航天科技图书出版基金资助出版

航天软件需求工程

刘 姝 程 胜 编著

中国宇航出版社

航天科技图书出版基金资助出版

航天软件需求工程

刘 姝 程 胜 编著

中国宇航出版社
·北京·

图书在版编目（CIP）数据

航天软件需求工程 / 刘姝，程胜编著. --北京 : 中国宇航出版社，2016.8

ISBN 978-7-5159-1174-8

Ⅰ.①航… Ⅱ.①刘… ②程… Ⅲ.①航天系统工程—软件需求 Ⅳ.①V57②TP311.52

中国版本图书馆 CIP 数据核字（2016）第 217709 号

责任编辑　侯丽平　　**封面设计**　宇星文化

出　版 发　行	中国宇航出版社		
社　址	北京市阜成路 8 号	邮　编	100830
	(010)60286808		(010)68768548
网　址	www.caphbook.com		
经　销	新华书店		
发行部	(010)60286888		(010)68371900
	(010)60286887		(010)60286804(传真)
零售店	读者服务部		
	(010)68371105		
承　印	北京画中画印刷有限公司		
版　次	2016 年 8 月第 1 版		2016 年 8 月第 1 次印刷
规　格	880×1230	开　本	1/32
印　张	9.25	字　数	266 千字
书　号	ISBN 978-7-5159-1174-8		
定　价	98.00 元		

航天科技图书出版基金简介

航天科技图书出版基金是由中国航天科技集团公司于2007年设立的，旨在鼓励航天科技人员著书立说，不断积累和传承航天科技知识，为航天事业提供知识储备和技术支持，繁荣航天科技图书出版工作，促进航天事业又好又快地发展。基金资助项目由航天科技图书出版基金评审委员会审定，由中国宇航出版社出版。

申请出版基金资助的项目包括航天基础理论著作，航天工程技术著作，航天科技工具书，航天型号管理经验与管理思想集萃，世界航天各学科前沿技术发展译著以及有代表性的科研生产、经营管理译著，向社会公众普及航天知识、宣传航天文化的优秀读物等。出版基金每年评审1～2次，资助20～30项。

欢迎广大作者积极申请航天科技图书出版基金。可以登录中国宇航出版社网站，点击“出版基金”专栏查询详情并下载基金申请表；也可以通过电话、信函索取申报指南和基金申请表。

网址：http://www.caphbook.com

电话：(010) 68767205，68768904

前　言

随着航天型号信息化和智能化水平的提升，系统越来越复杂，软件发挥的作用越来越大。软件需求引发的质量问题会带来严重的后果，将直接影响任务成败。系统、全面地了解航天软件需求工程相关的原理、技术和方法，对于提升航天软件研发能力，保证软件质量具有重要意义。

本书立足航天领域，结合国内外研究成果和项目实践，系统地梳理了航天软件需求工程相关的原理、技术和方法，形成完整的知识体系和实施指南，供航天软件设计与开发人员、项目管理人员、质量保证人员等参考。本书共分为7章，各章主要内容说明如下。

第1章介绍软件需求与软件开发过程模型、软件需求工程的基本内容，分析需求与其他过程的关系以及软件需求工程对航天型号任务的重要性。

第2章介绍航天软件需求工程的上下文环境，国内外航天主要标准规范中对需求开发、需求管理的要求。

第3章介绍软件需求开发的过程、方法和工具，涉及从型号任务总体目标到系统、再到分系统的用户需求开发与规格说明，以及软件需求分析与规格说明。

第4章介绍软件需求管理，包括需求追踪、需求优先级排序、需求基线与变更管理以及主流的需求管理相关工具。

第5章围绕软件需求的验证与确认展开，明确其定义和工作内容，并详细介绍验证和确认的方法。

第6章介绍软件安全需求开发与验证。安全需求工程是需求工程的一个重要分支，包括安全需求分析、验证和追踪管理等。

第7章介绍软件需求质量管理与过程改进，描述基于需求的质量定义、质量监测框架和质量测量过程，概述过程改进相关的标准，分析需求过程改进存在的主要问题，并介绍软件需求过程改进的方法。

本书的编写过程，参阅了大量的国内外图书、标准、规范、报告、论文，吸纳借鉴了许多专家和学者的研究成果和实践经验，并得到了北京大学金芝教授、载人航天工程软件专家组许聚常研究员等专家的指导，在此表示衷心的感谢！同时也感谢航天科技图书出版基金的资助和中国宇航出版社的大力支持。

因作者水平有限，书中难免有谬误和不妥之处，恳请同行专家、学者和广大读者批评指正。

作　者

2016年6月

目　录

第 1 章　软件需求与软件需求工程

随着航天型号信息化水平的不断提升，软件的重要性和规模越来越大。据统计，美国国家航空航天局（NASA）的飞行软件规模每 10 年增长一个数量级[1]，我国神舟飞船、运载火箭等航天型号中软件规模也显著增长。软件系统是实现制导导航、遥控遥测、生命保障、科学实验等功能的核心要素，已经成为影响任务成败的决定性因素。

软件需求作为软件研制的基础，在软件生存周期与过程模型中处于重要地位，与项目管理、产品研制、维护和质量保证有紧密关系，对项目的成败起决定作用。软件需求工程是软件工程和系统工程的一个重要分支，对于涉及安全可靠性要求的航天型号复杂软件系统而言，研究软件需求工程方法、技术与实践具有重要的理论意义和实用价值。

1.1　什么是软件需求

需求描述了所要设计、实现和操作的软件系统必要的功能和特征，是软件系统的源头。航天型号系统中的软件需求依赖于型号任务、系统需求、系统划分，可以表示为层次结构，并具有特定的属性。需求是软件生存周期与软件过程模型的重要组成要素，需求过程与其他过程密切关联。

1.1.1　需求的定义与分类

IEEE《软件工程标准词汇表》[2]将需求定义为：

1）用户为解决问题或达到目标所需的条件或特性；

2）系统或系统部件要满足合同、标准、规范或其他正式规定文档所需具有的条件或特性；

3）描述上述的条件或特性的文档说明。

通常，需求来源于用户。用户原指使用系统的人员，可以是组织外部的客户，也可以是本组织上层的系统总体人员。外部客户对软件项目提出的需求称为客户需求；系统总体分配给软件的需求称为分配需求，是系统需求的一个子集。本书中的用户需求泛指这两类需求。用户需求以文档化的单独的“用户需求规格说明”的形式提出。

软件需求分析的对象是用户对软件项目提出的用户需求。经过与用户的交流、协商，软件开发人员将用户提出的需求变为软件需求。软件需求分析就是在用户和软件开发者之间建立对用户需求的共同理解，由软件开发人员进行分析、精化并详细描述后，按照文档规范编写出“软件需求规格说明”。然后，软件开发人员在此基础上开发软件系统，使其与用户最终的要求相适应。

需求是按照层次化结构组织的，如图 1－1 所示，从系统、分系统到每个硬件和软件，需求逐渐细化，这也体现了需求分析的流程。各国航天软件工程标准都对需求采用层次划分方法。NASA 定义的需求层次见图 1－2[3]，第一级的任务需求通过分解得到第二级的分配需求；进一步细化得到第三级的衍生需求，用于招投标或者任务书；第四级是软件开发人员进行需求分析后得到详细的软件需求，用于指导设计和编码。第一级和第二级类似于我国航天软件工程中通常提到的系统需求和分系统需求，第三级对应软件配置项研制任务书，第四级对应软件需求规格说明。

不同类型的软件项目具有不同的特点，如航天器嵌入式系统、地面信息管理系统，应从不同的角度进行需求分析，形成不同的需求视图。软件需求可以进一步分为功能需求、性能需求、接口需求、安全性需求、可靠性需求等。

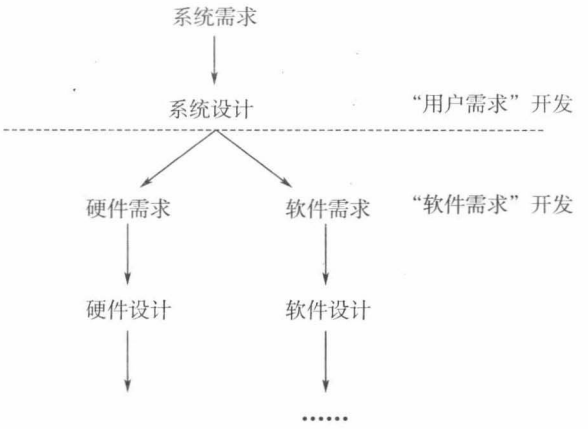

图 1-1　需求开发路径

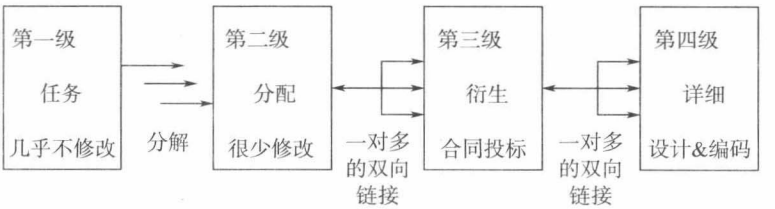

图 1-2　NASA 需求层次定义

需求具有完整性、正确性、无二义性、可行性、有优先级、可跟踪性、可验证性、挥发性等属性。

1.1.1.1　完整性

需求必须将所要实现的功能描述清楚，使开发人员得到设计和实现这些功能所需的所有必要信息。

1.1.1.2　正确性

需求必须准确地陈述其开发的功能。做出需求正确性判断的依据是需求的来源，即上层需求可以用于判断下层需求的正确性，只有客户才能判断用户需求的正确性。

1.1.1.3 无二义性

需求对所有读者都只能有一个明确统一的解释。二义性主要是不同背景的人在传递信息时加入不同的理解导致的。由于自然语言极易导致二义性，所以尽量把需求用简洁明了的语言表达出来。避免二义性的有效方法包括正规评审、形式化描述等。

1.1.1.4 可行性

需求必须是在已知系统和环境的权能和限制范围内可以实施的。为了避免不可行的需求，最好在需求阶段由软件工程人员与需求分析人员或市场人员一起工作，检查技术可行性。

1.1.1.5 有优先级

每项需求、特性或者使用实例要有一个实施优先级以指明它在特定产品中所占的分量。优先级是相对的，可以从业务、技术开发、项目管理3个角度进行划分。

1.1.1.6 可跟踪性

每项需求都应该把客户真正所需要的和最终系统所遵从的标准记录下来，能追溯到客户的输入，与上层需求相对应，以及与代码、测试相对应。

1.1.1.7 可验证性

需求必须可以通过设计测试用例或者其他方法进行验证。如果需求不可验证，确定需求实施是否正确就没有客观依据了。

1.1.1.8 挥发性

需求不是静止的，在软件生存周期中，需求修改的频率和时间即反映了需求的挥发性。

1.1.2 需求在软件开发中的位置

需求阶段在整个软件生存周期中处于最基础、最主要的位置。航天型号软件研发可以采用多种软件过程模型，在不同的模型中，

需求都是驱动软件过程模型的主要因素，需求为其他过程及管理活动奠定了基础。

1.1.2.1　软件生存周期与软件过程模型

软件产品从计划开始，经过开发、设计、使用和维护等活动，直到退役为止的全过程称为软件生存周期。按照软件所处的状态、特征以及软件开发活动，通常可以分为需求分析、设计、实现、测试、维护等阶段。

软件开发过程各阶段之间的关系可以用过程模型表示。软件过程模型是软件开发过程的抽象描述，是软件开发人员经过多年实践形成的步骤和方法。接下来介绍主流的软件过程模型，以便读者清晰地理解需求在软件开发过程中的地位。航天软件开发人员应结合软件的特点选择适当的软件过程模型。

（1）瀑布模型

瀑布模型是软件工程的经典模型，软件开发过程的各个阶段像瀑布一样。如图 1-3 所示，该模型从建立系统需求和软件需求开始，逐步进行阶段转化，开展结构设计、详细设计、编码、测试和维护。瀑布模型按照时间把软件研制分为有序的步骤，推迟了物理实现，而且每个阶段结束时，通过审查确定是否开始下一阶段，便于实现质量保证。

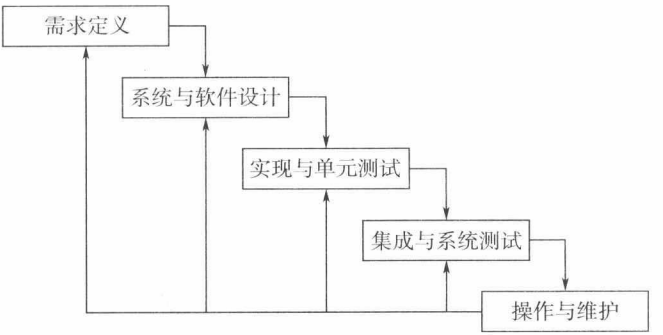

图 1-3　瀑布模型

瀑布模型具有设计和实现分离的特征，适用于需求明确的大型系统开发和嵌入式系统开发。但是，瀑布模型有一定的缺点。例如，在纯瀑布模型中，需求必须在设计开始之前确定，编码开始之前设计必须描述清楚，各个阶段之间没有交叠。但在实际工作中，系统需求不明确、分析人员对于应用领域不熟悉等情况不可避免，在设计或者编码阶段也有可能发现需求错误。

（2）原型模型

原型是开发人员根据用户提出的需求快速开发出的一个样本，向用户展示待开发软件的全部或部分功能和性能。开发者通过原型系统与用户沟通，然后进行进一步的修改、完善，确认软件系统的需求并达成一致理解[4]。原型模型如图 1-4 所示。

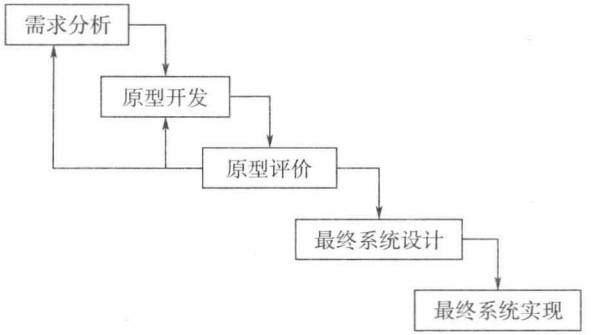

图 1-4 原型模型

原型开发过程中，开发者可以使用自己比较熟悉的语言和开发环境尽快构造原型，便于用户感受实际系统。原型模型有助于获取准确的用户需求，或者进行某种技术和方法的可行性研究；产品开发快，侧重小型系统中系统核心部分的开发或者大型系统的界面沟通。但完善原型时，其他部分会因为迁就原型已有部分，造成结构不合理，影响维护。

（3）增量模型

增量模型融合了瀑布模型的特点，同时适应软件需求变化的特

征，通过不断增加功能形成最终系统。第一个增量往往是核心部分，实现了系统的基本功能。下一个增量的开发计划包括对前一个增量的修改和完善。增量模型如图 1－5 所示。

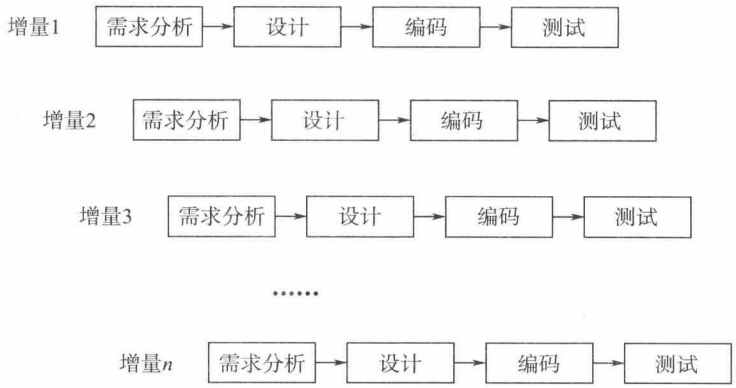

图 1－5　增量模型

采用增量模型时，用户可以很快使用系统，早期增量可以作为系统原型，降低了项目风险。但是，由于功能是递增加入的，对软件体系架构有较高的要求，而且增量的划分、增量大小的确定有时比较困难。如果应用不好，增量模型的灵活性容易退化为边做边改模型。

（4）螺旋模型

螺旋模型是 Boehm 于 1988 年提出的，与增量模型类似，也强调风险分析。如图 1－6 所示，螺旋模型的每个回路表示软件过程的一个阶段，最内层是操作概念分析，然后是软件需求分析、产品设计、详细设计等。每个回路又分为 4 个象限：

1）制订计划，确定软件项目的目标、选择方案，获取系统的约束条件；

2）风险分析，对预选方案进行风险识别与分析，并采取规避风险的措施；

3）工程实施，该阶段确定软件模型，开发软件产品，进行软件