文章编号:1671-4598(2018)12-0130-06 DOI:10.16526/j.cnki.11—4762/tp.2018.12.030 中图分类号:TP311 文献标识码:A

舰船装备软件可信性分析设计技术研究

吴立金,韩新宇,闫 然,许兆伟,唐龙利
(中国船舶工业综合技术经济研究院,北京 100081)

摘要:针对舰船装备软件研制过程开展软件可信性分析设计工作中缺乏数据基础支撑、与工程实践不够紧密以及缺乏可操作性分析技术的现状,进行舰船装备软件缺陷信息收集并形成缺陷模式,研究基于缺陷数据的舰船装备软件可信性设计分析技术、方法和工具,包括:舰船装备软件可信性设计准则、舰船装备 SFMEA 技术方法、SFMEA 与 SFTA 综合分析方法,并提供方法的辅助工具和数据库,为提高舰船装备软件可信性提供技术支撑。

关键词:软件可信性;失效模式分析;设计准则

Research on Dependability Analysis and Design Technology of Shipboard Equipment Software

Wu Lijin, Han Xinyu, Yan Ran, Xu Zhaowei, Tang Longli
(China Institute of Marine Technology&Economy, Beijing 100081, China)

Abstract: In the software developing process of shipboard equipment software, there is a lack of data foundation and practical engineering practice. So this paper collected software defect information of shipboard equipment and researched defect mode. On the basis of the defect information, the technology of equipment software dependability analysis and design is researched, such as shipbuilding equipment software dependability design criteria, SFMEA and SFTA comprehensive analysis methods. Besides, we provide accessory tools and databases to enhance the software dependability of shipboard equipment.

Keywords: software dependability; SFMEA; design guidelines

0 引言

当前,舰船行业软件可信性保证技术的应用情况远远落后于其它国防行业。近年来,军方对型号软件的可信性予以了高度重视,对于一些重点型号,要求在软件研制中进行可信性设计分析及管理,在交付前进行评估等[1]。

本文针对舰船装备软件研制过程开展软件可信性分析工作中缺乏数据基础支撑、与工程实践不够紧密以及缺乏嵌入式的软一硬件系统可信性分析技术的现状,收集舰船装备软件缺陷信息,进行缺陷分类、缺陷模式研究,基于缺陷数据进行舰船装备软件可信性设计准则、舰船装备软件可信性分析技术的研究,在技术研究基础上选择典型舰船装备软件进行技术应用验证,以及开发相应的辅助工具和数据库系统;为舰船装备软件开展可信性设计分析活动提供基本的技术、方法、工具和数据,也为制定舰船行业内的有关软件可信性的规范、标准提供技术依据。

1 研究现状分析

软件可信性设计、分析技术发展至今,已经具备一定的技术基础。然而目前在舰船装备领域,软件可信性设计分析技术应用的总体现状是:各种技术方法与工程实践结合欠缺,能指导工程应用的较少;技术方法缺少数据的支撑,没有数据、示例的支撑,方法应用起来效果较差;对于嵌入式的软一硬件系统,软件可信性分析技术相对匮乏。这种现状导致了当前在舰船行业可信性工作难以开展,没有真正形成有效的舰船装备软件可信性设计分析的能力,以下分别对相关技术的研究现状和发展必要进行阐述。

1.1 缺陷模式现状

在利用缺陷模式进行可信性分析研究上,目前仅有很少数研究提出了利用软件缺陷模式特征,利用静态分析方法进行软件失效推理的方法,但是由于缺陷模式特征是和编程语言相关的,缺陷模式特征知识库的建立需要更多数据的支持,目前的研究还仅仅是非常初步的理论研究,需要进一步收集更多地缺陷数据,提取软件缺陷模式特征,建立缺陷模式特征知识库,提出更为有效的方法,建立合理的软件工具,将缺陷模式特征库应用到软件可信性分析技术中,能够较为有效地帮助发现软件中存在的缺陷。

软件缺陷的分类是研究软件缺陷的基础。软件缺陷的分类有多种方法,目的不同,角度和复杂程度也不一样[2]。具代表性的软件缺陷分类方法包括:1)基于软件错误来源的软件缺陷分类,代表有 Putnam 等人、国家军用标准 GJB—437;2)基于错误性质的软件缺陷分类,代表有 Goel、Thayer、Beizer 等人;3)基于正交分类的软件缺陷分类,由 IBM TJ Watson 研究中心在 1992 年提出;4)基于软件生命周期活动软件缺陷分类,由电气和电子工程师学会制定的软件异常分类标准(IEEE Standard Classification for

收稿日期:2018-05-12; 修回日期:2018-05-24。

作者简介:吴立金(1987-),男,山东人,工程师,主要从事软件测评与可信性技术研究方向的研究。

Anomalies1044 1093）对软件异常进行的全面的分类；5）基于开发阶段的软件缺陷分类（Phase－DC），通过对缺陷所作的实际修该来确定类型，缺陷类型定义为着重关注缺陷关联的开发阶段，确定每个缺陷的引入阶段和发现阶段，利用阶段的信息对采用专家方法和正式评审的方式将缺陷类型进行的定义；6）基于某类特定软件研究软件缺陷分类，如针对型号软件的特点，将软件缺陷可分为“基本软件缺陷－子类”这样的一种层次结构分类。

1.2　软件可信性设计准则现状

国外相关机构对软件可信性设计进行了长期研究，最早由著名软件工程专家 Myers 提出在可靠性设计中必须遵循的两个原则：一是控制程序的复杂程度；二是与用户保持紧密联系[3]。美国航空和宇宙航行局制定了 NASA－GB－8719.13－2004《美国宇航局软件安全性指南》和 NASA－STD－8719.13B－2004《美国宇航局软件安全性标准》，为软件开发人员和从事软件安全性工作的工程师们提供适用的软件安全性设计和分析方法和技术，美国航空航天局（NASA）下属机构马歇尔空间飞行中心（MSFC）在某型号项目实施的可信性设计准则。这些标准或要求反映了当时已有的经验教训、最佳实践的要求和类似环境和软件可能经受的类似或相同问题。国外虽积累了丰富的工程实践经验，但由于语言和经验的限制，对于其准则细则不能完全理解透彻，难以用于国内的项目实践中。

国内对软件可信性设计研究始于近 20 年，已颁布 GJB/Z 102－1997《软件可靠性和安全性设计准则》，作为指导性技术标准，给出计算机软件可靠性和安全性设计的准则和要求，指导武器装备嵌入式软件的开发与设计，主要是空空导弹的开发项目。2012 年，结合国内外软件可靠性和安全性研究和实践的现状，补充国内外相关研究成果和优秀实践，对 GJB/Z 102 进行了修订，形成了 GJB/Z 102A－2012《军用软件安全性设计指南》。但是 GJB/Z 102A 仍旧讲述的概念宽泛，可操作性不强，在国内未能广泛应用。

软件可信性设计准则可以用于在软件设计开发过程中对软件缺陷进行预防，对已有的缺陷数据进行研究，提出相应的缺陷预防措施，可以避免类似缺陷的再发生。因此，有必要对软件缺陷的信息进行充分的分析和利用，进行软件可信性设计准则的研究。

1.3　软件可信性分析现状

SFMEA 和 SFTA（软件故障树分析）两种技术自 20 世纪 70 年代末提出以来，主要应用在安全性要求较高的模块中，但它们在应用时有各自的缺点，比如：SFMEA 是一种自底向上分析的单一失效线索的方法，其分析结果以表格方式列出，无法完善的表达失效原因之间的各种逻辑关系，因此也影响了失效措施的制定，即，只制定单点失效的改进方案，缺少对多点失效的考虑；SFTA 是一种自顶向下的依照树状结构倒推失效原因的方法，选取顶事件时，往往会遗漏潜在因素的顶层影响，另外，SFTA 在分析底事件时也会有所遗漏，这回影响到底事件的重要度排序，从而影响实施改进措施的轻重缓急判断。二者在表达方式也各有不足，表格方式不如树形结构直观，而树形结构在分析复杂的软件系统时相当庞大，人工查找单一失效的线索不是很方便。目前，将它们相结合，互相弥补不足，使分析过程更加完备的综合分析方法以及方法的应用日益受到人们的重视。

目前对 SFMEA 的研究，还存在以下问题：

1）如何收集软件失效模式和失效原因。失效模式和失效原因是系统级 SFMEA 的基础，硬件系统标准单元的失效模式一般比较明确，失效原因也便于提取，但软件系统的失效模式和失效原因却不是非常明确、难以准确提取[4]。

2）如何对目标软件系统划分层次、确定模块间的逻辑关系以及系统各模块间的失效影响。传统的系统级 SFMEA 对目标系统（尤其是任务交叉、不易分割的软－硬件系统）层次划分和模块间逻辑关系的确定没有很明确清晰的方法，对硬件和软件的相互作用也欠缺考虑，没有准确判断软件模块间失效影响的有效方法，往往依赖于软件分析人员的经验，分析过程精确性低、客观性差，且没有效率。

3）如何由系统级 SFMEA 的分析结果指导详细级 SFMEA，以及详细级 SFMEA 的实施过程和方法。由于详细级 SFMEA 要涉及复杂多样的程序结构，目前还没有一套简易有效的方法，阻碍了 SFMEA 在工程中的应用。

4）如何提高分析过程的自动化程度。目前针对硬件的 FMEA 自动化工具国内外已经开发了许多，例如国内的可维公司就已成功自主研发 FMEA 自动化工具。但是针对 SFMEA 的自动化工具还是比较缺乏，系统级 SFMEA 的大量工作仍需手工完成，详细级 SFMEA 辅助分析工具更为匮乏，导致了分析效率低下。

2　软件可信性分析设计过程

根据舰船装备软件可信性设计、可信性分析研究的需要，首先进行舰船装备软件缺陷数据收集，从而使后续的研究更具有针对性、适用性。在此基础上进行舰船装备软件缺陷模式分析，基于缺陷收集和缺陷模式分析，进一步考虑舰船装备软件可信性设计准则的研究。针对目前嵌入式软－硬件系统可信性分析及分配技术中存在的问题。对于技术研究过程中形成的和方法和数据，开发相应的数据库系统；在技术方法的应用上，选择典型舰船装备软件进行可信性分析以及可信性分配技术应用验证。整个课题研究为舰船装备软件开展可信性设计分析活动提供技术方法和数据库系统。项目总体实施途径如图 1 所示。

2.1　舰船装备软件缺陷收集、缺陷模式研究

1）按照不同软件类别，包括嵌入式/非嵌入式、编程语言（C/C＋＋/C＃等）、应用领域（科学计算/人机交互/数据处理等）分类，收集舰船装备软件缺陷信息，对缺陷进行原因分析；

2）在现有的软件缺陷分类、缺陷模式研究基础上，针对开展舰船装备软件可信性设计、舰船装备软件 SFMEA 等分析工作的需要，进行舰船装备软件缺陷分类研究、定

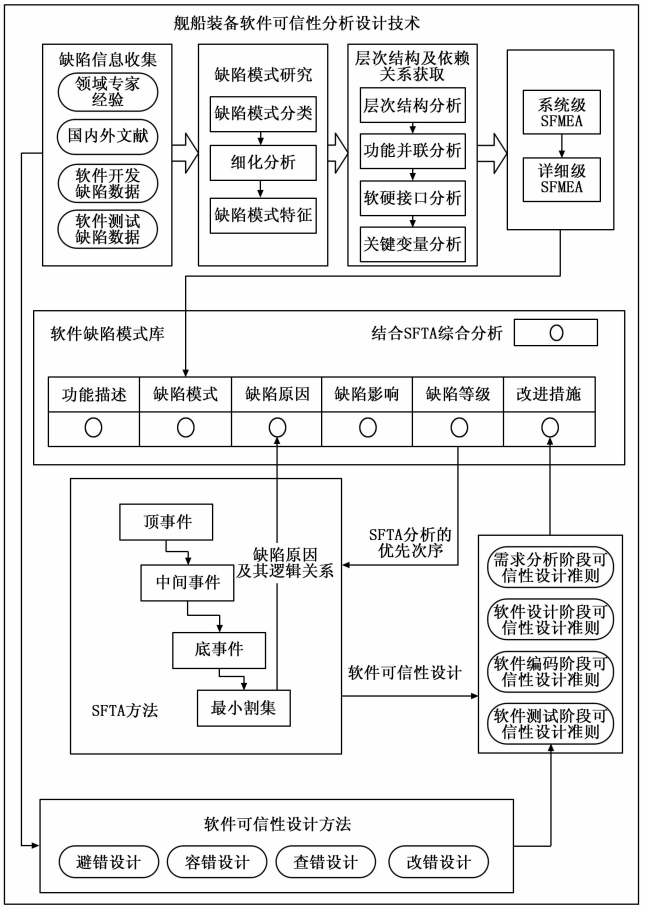

图 1 软件可信性分析设计过程

义并提炼舰船装备软件缺陷模式，并对收集到的缺陷数据按缺陷分类、缺陷模式进行统计；

3）基于缺陷分类和缺陷模式研究，进行舰船装备软件缺陷模式特征知识库的研究，将软件缺陷模式特征与知识库进行综合研究；开展基于软件缺陷模式特征知识库的软件失效推理技术的研究[5]。

4）建立舰船装备软件缺陷、缺陷模式数据库，以及相应的数据库管理工具。

2.2 舰船装备软件可信性设计准则研究

1）基于缺陷收集和缺陷模式研究，考虑避错、容错、查错、改错 4 种软件可信性设计技术，提出软件研制过程的需求分析阶段、设计阶段、编码阶段、测试阶段的可信性设计准则；

2）针对每部分设计准则，给出准则示例，即从满足设计准则时可采取的设计措施方面对设计准则的应用进行细化。

3）建立舰船装备软件可信性设计准则、准则示例数据库及相应的数据库管理工具。

2.3 舰船装备 SFMEA/SFTA 分析技术研究

1）基于系统层次结构及依赖关系的系统级 SFMEA 方法。区分嵌入式软－硬件系统的软－硬件功能交叉、不易分割的情况，以及软件系统任务与硬件系统独立、可分割两种情况，分别研究基于系统层次结构及依赖关系的系统级 SFMEA 方法，包括系统层次结构及依赖关系的获取，以及系统级 SFMEA 的实施步骤和方法。

2）舰船装备软件详细级 SFMEA 分析技术研究。在系统级 SFMEA 的研究基础上，研究系统级 SFMEA 与详细级 SFMEA 接口、从而由系统级 SFMEA 分析结果到详细级 SFMEA 实施的步骤和方法，给出应用示例。

3）舰船装备软件 SFMEA/SFTA 综合分析方法研究。结合 SFMEA 的研究基础，研究舰船装备软件 SFMEA 与 SFTA 综合分析方法的研究，包括正向综合分析与逆向综合分析的实施步骤和方法[6]。

4）舰船装备软件 SFMEA/SFTA 分析辅助工具开发。根据技术方法，实现 SFMEA 计算机辅助分析工具，SFMEA/SFTA 综合分析辅助工具。

3 舰船装备软件缺陷模式研究

舰船装备软件缺陷收集、缺陷模式研究包括收集舰船装备软件缺陷信息、舰船装备软件缺陷分类研究、舰船装备软件缺陷模式特征知识库的研究以及基于软件缺陷模式特征知识库的软件失效推理技术的研究。本项内容的主要研究方案如图 2 所示。

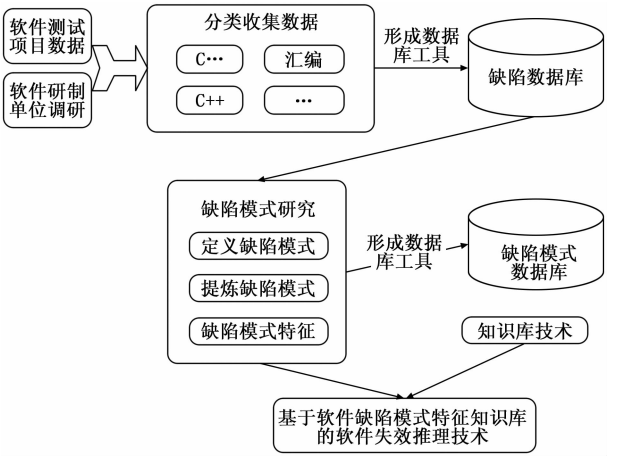

图 2 舰船装备软件缺陷模式研究方案

首先对舰船装备软件缺陷进行收集：主要包括 C、C++、汇编语言实现的各种实时控制、数据解算系统等。数据的来源主要依靠两种方式：软件测评机构的测试项目数据以及对软件研制单位调研。

其次，在缺陷收集的基础上，研究舰船装备软件缺陷的分类。分析现有的各类方法侧重点及适用条件，得出各自的优缺点和适用范围。在分析的基础上，选取采用其中一种分类方式为主，提炼舰船装备软件缺陷模式及模式特征，并根据其他分类，对该模式及模式特征进行补充完善。软件缺陷分类参考以下几种方式：

1）基于软件错误来源的软件缺陷分类方法；

2）基于错误性质的软件缺陷分类方法；

3）基于软件生命周期活动软件缺陷分类方法；

4）基于某类特定软件研究软件缺陷分类方法。

然后，根据提炼的舰船装备软件缺陷模式及特征，运用知识库技术，考虑使用静态分析手段，开展基于软件缺陷模式特征知识库的软件失效推理技术的研究，提出进行失效推理基本方法和思路。

最后，对研究形成的缺陷数据及缺陷模式数据建立数据库系统，提供便捷的查询、更新功能。

4　舰船装备软件可信性设计准则

本部分主要提出软件研制过程的需求分析阶段、设计阶段、编码阶段、测试阶段的可信性设计准则、准则细化以及建立舰船装备软件可信性设计准则、准则示例数据库系统。主要技术方案如图 3 所示。

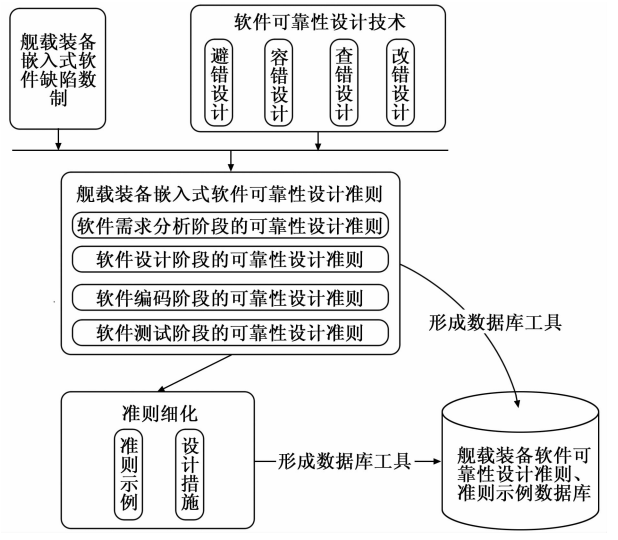

图 3　软件可信性设计准则研究方案

首先，基于本项目第一部分的研究中的数据收集，以舰船装备软件缺陷为基础，分析舰船装备软件研制过程的需求分析、设计、编码开发、测试各阶段涉及到的缺陷模式。软件可靠性设计的实质是在常规的软件设计中，应用各种必须的方法和技术，使程序的设计在兼顾用户的各种需求时，全面满足软件的可靠性要求[7]。软件可靠性设计应和软件的常规设计紧密结合，贯穿在软件常规设计的始终。通过采用避错、容错、查错、改错等可靠性设计方法，使软件产品在设计过程中不出现错误或少出现错误，使程序在运行中自动查找存在的错误，以及使错误发生时不影响系统的特性，或使影响限制在容许的范围内，从而提高软件的可靠性。

其次，分析各阶段所涉及缺陷模式的产生原因，从避错、容错、查错、改错 4 种软件可信性设计技术角度进行考虑，参考《GJB/Z 102 软件可信性安全性设计准则》等资料，提出针对各个阶段所涉及缺陷模式的预防或改进措施，将这些措施提炼形成各设计阶段的可信性设计准则。

1）在各种舰船装备嵌入式软件可靠性设计方法的指导下，以预防各舰船装备软件缺陷模式为目标，结合各种成熟先进的软件工程方法和技术，通过分解、分类、分层的机制，将预防措施转化为舰船装备嵌入式软件可信性设计准则。

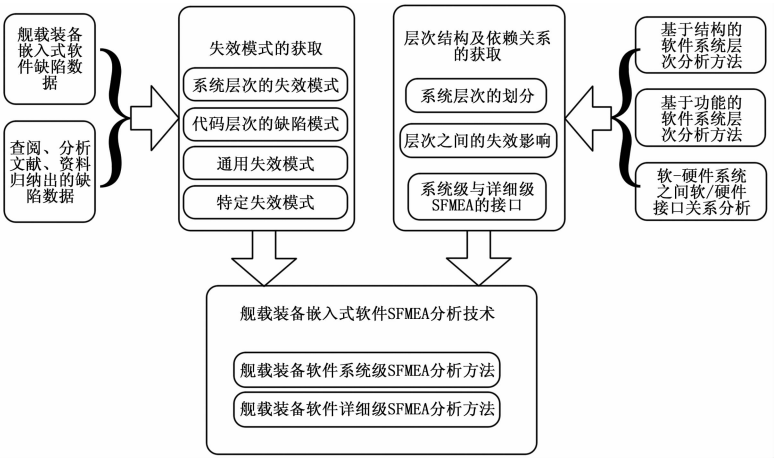

图 4　舰船装备 SFMEA 分析技术研究方案

2）收录部分 GJB/Z102A－2012 的设计准则，加以补充和细化，形成舰船装备嵌入式软件可信性设计准则。GJB/Z102－1997《软件可靠性和安全性设计准则》讲述的概念宽泛，可操作性不强。2012 年，总装备部发布了 GJB/Z102A《军用软件安全性设计指南》，标准的细化和可操作性程度大大提升。经过分析对比，本文中所提出的部分准则与该指南存在少量重叠和交叉，因此，在该标准发布之后，本文又进行了补充完善。本文“安全和保密需求完整性准则、配合硬件进行处理的若干设计考虑、中断设计准则、安全关键功能的设计、安全关键信息的设计、安全关键接口的设计”基本直接来源于 GJB102A，补充了应用示例；设计阶段的其他软件可信性设计准则根据本文第 2 章中所提出的可靠性设计方法导出，另一方面，也一定程度上参考了 GJB102A 的“容错和容失效的设计、接口设计、人机界面设计、通讯设计、模块设计”等，加以补充细化，形成设计准则。

3）收集实践证明有效的软件工程领域的设计技术和方法，对形成的舰船装备嵌入式软件可信性设计准则进行补充。

4）参考相关军用标准的要求，对测试阶段的软件可信性设计准则进行补充。

然后，对典型可信性设计准则，给出准则示例，即从满足设计准则时可采取的设计措施方面细化设计准则，保证软件可信性设计准则的实用性。对本项研究形成的可信性准则及准则示例数据建立数据库系统，提供便捷的查询、更新功能。

最后，软件开发工程化中应用可信性设计准则。采用软件工程方法是软件可信性设计的前提。应特别注意以下几点：

1）软件开发规范化。应按照 GJB 2786A－2009《军用软件开发通用要求》和 GJB438B－2009《军用软件开发文

档通用要求》的规定，将软件开发过程分为若干阶段，每个阶段软件开发人员间相互配合编制必要的文档，并进行检查、分析和评审，严格实行配置管理。图形符号、程序构造及表示应符合 GB1526 和 GB13502 的规定。

2）软件开发人员间（包括系统设计人员、需求分析人员、设计人员及编码人员）应采用统一的方法（N 版本程序设计中要求相异性设计除外）。尽可能采用先进、适用的软件开发工具，并确保开发工具免受计算机病毒侵害。

3）加强软件检查和测试。应尽早开展软件检查和测试，采取措施（如自检、互检、专检相结合的“三检制”，制定设计检查单等）使检查工作切实有效，软件测试应达到规定的要求[8]。

5 舰船装备 SFMEA 分析技术

5.1 系统级 SFMEA

进行 SFMEA 分析的基础包括两个方面，第一是获取系统的各种失效模式，第二是确定所采用的分析技术。主要技术方案如图 4 所示。

本论文中 SFMEA 基于两个方面考虑：一方面是提供舰船装备失效模式的提炼方法；另一方面是针对现有 SFMEA 分析方法的不足，给出适用于舰船装备嵌入式软－硬件系统的软件 FMEA 分析方法和步骤。在舰船装备失效模式的提炼方法研究中，考虑以下方式：

1）基于本项目第一部分的研究内容中的缺陷及缺陷分类数据，分析待 SFMEA 的系统属于哪个类别，检索该类别软件所有的缺陷数据，由缺陷数据推导可能产生的失效模式；

2）此外，从“通用失效模式”和“特定失效模式”两个方面考虑来引导分析人员获取失效模式。

其次，在舰船装备嵌入式软－硬件系统的软件 FMEA 分析方法研究中，研究系统层次结构划分以及依赖关系的获取方法，在此基础上给出舰船装备软件系统级 SFMEA 分析方法及步骤。系统层次结构划分以及依赖关系的获取综合考虑以下 3 个方面：

1）基于软件结构的系统层次划分法，包括软件程序的逻辑控制结构以及数据流的依赖关系。可以依据软件的设计流程图得出。

2）基于功能的软件系统层次划分法，包括系统功能、功能点划分以及功能、功能点之间的层次、依赖关系。可以参考软件的使用剖面方式来对系统功能进行层次划分及依赖关系描述。

3）软－硬件系统之间软/硬件接口关系分析，包括分析舰船装备嵌入式软－硬件系统的软件和硬件之间相互作用，分析各自失效所能产生的影响，以及影响的传递方式。可以考虑在分析过程中，将与软件存在着制约关系的硬件部分看作一个软件模块的方式，来考虑软－硬件之间的控制及依赖关系。

5.2 详细级 SFMEA

系统级 SFMEA 之后，研究系统级 SFMEA 与详细级 SFMEA 分析方法的接口关系，并针对详细级 SFMEA 涉及复杂多样的程序结构，分析过程复杂、失效模式数目繁多的现状，采取以系统级 SFMEA 分析结果指导详细级 SFMEA 过程，进行详细级 SFMEA 分析策略制定，给出详细级 SFMEA 的实施过程和方法。

对于软件详细级 FMEA 来说，由于软件代码量庞大，软件部件之间的逻辑关系不明显，且比较复杂，如果不进行有针对性的选择分析，对软件系统的每一部分都深入到基本的语句结点，将导致分析过程复杂、失效模式数目繁多等问题。因此，如何开展软件详细级 FMEA 成为技术难点之一。

软件详细级 FMEA 技术与方法如图 5 所示，方法被总结为四步：确定分析层次及模块、制定分析规则及失效模式、建立变量线索、影响分析及改进措施制定。

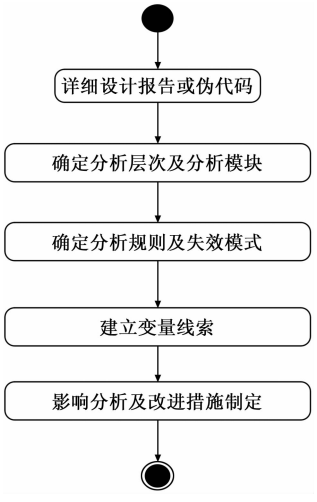

图 5 详细级 SFMEA 分析方法

5.2.1 确定分析层次及分析模块

为了实现与系统级 SFMEA 的结合，推荐以系统级 SFMEA 的底层作为分析层次。在选定了层次后，具体选择哪个模块进行详细级 SFMEA 可以依据以下指导原则：1）根据系统级 SFMEA 分析结果，存在严酷度较高或存在较大影响的失效模式的模块；2）系统的核心模块，实现其主要功能；3）与其他模块有较多的交互，需要处理较多输入数据，交联关系比较复杂；4）模块实现的逻辑比较复杂。

5.2.2 确定分析规则及失效模式

在选定好分析层次及分析模块后，进一步的确定分析规则，而不是无针对性的对所有变量、算法等都进行分析（这样的分析仍然工作量大、无针对性、效果不理想）。分析规则的制定考两个方面：1）一方面依据系统级 SFMEA 分析中失效模式的失效原因，重点选取相关的规则；2）根据分析的代码不同而分别制定。每一组规则都用于每一个特定的分析，以下是几条典型的分析规则：1）一次只分析一种失效模式；2）只分析变量失效；3）只分析输入变量；4）重点分析影响逻辑的变量。基本的一套分析规则制定以后，则可以根据软件代码缺陷及缺陷模式的相关研究，得

出本次分析的各种失效模式。

5.2.3　建立变量线索

由于详细级 FMEA 是在给定的模块内分析，因此变量线索就是输入变量经过一系列处理变为模块输出的途径。通过分析变量在模块内的读写过程，就能把握住变量的处理流程。建立变量线索可以快速跟踪失效对模块的影响。变量线索的表现形式是各种表格。常用的表格有：模块定义表、函数定义表、变量定义表，变量使用表、函数调用表[9]。

5.2.4　影响分析及改进措施制定

通过建立变量线索，能够快速把握一个变量失效模式对待分析模块的影响，同时建立软件执行路径，能够得出该模块的处理结果与系统的关系，最终明确该变量失效模式对系统的影响，并根据影响分析制定相应的改进措施。在影响分析过程中可以结合系统级 FMEA 分析的结果，以确定对系统的影响。

5.3　SFMEA 与 SFTA 综合分析

软件故障树分析（SFTA）是一种自顶向下的软件可信性分析方法[10]，即从软件系统不希望发生的事件（顶事件），向下逐步追查导致顶事件发生的原因，直至基本事件（底事件）。在软件 FMEA 的基础上，利用 FMEA 对系统中单一故障模式的归纳分析结果，依据 FMEA 中的严酷度级别，从高严酷度级别所对应的故障影响中选择一个或多个严酷度作为故障树的顶事件，建立系统的故障树，分析并补充失效原因，用软件 FTA 树形结构图可以更加直观的表达各种失效原因之间的逻辑关系，使失效原因的分析更加彻底，从而在制定失效措施时，能够考虑到多点失效的逻辑关联，提出更为合理的该进建议。

6　技术应用

6.1　工具研制

通过本文方法，研制技术平台，具备数据管理更新、分类查询等各项功能，便于操作使用；具备层次依赖模型建模、SFMEA 辅助填表等各项需求规定的功能，界面美观便于操作，对 SFMEA 有很大的辅助作用，如图 6 所示。

其主要功能需求如下：

1）工程管理部分主要负责工程创建与删除、项目模型管理、分析级别管理等；

2）软件模型建模与分析部分主要用于辅助完成软件层次依赖模型构造、模型属性信息输入、遍历分析等；

3）SFMEA 辅助填表模块包括原因线索显示、影响线索显示、SFMEA 表格信息显示、SFMEA 信息管理等；

4）辅助分析数据库部分主要用于收集和管理可信性分析过程中所需的失效模式、失效原因、设计准则等数据；

5）信息输出包括用于输出 SFMEA 报表等报告；

6）系统帮助模块用于指导 SFMEA 与 SFTA 综合分析和软件使用。

6.2　准则示例

本技术成果形成的缺陷模式和设计准则较多，以“性能需求完整性准则”以及相关“示例”对成果进行展示。性能需求完整性准则有以下几方面：

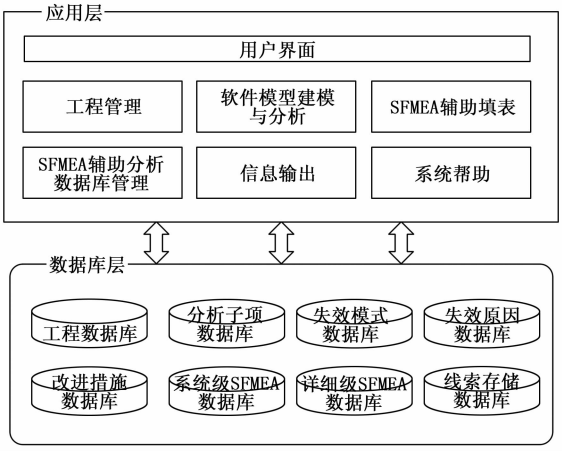

图 6　舰船装备软件可信性分析设计工具

1）定量描述软件系统应满足的具体性能需求。如处理数据的最大容量、精度要求、从询问到响应所允许的最长时间以及适应用户需求变化的能力等。

2）如有容量要求，须确定系统的容量要求。一般包括处理的记录数和处理数据的最大容量等。

3）如有精度要求，须确定其精度要求。一般包括数据或数值计算的精度要求、数据传输的精度要求等。

4）如有时间特性要求，须确定其时间特性要求。一般包括处理时间、响应时间等。

5）对于实时嵌入式软件，必须说明的实时性要求。一般包括周期任务处理时间、中断响应时间、采集数据时间、两次输出间隔时间等。

6）制定的性能参数，尤其是安全关键软件或功能的性能参数，应在需求分析完成后，与用户进一步确认；若不能确定具体值，一般应提出适当的余量要求，以保证设计正确，舰船装备嵌入式软件一般要求留有不少于 20％的余量。

举例 1：以下是一些软件的性能要求。

存储容量：满负荷运行时占用的内存资源不超过 100 M，1 分钟内处理的记录数为 10000 条，5 分钟内导入的数据大小 10 M。

处理时间：每 2 秒完成一次对 25 个传感器采集信号的轮询，每 2 秒将轮询结果上传至数据处理中心。

数据精度：向外输出一个固定的电压信号时，数据处理误差不大于 0.05 V。

并发能力：系统支持 100 个用户同时上传数据。

举例 2：对于时序安排的余量考虑：软件工作的时序处理要求，要结合具体的被控对象确定各种周期。当各种周期在时间轴上安排不下时，应要求采取更高性能的 CPU 或多 CPU 并行处理，以确保软件设计时的工作时序之间留有足够的余量[11]。一般包括采样周期、数据处理周期、控制周期、自诊断周期、输入输出周期等。

（下转第 170 页）