文章编号: 1000-6893(2002)03-0206-05

基于 RSMTL-CAD 框架的 FMECA 软件设计

苏铁军, 孙琳玲, 赵廷弟
(北京航空航天大学 可靠性工程研究所, 北京 100083)

DESIGN OF FMECA SOFTWARE BASED ON RSMTL-CAD FRAMEWORK

SU Tie-jun, SUN Lin-ling, ZHAO Ting-di
(Reliability Engineering Institute, Beijing University of Aeronautics and Astronautics, Beijing 100083, China)

摘 要: 分析了当前工程实际对计算机辅助 FMECA (故障模式影响及危害性分析) 软件的要求, 描述了基于 RSMTL (可靠性、安全性、维修性、测试性、保障性)-CAD 框架的 FMECA 软件的主要功能和体系结构, 并讨论了软件设计过程中的 2 个关键问题: ①通过对 FMECA 数据特点的分析, 利用面向对象思想建立了一种灵活开放的数据模型。这种数据模型利用层次关系和属性集合, 描述了 FMECA 结果数据中的 4 种关系: FMEA 结果和 CA 结果之间的依存关系; 上下级产品故障模式因果逻辑关系; 同一产品在不同初始约定层次设置下的数据组织关系; 版本关系。②在数据关系的映射中, 利用等价关系的方法解决了各软件工具之间数据引用关系的表达问题。该软件以 Client/Server 机制运行, 支持网络化和多用户并行使用。

关键词: 可靠性; 计算机辅助设计; FMECA; 数据模型
中图分类号: V 215.7 **文献标识码**: A

Abstract: Firstly, the requirement to Computer Aided Failure Mode, Effects and Criticality Analysis (FMECA) software is analyzed. Then main functions and architecture of the FMECA software based on Reliability, Safety, Maintainability, Testability, Logistics (RSMTL)-CAD Framework are described. Two issues in the development process of the software are discussed. 1) After analyzing interrelation of FMECA results, a flexible and open data model based on Object Oriented Method is presented. Through using the hierarchy and property set, the model describes four relations of FMECA result data, that is, the dependency of various FMECA results, causality of the failure modes of products from different indenture levels, organization of FMECA results at different analysis initial indenture levels of the same product and the version management of FMECA result. 2) Equivalence Relation is used to describe the reference relations among the tools of RSMTL-CAD. The software runs in Client/Server mode and can be operated in networks and multi-user environments.

Key words: reliability; computer aided design; FMECA; data modeling

FMECA 是工程中常用的一种可靠性设计分析技术, 但 FMECA 的特点是工作量很大, 费时费力。因为 FMECA 的分析对象包括系统内的所有部件, 而且 FMECA 要和产品的整个设计开发过程紧密结合才能最大限度地发挥作用[1], 所以数据量非常大, 而且数据项之间关系很复杂。从最开始的方案论证阶段一直到详细设计阶段, 要根据不同的设计阶段采用不同的 FMECA 方法, 而且后面设计阶段的 FMECA 工作要参考前面设计阶段的 FMECA 数据。在系统研制中, FMECA 居于可靠性工作的中心地位, 测试性、保障性、安全性等设计分析工作要在 FMECA 的基础上进行, 因此这些设计分析工作需要及时地访问 FMECA 的结果数据。

目前, 在大型武器装备的研制中, CAD 技术已经得到普遍的应用, 大型的 CAD 软件基于网络运行, 支持开发设计和数据共享, 这对 FMECA 软件提出了新的要求。

近年来 FMECA 自动化方面的研究很多, 国内外出现了很多计算机辅助 FMECA 软件工具, 有些已经商品化。这些软件工具在一定程度上减轻了分析人员的文字工作负担, 但大部分是脱胎于单机版本, 因此对网络应用的支持不够, 特别是在与产品设计过程结合方面有欠缺。

当前工程实际对 FMECA 软件有下述要求:

(1) 必须与产品整个设计过程结合起来, 提供与设计阶段相适应的 FMECA 方法, 也就是说, 要进行 FMECA 的分析流程管理;

收稿日期: 2001-09-05; 修订日期: 2001-11-28
文章网址: http://www.hkxb.net.cn/hkxb/2002/03/0206/

(2) 处理好 FMECA 结果数据的版本管理问题, 使后面的分析能充分利用前面的分析结果;

(3) 提供全面的辅助分析功能, 提供产品故障率、常见故障模式等基础信息;

(4) 能网络化运行, 支持多用户和数据共享;

(5) 能给其它分析工作提供方便的数据接口, 并通过合适的机制表示不同分析工作之间的数据引用关系, 以保持数据的一致性和完整性, 尤其是要处理好这种数据引用关系与版本管理的交联关系。

本文中描述的 FMECA 软件工具是 RSMTL-CAD-SIE (可靠性、安全性、维修性、测试性、保障性计算机辅助设计分析软件集成环境) 的一部分, 是基于 RSMTL-CAD 框架开发的 (图 1)。RSMTL-CAD-SIE 是为了满足武器装备研制过程中对可靠性、安全性、维修性、测试性、保障性设计分析的需求而研制开发的大型软件集成环境。它从结构上可分为 3 部分[2], 即 RSMTL-CAD 框架、RSMTL 数据库系统和 RSMTL 设计分析工具。其中, RSMTL-CAD 框架集成所有的设计分析工具, 提供共性的、底层的服务, 实现设计分析工具对数据库的访问。设计分析工具按照框架对集成及数据访问的统一要求开发, 完成某种特定的设计分析工作, 相互之间具有相对的独立性。RSMTL 数据库保存着框架及各个工具的数据, 实现各个工具之间的数据共享。

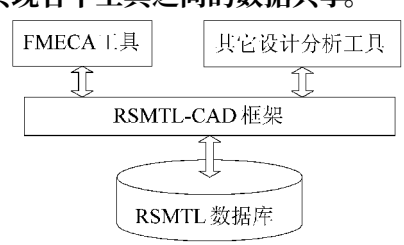

图 1　RSMTL-CAD 集成环境

Fig. 1　RSMTL-CAD integrated environment

1　FMECA 软件模型

FMECA 工具是以 FMECA 工作流程为主线, 以可靠性数据库为核心, 全面支持 FMECA 的各项工作 (包括故障模式分析、危害性分析、报告生成等等), 并在 RSMTL-CAD 框架下与其它各设计分析工具集成应用的计算机辅助 FMECA 软件。

1.1　软件功能

FMECA 软件以 GJB 1391《故障模式、影响及危害性分析程序》为基础, 并考虑到当前装备研制过程中的实际需求, 支持各个设计阶段的 FMECA 工作。主要功能包括:

(1) 分析设置　包括设置分析方法、设置打开版本、定义故障模式发生概率等级、设置初始约定层次、设置严酷度、新建严酷度定义、设置保存方式等功能。

(2) 辅助分析部分　包括硬件法故障模式影响分析、功能法故障模式影响分析、定量故障模式危害性分析、自动计算故障模式危害度、自动计算产品危害度、利用 FTF (FTA 与 FMECA 综合分析) 计算结果辅助填写故障模式影响概率、绘制危害度矩阵、定性故障模式危害性分析、向下迭代填写最终影响和严酷度。

(3) 提供各种参考信息　包括用户描述参考库、常用故障模式参考 (来自 GJB)、本项目结果数据参考、相似项目结果数据参考。

(4) 提供各种浏览查询工具　包括浏览故障模式、故障模式原因影响查询、单点故障模式清单、按严酷度的故障模式清单、关键件重要件清单、自动生成可自定义的 FMECA 报告。

1.2　软件体系结构

FMECA 软件是 RSMTL-CAD 集成环境中的一部分, RSMTL-CAD 以 Client/Server 的方式, 运行在 Microsoft Windows NT/95/98/2000 构成的局域网上。其软件集成环境如图 2 所示[3], 软件总体结构如图 3 所示。

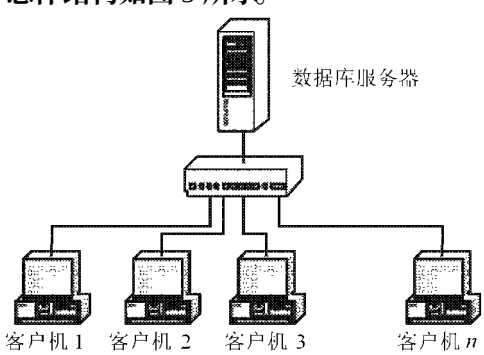

图 2　RSMTL 网络体系图

Fig. 2　RSMTL network architecture

FMECA 软件工具对数据库的访问通过 RSMTL-CAD 框架进行, 其它设计分析工具对 FMECA 数据的访问则是通过 FMECA 软件工具提供的数据接口进行。

(1) 数据库　存在于数据库服务器上, 保存项目的全部数据, 包括框架控制的数据以及各软

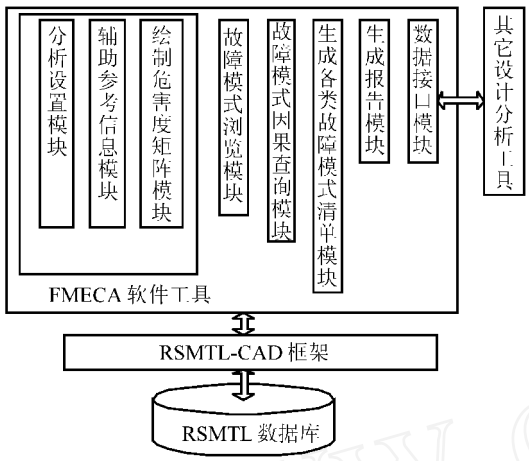

图 3 FM ECA 软件结构

Fig. 3 FM ECA software structure

件工具特有的数据;

(2) 框架 对整个集成环境进行总体控制, 给各软件工具提供底层的服务, 使各软件工具能对数据库进行访问;

(3) FM ECA 软件工具 辅助用户进行 FM ECA 工作, 并且给其它设计分析工具提供数据接口, 使其它设计分析工具能读取 FM ECA 的数据;

(4) 其它设计分析工具 完成其它设计分析工作, 通过 FM ECA 工具提供的数据接口读取 FM ECA 数据。

2 关键技术研究

2.1 FM ECA 数据模型研究

FM ECA 的数据建模主要面临 4 个方面的困难[4]:

(1) FM EA 结果和 CA 结果之间的依存关系 FM ECA 一般包括故障模式分析(FM EA)或危害性分析(CA), CA 要在 FM EA 的基础上进行。因此, CA 和 FM EA 的结果中, 有些数据项是相同的, 另一些则是各自特有的。根据掌握基础信息的多少, CA 又分定量 CA 和定性 CA 两种。

(2) 上下级产品故障模式因果逻辑链表示 在 FM ECA 中, 下级产品故障模式的"对上层次影响"往往就是上层次产品的故障模式, 即上下级产品的某些故障模式之间存在因果逻辑关系链。充分利用这种因果链, 可以更有效地进行 FM ECA。

(3) 同一产品在不同初始约定层次设置下的数据组织 在不同的初始约定层次设置下, 产品的 FM ECA 结果中有些数据项不会变化, 例如故障模式描述、检测方法、故障模式频数比等, 但有些数据项是不同的, 例如最终影响、严酷度、故障影响概率等。如何将数据冗余降至最低, 又将数据的特性表达清楚, 是数据建模必须考虑的问题。

(4) 版本管理问题 FM ECA 工作要贯穿整个设计过程, 在不同的设计阶段会产生不同的分析结果。并非只有最终的分析结果需要保留, 因为中间阶段的分析结果反映了当时的设计思路, 尤其是当这些分析结果被其它分析工具(如维修性、测试性分析)引用时, 为了保持数据的一致性, 必须要保存 FM ECA 分析的不同版本。

版本管理问题是所有 CAD 软件都要面临的问题, FM ECA 的版本管理尤其困难, 主要体现在: ①FM ECA 的数据量很大, 如果版本管理的问题解决得不好, 产生数据冗余现象, 将影响分析效率; ②上下级产品的故障模式之间存在因果逻辑链, 如果版本管理问题解决得不好, 会使数据不一致。

本文采用面向对象的思想, 综合考虑上述问题, 设计的数据模型如图 4 所示。

这种数据模型的主要特点是:

(1) 采用面向对象的思想, 将有关的数据对象化。例如将对一个产品的一次 FM ECA 结果作为"故障模式集合对象", 将一个产品的一条模式作为"故障模式对象", 将一个产品的一条模式的检测方法作为"检测方法对象";

(2) 以"故障模式对象"为中心, 将已经对象化的各种不同 FM ECA 分析方法的结果集成在一起。如故障模式影响分析得到的模式描述、故障原因、严酷度等, 故障模式危害性分析得到的故障发生概率等级、故障模式频数比等;

(3) 通过"故障模式集合"对象实现版本管理, 每个"故障模式集合"对象对应产品的一次 FM ECA 工作, 它们之间是版本关系。将版本管理放在这一层次上, 使最终得到的数据模型既满足了灵活性的要求又避免了数据冗余;

(4) 具有可扩充性。可扩充性不仅体现在将来有新的结果数据项产生时可以方便地加入数据模型, 还体现在这个数据模型记录维护了上下级产品故障模式间的因果关系链(故障原因), 为将来 FM ECA 故障影响的智能推理打下了基础。

2.2 数据关系的映射

前面的数据模型利用面向对象的思想描述了 FM ECA 中复杂的数据关系, 为了在关系数据库

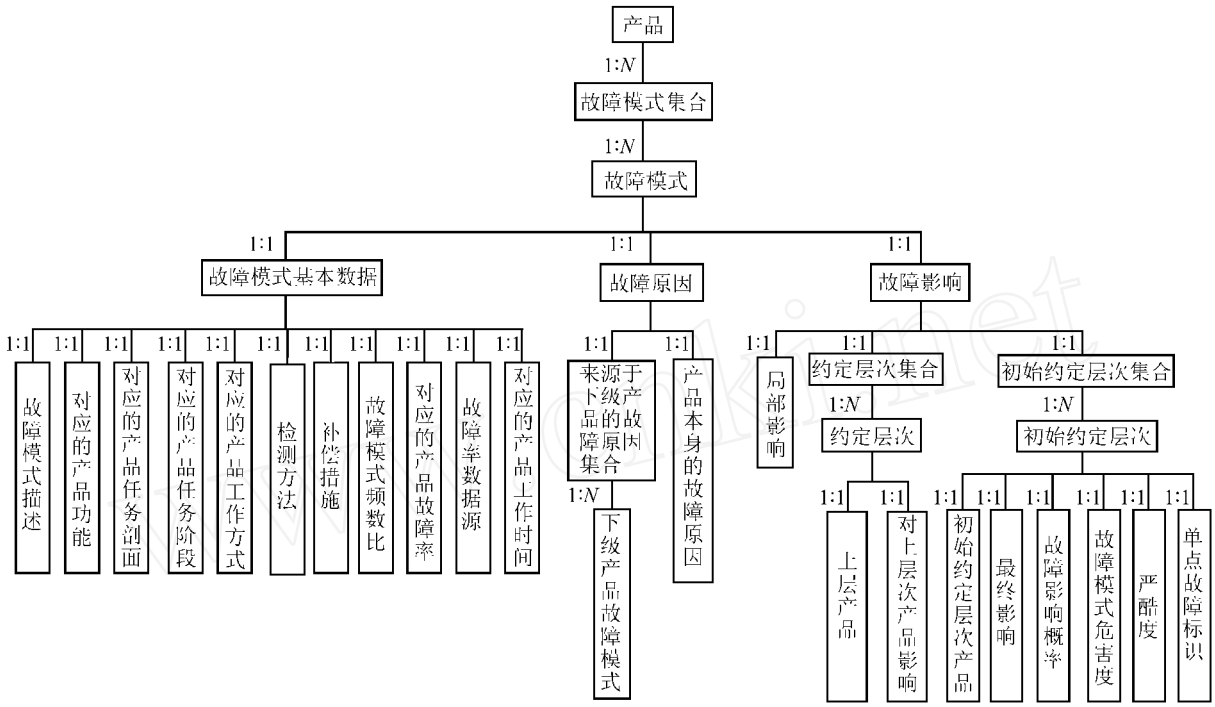

图 4　FM ECA 数据模型

Fig. 4　FM ECA data model

系统中实现, 必须要进行数据关系的映射。而且这种映射还要考虑框架对数据管理的要求。

框架对各工具的数据的管理是通过等价关系实现的[2]。每一对等价关系描述了哪个工具对哪个已知对象进行了什么操作之后得到了什么对象。等价关系有 4 个要素: ①源对象: 已知对象; ②目标对象: 得到的对象; ③等价关系, 操作的种类; ④工具: 表示哪个工具建立了这个等价关系。

例如, 如果可靠性预计工具对产品 A 进行可靠性预计, 得到了该产品的故障率 λ_A, 把产品 A 和故障率 λ_A 都对象化, 就得到了如下的一对等价关系:

(产品 A, 故障率 λ_A, 可靠性预计, 可靠性预计工具)

值得注意的是, 等价关系只是记录对象之间的关系, 而不记录对象所代表的具体数据, 所以对象"产品 A"和"故障率 λ"的详细数据, 如产品的名称、型号, 故障率的数值、单位等, 都是由相应的工具控制的。但这种控制也必须在框架的监控下。

通过对等价关系的控制, 可以清晰的管理各工具之间的数据调用关系, 因此就可以保证数据的一致性和完整性。

对数据的管理还通过对对象的生成、更新、删除的控制来体现, 并通过对对象的导出和导入之间的一个事务的管理来实现多用户的环境。

于是得到 FM ECA 软件工具建立的等价关系(见表 1)。

表 1　FM ECA 工具建立维护的部分等价关系

Table 1　Some equivalence relations in FM ECA tool

源对象	目标对象	等价关系
产品	故障集合	故障分析
故障集合	故障	故障集合包含的故障
故障	功能	故障对应的功能
故障	约定层次集合	约定层次集合
约定层次集合	约定层次	包含的约定层次
约定层次	产品	约定层次对应的产品
约定层次	上一层次影响	对应的对上层影响
故障	初始约定层次集合	初始约定层次集合
初始约定层次集合	初始约定层次	包含的初始约定层次
初始约定层次	产品	初始约定层次对应的产品
初始约定层次	最终影响	故障的最终影响
故障	故障原因集合	从下层次产品故障影响来的原因
故障原因集合	故障	故障原因集合包含的从下层次产品故障影响来原因

3　FM ECA 软件的特点

(1) 基于 Client/Server 机制运行, 实现数据共享和用户并行, 实现完善的版本管理。

(2) 紧密地与框架集成, 数据接口清楚, FM ECA 软件工具充分利用 RSM TL CAD 框架提供的全局框架模型、设计对象模型、设计事务模型实现了与框架和其它软件工具的集成, 更符合

工程实际的要求。

(3) 全面的、多层次的辅助分析机制, 包括用户自定义的常用描述参考、GJB 中几类典型系统的常用故障模式描述以及当前项目和相似项目的 FMECA 结果参考。

(4) 通过"影响来的原因"、"对上层次影响"等数据项描述上下级产品的故障模式逻辑关系链。

4 结 论

FMECA 软件工具采用面向对象技术进行数据建模, 基于 RSMTL-CAD 框架进行软件设计和开发, 实现了网络化、多用户运行, 通过等价关系的应用实现数据库设计。该软件工具已经在"九五"某重点预研项目中实现, 验证了数据模型及数据库设计的可行性, 为进一步的 FMECA 专家系统、智能推理打下了基础。

参 考 文 献

[1] Bowles J B. The new SAE FMECA standard[A]. In: Proceedings Annual Reliability and Maintainability Symposium [C]. Atlanta Georgia USA: IEEE, 1998. 48-53.

[2] van der Wolf P. CAD frameworks principles and architecture[M]. Dordrecht Netherlands: Kluwer Academic Publishers, 1994. 35-47.

[3] 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(3): 206-209.
(Zhao T D, Zeng S K, Kang R. Study on computer-aided reliability design and analysis system[J]. Acta Aeronautica et Astronatutica Sinica, 2000, 21(3): 206-209.)

[4] Kukkal P, Bowles J B, Bonnell R D. Database design for failure modes and effects analysis[A]. Proceedings Annual Reliability and Maintainability Symposium [C]. Atlanta Georgia USA: IEEE, 1993. 231-239.

作者简介:

苏铁军(1974-) 男, 北京航空航天大学可靠性工程研究所博士研究生。主要研究方向为可靠性设计分析技术, FMECA 自动化及智能化。电话: 010-82316441。E-mail: stj74@263.net, 通讯地址: 北京航空航天大学可靠性工程研究所 016 教研室, 邮编: 100083

孙琳玲(1975-) 女, 北京航空航天大学可靠性工程研究所工程师。主要研究方向为可靠性设计分析技术。电话: 010-82316443。E-mail: sunll@263.net, 通讯地址: 北京航空航天大学可靠性工程研究所 016 教研室, 邮编: 100083

赵廷弟(1965-) 男, 北京航空航天大学可靠性工程研究所教授。主要研究方向为可靠性设计分析技术, 可靠性 CAD 及其智能化, 软件可靠性与测试, 故障诊断与专家系统等。电话: 010-82316570。E-mail: ztd@cenpok.net, 通讯地址: 北京航空航天大学可靠性工程研究所 016 教研室, 邮编: 100083

(责任编辑: 李铁柏)