系统级软件FMEA计算机辅助设计研究

曾福萍 杨顺昆 陆民燕
(北京航空航天大学工程系统工程系 北京 100191)

摘 要 软件失效模式和影响分析(SFMEA)是提高软件可靠性的一种重要方法。针对人工SFMEA分析费时费力的问题,着眼于SFMEA的分析过程,对系统级SFMEA计算机辅助设计及相应辅助工具的实现展开了研究,介绍了系统级SFMEA分析的具体步骤,提出了对软件功能单元建模辅助生成软件约定层次,由已有通用失效模式库和相邻层次分析结果辅助获取软件失效模式、软件失效原因和纠正措施辅助设计等,并在此基础上开发了相应的辅助工具,从而减少SFMEA的分析工作量,提高SFMEA分析的效率。

关键词 计算机辅助设计,软件失效模式和影响分析,系统级软件FMEA,失效模式
中图法分类号 TP311 **文献标识码** A

Study on Computer Aided Design for System Software FMEA

ZENG Fu-ping YANG Shun-kun LU Min-yan
(Department of System Engineering of Engineering Technology, Beihang University, Beijing 100191, China)

Abstract Software failure modes and effects analysis(SFMEA for short) is a important method to improve software reliability. To solve the time-consuming problem of the artificial SFMEA, with a view to the SFMEA's process, the research on system SFMEA computer aided design and corresponding tool were carried out, the specific steps of the system SFMEA were introduced, the aided design methods as follows were advanced: the software conventional level was made by modeling the functional unit; the software failure mode was acquired from the existent failure mode and the analysis results of the adjacent level; the software failure cause and corrective measures were designed, and the corresponding tool was developed to reduce the system SFMEA's workload and improve the system SFMEA's efficiency.

Keywords Computer aided design, Software failure modes and effects analysis, System SFMEA, Failure mode

软件失效模式和影响分析(Software Failure Modes and Effects Analysis,简称SFMEA)是一种自底向上的软件可靠性分析方法,通过识别软件失效模式,分析造成的后果,研究分析各种失效模式产生的原因,寻找消除和减少其有害后果的方法,以尽早发现潜在的问题,并采取相应的措施,从而提高软件的可靠性和安全性。根据SFMEA分析对象的不同,一般可将SFMEA分为两个层次,即系统级SFMEA和详细级SFMEA。SFMEA自1979年由Reifer提出之后,近30年来,SFMEA的研究和应用主要集中在嵌入式软件中安全关键领域,如军用产品、汽车业等,还未得到普遍的应用。究其根本原因是人工SFMEA分析过程繁琐,进行SFMEA工作需要耗费大量时间、人力和物力,因此阻碍了应用的步伐。为了解决这个问题,SFMEA的自动化辅助工具的开发已经开展研究[1,2],Tribble在实验报告[3]中提到了如何借助辅助技术实现分析的自动化,但是SFMEA的计算机辅助研究还处于摸索阶段,目前仍然没有开发出适用的工具;目前国内对FMEA计算机辅助研究主要针对硬件方面[6-8],对软件FMEA的计算机辅助及其工具研究很少。因此对系统级SFMEA的计算机辅助设计及相应辅助工具的实现展开研究是很有意义的,本文提出了功能单元建模、失效模式描述和失效原因等系统级辅助设计方法并开发了相应的辅助工具,有着很强的工程意义。

1 系统级SFMEA实施步骤

系统级SFMEA的分析对象是开发早期阶段的高层次的子系统或部件,应该在开发过程的早期阶段开始实施,一般从软件的需求分析展开,并分别在软件需求分析、概要设计阶段进行系统级SFMEA,这样有助于发现软件设计的薄弱环节和缺陷,参照分析提出的改进措施及时修改这些缺陷使软件达到可靠性、安全性要求。另外可以通过系统级SFMEA找出影响系统失效的关键模块,可以作为一种展开详细级SFMEA模块确定的依据。系统级SFMEA分析主要包含:软件约定层次、软件失效模式、软件失效原因和软件失效影响等几个要素:

(1)软件约定层次:根据SFMEA的需要,按功能关系或组成特点确定SFMEA的软件功能层次或结构层次;

到稿日期:2008-10-28 返修日期:2009-01-07 本文受总装十一五预研项目(No:513190702)资助。
曾福萍(1977-),女,硕士,讲师,主要研究方向为软件可靠性工程、软件测试,E-mail:zfp@buaa.edu.cn;杨顺昆(1978-),男,博士,主要研究方向为软件测试、故障诊断;陆民燕(1963-),女,教授,博士生导师,主要研究方向为软件可靠性测试技术、软件可靠性度量、软件可靠性设计分析、软件可靠性设计管理等。

(2)软件失效模式:指软件失效的不同类型,通常用于描述软件失效发生的方式以及对设备运行产生的影响;

(3)软件失效原因:指造成软件失效模式的各种可能因素,除了软件缺陷,还包括人为、环境等多种因素;

(4)软件失效影响,指软件失效模式对软件系统的运行、功能或状态等造成的后果。

系统级 SFMEA 一般在软件开发的需求分析、概要设计阶段进行,根据分析对象的特点,可将系统级 SFMEA 分析的具体步骤进一步定义为:

(1) 定义软件约定层次:绘制软件功能流程图,将功能流程图中的每一个功能单元等同于硬件系统中的一个元件,即为软件的约定层次;

(2)分析每个功能单元的各种失效模式;

(3)区分各种失效模式可能的失效原因、失效影响及其严重性,有针对性地提出纠正措施,填写如表 1 所列的 SFMEA 工作表格;

(4)编写系统级 SFMEA 报告,并随着工作的进展不断充实、更新其内容。

根据系统级 SFMEA 结果,对软件需求和概要设计进行修改,并反复进行系统级 SFMEA 直到设计满足软件可靠性和安全性要求。

表 1 SFMEA 工作表格

编号	单元	功能	失效模式	可能的失效原因	失效影响			严重性	改进措施
					局部影响	高一层次影响	最终影响		
1.1	输出	输出数据提交用户显示	数值高于正常范围	逻辑问题、计算问题、数据操作问题	N/A	影响输入值的正确性	任务出错	重要	…
1.x	x	x	x	x	x	x	x	x	…

2 系统级 SFMEA 辅助设计

系统级 SFMEA 辅助设计从其分析步骤着手,通过图形化的方式辅助绘制功能流程图,对每一个功能单元建模,确定软件的约定层次,在此基础上引导完成失效模式、失效原因、失效影响及纠正措施,具体来讲,系统级 SFMEA 辅助设计包括软件约定层次、软件失效模式及软件失效原因和纠正措施等。

2.1 软件约定层次辅助设计

由系统级 SFMEA 的分析步骤可知,软件的约定层次一般为功能流程图中的某个功能单元,所以为了更好地确定软件的约定层次,可以通过图形化方式辅助绘制软件功能流程图,同时对功能流程图中的每一个功能单元建模。

功能流程图中的每一个功能单元的建模信息包括基本信息和关联信息两部分,如图 1 所示。功能单元基本信息又包括功能单元名称、输入变量集合、输出变量集合和处理过程描述集合 4 部分内容;功能单元关联信息包括上一层功能单元集合和下一层功能单元集合。

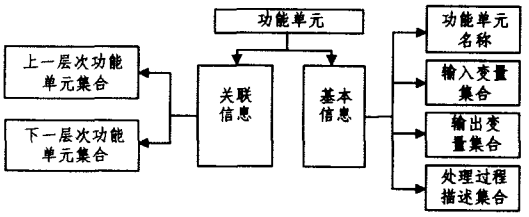

图 1 功能模型组成示意图

定义 功能单元模型是一个六元组 $\psi=(N,I,O,P,L,Q)$,其中:

(1)N 是功能单元的名称,能唯一标识这个功能单元,且不为空值;

(2)I 是功能单元的输入变量集合,非空,集合中的每个变量又分别是一个变量模型,变量模型包括变量 ID、变量名称、变量类型;

(3)O 是功能单元的输出变量集合,其属性与输入变量 I 相同;

(4)P 是处理过程描述集合,一个功能的处理过程可能用到的一些关键性处理。例如功能单元处理用到的"中断"等关键性描述词汇;

(5)L 是功能单元的上一个层次功能单元集合,当功能单元不是最顶层功能单元时,L 非空,即非顶层的功能单元至少有一个上一层次的功能单元;而当该功能单元为最顶层功能单元时,L 为空;

(6)Q 是功能单元的下一个层次功能单元集合,当功能单元不是最底层功能单元时,Q 非空;而当该功能单元为最顶层功能单元时,Q 为空。

例如:某教师评价系统软件中"添加教师"的功能需求描述如图 2 所示。

a. 输入
- ✧ 姓名;
- ✧ 性别;
- ✧ 所在系;
- ✧ 课程备注。

b. 输出
- ✧ 当输入数据符合要求时,在数据库中添加一条记录并在图形用户界面中能够显示;
- ✧ 当输入数据不符合要求时,在图形用户界面中给出出错提示。

c. 处理

对教师进行添加操作。

图 2 教师评价系统软件某一功能需求

则"添加教师"功能单元定义如下:

(1) $N=${"添加教师"};

(2) $I=${"姓名","性别","所在系","课程备注"};

(3) $O=${"教师记录"};

(4) $P=${"对教师进行添加操作"};

(5) $L=${"教师管理"};

(6) $Q=${ Null }。

可以以软件向导方式引导分析人员填写相应的信息完成功能单元模型的建立。功能单元基本信息是辅助生成失效模式的基础;功能单元关联信息是构造功能流程图的必要因素,各个功能单元之间的关联关系都是通过关联信息确定的。另外分析过程中的相邻层次之间的影响关系也需要依据功能层次间的关系确定,通过功能单元关联信息可以确定各个功能单元之间的层次关联。功能单元关联信息的建立对功能单元

之间的组织和关联至关重要，功能间的层次关系和失效影响等都与此部分紧密关联。

2.2 软件失效模式辅助设计

软件失效模式的确定是软件失效模式影响分析的难点。一方面分析人员由于自身经验有限难以考虑到全面的失效模式，甚至有时还会遗漏某些重要的失效模式；另一方面分析人员进行 SFMEA 时，很少收集已有的失效模式作参考，即使找到一些失效模式也会因分类繁多而参考困难，因此引导分析人员完成并尽可能找到全面的失效模式至关重要。

本文提出两种软件失效模式辅助设计方法，一种是从已有的通用失效模式库中结合软件约定层次功能单元建模信息辅助生成；另一种是从相邻层次的分析结果中辅助获得。

(1)由已有的通用失效模式库辅助生成

由已有的通用失效模式库辅助生成失效模式依赖于通用失效模式库的质量，所以本文首先研究整理了一个通用失效模式库，通用失效模式根据功能单元的基本信息进行分类，即从输入不符合要求、输出不符合要求及处理过程不符合要求等方面进行分类，表 2 是通用失效模式库的一部分。

表 2 通用失效模式库

一级分类	二级分类	三级分类	失效模式
输出不符合要求	标准设备输出类	输出失效	输出格式不正确
			输出数据无法显示
			输出错误数据
			输出数据超过上限
			输出数据低于下限
			输出数据超过屏幕的一屏显示
		输出时间失效	输出频率过高
			输出提前
			输出滞后
			输出超时

在通用失效模式库的基础上结合功能单元基本信息(含功能单元名称、输入变量集合、输出变量集合及处理过程描述集合)辅助生成失效模式，那么失效模式 Φ 可以由式(1)确定，其中 A 是功能单元基本信息，亦称失效模式主体集合，B 是通用失效模式集合，$\times$ 是笛卡尔乘积。

$$\Phi=A\times B \tag{1}$$

假设已有相同类型失效模式主体集合 $A=\{a,b,c\}$，对应此类型通用失效模式集合 $B=\{x,y,z,w\}$，则形成的失效模式集合是 $\Phi=\{ax,ay,az,aw,bx,by,bz,bw,cx,cy,cz,cw\}$。如："添加教师"功能单元定义中输出变量集合 $O=${"教师记录"}，即 $A=${"教师记录"}，B 为表 2 通用失效模式库中第四列的内容，则失效模式 $\Phi=A\times B$，如表 3 所列。

表 3 失效模式

序号	失效模式
1	"教师记录"输出格式不正确
2	"教师记录"输出数据无法显示
3	"教师记录"输出错误数据
4	"教师记录"输出数据超过上限
5	"教师记录"输出数据低于下限
6	"教师记录"输出数据超过屏幕的一屏显示
7	"教师记录"输出频率过高
8	"教师记录"输出提前
9	"教师记录"输出滞后
10	"教师记录"输出超时

分析人员可对自动生成的失效模式进行适当的修改、增加或删除以满足实际 SFMEA 分析的需要。

(2)从相邻层次的分析结果获得

上文阐述了系统级 SFMEA 的软件约定层次为软件功能流程图中功能单元，因此功能单元之间存在层次关系，这种层次关系可以使上层功能单元调用下层功能单元完成相应功能。功能单元的关联也必然导致软件失效的相互关联，由于上层功能单元是调用底层功能单元，因此当上层功能单元发生某种失效时，其原因基本都是来自底层功能单元发生的失效。从某种意义上讲，可以认为上一个层次的失效模式原因就是底层功能单元的失效模式。而下一层次模块的失效影响是其对上一个层次的输出，因此其产生的影响也可作为上一个层次的失效模式。

例如图 3 中的功能单元"功能 2"是"功能 1"的子单元，则"功能 1"的一个失效模式描述"模式 1"可能为"功能 2"的"影响 2"，而"模式 1"的失效原因即为 "模式 2"。

这些相互之间的影响和关联都可作为分析人员参考依据，分析人员确认后可以辅助分析人员完成分析表格的自动填写，提高分析人员工作效率。

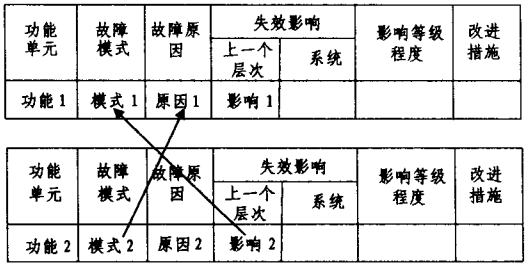

图 3 相邻功能层次间分析记录关系

2.3 软件失效原因、纠正措施辅助设计

确定失效模式后需要分析产生失效模式的原因，失效原因的确定是一个很棘手的问题，特别是在软件开发早期阶段，分析人员很难推测出对于一个可能的失效模式其发生的具体原因。因为 SFMEA 研究的失效是一种潜在发生的，不是一个具体、确定的失效。特别是对于一个没有经验的分析人员，有必要提供失效原因辅助技术，辅助分析人员进行失效原因定位。

辅助分析人员确定失效原因可以通过以下两种途径：

(1)利用相邻层次之间的分析结果，确定某个层次的失效模式原因时可参考其下一个层次的功能模块的失效模式描述。具体实现方法是首先获得分析功能单元的所有下层单元集合 ψ，然后在 SFMEA 分析结果中搜索所有属于集合 ψ 功能单元的分析记录，分析记录中的失效模式描述都可以作为待分析单元的失效原因参考，分析人员可根据实际情况进行分析选取；

(2)确定失效原因还可通过参考已有相关的失效案例信息确定。失效案例库中存放了许多典型的失效案例信息，这些案例信息按照失效模式分类存放，一个相同的失效模式可能含有多个失效案例信息，当进行某个特定失效模式分析时可以通过查看与其相关的失效案例信息。失效案例信息的提供可以辅助分析人员参考以前的失效原因，更加准确地定位发生失效的原因。

3 系统级 SFMEA 辅助工具

根据上文提出的系统级 SFMEA 辅助设计方法，用 VC6.0

实现了系统级 SFMEA 辅助工具，该工具主要包括以下几个主要功能：用户登录、功能单元管理、功能流程管理、SFMEA 记录管理、失效模式管理、失效案例管理、报告生成，每个功能描述如下：

(1)用户登录功能：通过口令检查的方式验证用户是否有权限登录本系统；

(2)功能流程管理：实现对功能流程图的功能单元的增加、删除和修改，以树状形式描述功能流程图的层次结构；

(3)功能单元管理：实现对功能单元建模信息(如：功能单元名称、输入变量、输出变量、下一层次功能集合等)的增加、删除和修改；

(4)SFMEA 记录管理：对 SFMEA 工作表中的内容实现增加、删除和修改功能；

(5)失效模式管理：提供一个通用的失效模式库，可以根据需要对失效模式库进行增加、删除和修改，以满足实际应用的需要；

(6)失效案例管理：对以往某个失效模式下的失效案例进行管理，包括失效案例的增加、删除和修改。

图 4 为 SFMEA 辅助工具的功能流程图。

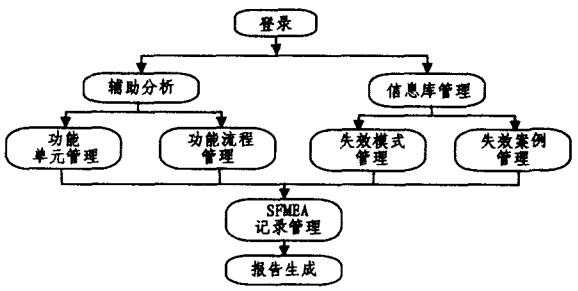

图 4　功能流程图

该工具已在多个系统级 SFMEA 中应用，通过友好界面引导分析人员完成系统级 SFMEA 的分析过程，最后生成图 5 所示的系统级 SFMEA 报表。

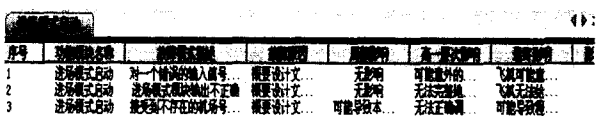

图 5　系统级 SFMEA 报表

通过实例应用进一步验证了采用辅助工具进行 SFMEA 分析至少有以下优点：

(1)分析人员可以方便地参考分类整理的失效模式，并借助工具提供的快捷功能，直接生成失效模式(在此基础上可以对已经生成的失效模式进行修改)，这样可以避免遗漏对某些失效模式的分析(对没有经验的分析人员尤其有效)；

(2)通过辅助工具的向导可以自动生成功能层次图，不仅可以让分析人员清楚地了解系统的功能流程，而且通过功能层次图可以关联失效模式间的影响；

(3)可以更加快捷有效地进行失效模式影响分析及原因定位，分析人员可以利用工具迅速查看相邻层次的分析记录，以及对应的失效模式下已有的失效案例信息，从而给分析人员提供更多的参考；

(4)最后可以通过辅助工具提供的 SFMEA 报表生成功能，有选择地生成需要的 SFMEA 表，省去了制作 SFMEA 报表的麻烦。

结束语　本文首先在实践过程中细化了 SFMEA 的实施步骤，其次以 SFMEA 分析过程为切入点研究相关辅助设计方法，在方法研究的基础上设计开发了 SFMEA 辅助工具，并对辅助工具进行了实例应用，进一步验证了辅助工具可以协助分析人员进行 SFMEA 分析，提高分析效率，减少分析工作量，提高 SFMEA 效果，极大地推动 SFMEA 的工程应用，后续还需进一步实现 SFMEA 更大程度的自动化。

参 考 文 献

[1] Ozarin N. Failure Modes and Effects Analysis during Design of Computer Software[C]// Proceedings: International Symposium on Product Quality and Integrity. 2004:201-206

[2] Hecht H, An Xuegao, Hecht M. Computer Aided Software FMEA for Unified Modeling Language Based Software[C]// Proceedings: International Symposium on Product Quality and Integrity. 2004:243-248

[3] Tribble A C, Miller S P. Software Safety Analysis of a Flight Management System Vertical Navigation Function-A Status Report[C]// Proceedings of the 22th Digital Avionics Systems Conference. Indianapolis, CA, October 2003:12-16

[4] John D, Musa. Software Reliability Engineering[M]. China: Machine Press, 2003:1-29

[5] 吴邦国，唐任仲. 软件 FMEA 技术研究[J]. 机电工程，2004，21(3)：8-12

[6] 赵廷弟，孙琳玲，屠庆慈. 计算机辅助 FMECA 软件模型[J]. 北京航空航天大学学报，2000，26(1)：118-121

[7] 赵廷弟，曾声奎，康锐. 计算机辅助可靠性设计分析系统研究[J]. 航空学报，2000，21(5)：206-209

[8] 陶建峰，王少萍，姚一平. 计算机辅助 FMECA 与 FTA 正向综合分析方法研究[J]. 北京航空航天大学学报，2000，26(6)：663-665

(上接第 88 页)

[3] Matthew C. On the throughput of Bluetooth data transmissions [C]// IEEE Wireless Communications and Networking Conference. Orlando, Florida: IEEE, 2002:119-123

[4] Bluetooth SIG. Specification of the Bluetooth System, version 2.1+EDR www.bluetooth.org 2007

[5] 徐飞，庄奕琪，郭峰. 载荷长度对蓝牙数据传输吞吐量的影响[J]. 电子科技大学学报，2008，37(1)：39-42

[6] 樊昌信，詹道庸，徐炳祥，等. 通信原理(第 5 版)[M]. 北京：国防工业出版社，2001

[7] 丁龙刚. 蓝牙射频技术的分析与应用[J]. 现代电子技术，2003，24：105-106

[8] Rodger E, Ziemer, Roger L, et al. Introduction to digital communication [M]. [S. L.]: Person Education, 2000:174-187

[9] Miller C, Lee J. BER expressions for differentially detected π/4-DQPSK modulation [J]. IEEE Transactions on Communications, 1998, 46(1):71-78

[10] Lee E J, Younhy. Efficient scheduling by incorporating bin packing with limiter and weighted round robin for Bluetooth[C]// Computational Science and Its Applications-ICCSA. [S. L.]: [s. n.], 2006(3983): 187-196

[11] Simon M K, WANG C C. Differential Detection of Gaussian MSK in a Mobile Radio Environment[J]. IEEE Transactions on Vehicular Technology, 1984, VT-33(4):307-320

[12] 郭梯云，杨家玮，李建东. 数字移动通信(修订本)[M]. 北京：人民邮电出版社，2000