态进行状态监测并告警
9	正常前进	前进过程中异常停车	1、系统硬件故障, 执行软件指令失效 2、软件动力控制输出失效	车辆失去前进动力, 异常停车	一般	实时监测系统硬件或者软件故障并告警, 启动紧急制动
10	正常后退	后退过程中异常停车	1、系统硬件故障, 执行软件指令失效 2、软件动力控制输出失效	车辆失去后退动力, 异常停车	一般	实时监测系统硬件或者软件故障并告警, 启动紧急制动
---	---	---	-----	---	---	---

表 5 测试用例

编号	用例名称	输入及操作步骤	预期输出
CS-6	车辆故障停车状态下异常前进	设置车辆处于故障停车状态 (=10); 设置动力手柄处于前进动力 (01) 状态; 系统上电	检测到在故障停车状态下, 动力手柄未处于无动力 (00) 状态, 系统启动失败并告警
CS-7	车辆故障停车状态下异常后退	设置车辆处于故障停车状态 (10); 设置动力手柄处于后退动力 (10) 状态; 系统上电	检测到在故障停车状态下, 动力手柄未处于无动力 (00) 状态, 系统启动失败并告警

5.4 测试执行结果

执行表 5 中 2 个测试用例结果可检测并发现系统的一个重要安全问题: 软件上电初始化模块设计存在重大缺陷, 在车辆初始化时, 未检测动力手柄是否处于无动力 (=00) 状态, 当动力手柄处于前进动力 (01) 或者后退动力 (10) 状态时未提出告警并限制车辆启动, 存在车辆失控运动风险.

同理设计并执行其它 8 类失效模式安全性测试用例, 也以检测软件是否存在其它的安全风险, 包括多种严重级别的安全隐患问题. 这其中部分问题我们可以通过常规安全性测试方法进行验证, 但是不能保证常规安全性测试方法进行的安全性测试用例能够覆盖表 4 中的各种失效风险问题, 这就是基于 SFMEA 技术进行安全性测试分析与常规安全性测试的差异.

6 总结

SFMEA 与软件产品正向设计流程不同, 它是一个典型的思维发散过程, 其核心是尽可能完整和正确地分析总结软件的失效模式. 其关注重点不在于产品“能干什么”, 而是产品“可能怎么坏掉”. 软件安全性测试

© 中国科学院软件研究所 http://www.c-s-a.org.cn

核心也是检验软件整体或者部分在“坏掉”情况下是否进行了预期判定和有效处理.

本文仅是以此为例介绍一种在软件安全性测试过程中进行安全性测试需求分析的方法. 在软件设计开发已经完成且不具备明显的安全性需求情况下, 与常规安全性测试采用的非法输入操作、猜错法等方式不同, 该方法采取的是一种逆向思维方法, 以系统方法逆向分析系统各种失效的可能性及带来的风险影响, 从而推进安全测试用例设计, 更大程度上保证了安全性测试充分性.

但 SFMEA 安全性分析方法在一定程度上存在工作量大、成本高、复杂程度高等特点, 所有在实际应用中, 应根据项目进度、规模等选择性进行, 针对系统中安全关键业务及模块进行安全性分析和测试. 同时也需要根据被测软件特点, 结合其他安全性测试方法, 综合其优缺点进行测试方法选择, 以更好地保证被测软件安全性测试工作的质量、进度以及成本等合理进行.

参考文献

1 侯海燕, 符志鹏. 软件安全性检测技术综述. 电脑知识与技术, 2014, 10(25): 5847–5841, 5854.

2 吴邦国, 唐任仲. 软件 FMEA 技术研究. 机电工程, 2004, 21(3): 8–12. [doi: 10.3969/j.issn.1001-4551.2004.03.003]

3 王思琪, 黄志球, 黄传林, 等. 一种基于状态事件故障树的软件安全性分析方法研究. 小型微型计算机系统, 2016, 37(1): 12–17. [doi: 10.3969/j.issn.1000-1220.2016.01.002]

4 施寅生, 邓世伟, 谷天阳. 软件安全性测试方法与工具. 计算机工程与设计, 2008, 29(1): 27–30.

5 冯瑞, 曹宁. 基于 SFMEA 的综合导航系统软件安全性分析. 科技视界, 2015, (20): 57–58. [doi: 10.3969/j.issn.2095-2457.2015.20.041]

© 中国科学院软件研究所 http://www.c-s-a.org.cn