



军用软件的 工程研制与管理

JUNYONG RUANJIAN DE GONGCHENG
YANZHI YU GUANLI

吴清才 郑琪 王首一 编著



国防工业出版社
National Defense Industry Press

.. 014907278

E919

103

军用软件的工程研制与管理

吴清才 郑 琪 王首一 编著



2919

103

国防工业出版社



北航

C1694196

014003278

内 容 简 介

本书共分为 12 章,内容包括:第 1 章软件与软件工程概述;第 2 章到第 8 章,按照软件生命周期的过程,顺序介绍了航天型号软件研制的几个重要阶段的工作内容、方法和质量要求等内容;第 9 章介绍了软件可靠性与安全性的概念、软件研制各阶段的工作内容,并介绍了典型的软件可靠性与安全性方法;第 10 章介绍了软件过程管理的有关概念、基本要求、主要活动、工作内容等有关内容;第 11 章介绍了军用软件定型与鉴定的概念、工作范围、分级管理、组织职责和定型程序;第 12 章重点介绍重用软件的选择、分类、重用程序及其研制要求等。

本书可以为软件研制人员提高软件工程研制水平和效率,为各单位在技改技施、体系建设等方面提供参考。

图书在版编目(CIP)数据

军用软件的工程研制与管理/吴清才,郑琪,王首一编
著. —北京:国防工业出版社,2013.9
ISBN 978-7-118-09019-2

I. ①军... II. ①吴... ②郑... ③王... III. ①军用
计算机—软件工程 IV. ①E919

中国版本图书馆 CIP 数据核字(2013)第 217548 号

※

国防工业出版社 出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100048)

北京嘉恒彩色印刷责任有限公司

新华书店经售

*

开本 710×960 1/16 印张 29¼ 字数 534 千字

2013 年 9 月第 1 版第 1 次印刷 印数 1—2000 册 定价 85.00 元

(本书如有印装错误,我社负责调换)

国防书店:(010)88540777

发行邮购:(010)88540776

发行传真:(010)88540755

发行业务:(010)88540717

序

随着各类装备数字化和智能化程度的不断提高,软件的应用越来越广泛,所起到的作用也越来越重要,软件实现的功能比重逐步增大,“系统信息化、硬件软件化、工程软件化”已经成为一种发展趋势。同时,由于软件功能需求的多样化,软件规模越来越大,软件结构越来越复杂,软件质量与可靠性对整个系统的影响也越来越大,是影响成败的核心因素之一。软件是人的智力活动的结果,是知识和技术集成于一体的信息化产品。软件的质量管理和控制只能通过过程控制来保证,由此对软件的工程研制和管理规范性提出了较高要求。

要提高软件研制效率、保证软件质量,就必须按照软件工程化的要求开展软件研制和管理工作的,在整个软件生命周期内实施全过程的风险分析和控制。因此,提高我国软件研制能力和软件工程化水平,是软件研制能力建设的重要内容。

20世纪90年代,我国开始实施载人航天工程,工程领导在研制工作初期就深刻认识到,软件的“个人作坊”、“自拉自唱”研发模式是工程隐患的重要根源,软件的“不透明”、“不可控”是工程质量的天敌,充分认识到“抓工程不抓软件不行,抓软件不抓工程化不行,抓工程化不抓质量不行,抓质量不抓管理不行,抓管理不抓领导不行”,提出软件工程化是确保工程质量的必由之路,率先推进实施软件工程化,提出了软件研制管理要求和技术规范。1996年阿里安-5运载火箭发射爆炸事件进一步警示了软件质量问题的严重性,人们更加清醒地认识到,软件工程化中每一个环节的失误都会带来毁灭性失败,软件问题既是技术问题,更是管理问题。我们根据这些经验和教训,进一步在软件系统分析与设计、软件安全性可靠性设计、软件等级确定、软件第三方评测等方面完善了软件研制管理要求和标准规范。通过工程实践,实现了软件质量的突破,有效地保障了历次载人航天飞行任务的成功。载人航天的实践成果也在航天和其它行业得到了广泛推广应用,我国航天行业逐步形成了一系列软件工程研制管理的标准和规范,为我国航天软件研制能力的整体提升起到了重要作用。

目前,我国各类装备研制任务不断发展,对软件研制能力要求不断提高,同

时软件技术也在突飞猛进。但我国软件研制单位的研制能力和技术水平参差不齐,研制能力还存在差距,特别是软件管理能力差距更大,同时由于研制队伍的新老交替,软件工程研制经验缺乏。在这种形势下,应该不断学习国际先进技术,总结国内软件研制成功经验,编写一些好的、值得推广的书籍和教材供大家借鉴,达到保持并不断提高软件工程研制和管理水平的目的。

本书介绍了国内外软件研制的标准规范,总结了软件研制实践中管理方面的经验教训,反映了军用软件的特殊性,结构合理,内容丰富,实用性强,既体现了技术的先进性,又结合了我国军用软件工程研制和管理实际情况以及作者多年的型号任务研制工作实践,凝结了作者的心血。相信这本书能为提高我国军用软件工程研制和管理水平起到积极作用。

周建

2013年11月5日

前 言

随着军用产品数字化和智能化程度的不断提高,软件在军用产品中的应用越来越广泛,规模和复杂性越来越大,其应用范围涉及到陆、海、空、二炮等各领域的车辆、舰船、飞机、导弹、火箭、卫星、飞船等型号的科研生产任务,其质量与可靠性对任务成败的影响也越来越大。目前,软件产品已经成为军用型号任务的一种重要产品类型。要提高军用软件研制效率、保障军用软件质量,就必须实施软件工程化,按照软件工程要求开展研制和管理工作,实施全过程、全要素的产品保证。

在 20 世纪 90 年代,通过载人航天工程开始推行软件工程化工作,并逐步在其他各领域推广应用,对我国军用软件工程研制和管理的规范性起到了引领作用,承担军用软件研制任务的中电集团、中航集团、船舶集团、航天科技集团、航天科工集团等大型军工集团及其所属院所积极探索军用软件工程研制和管理经验教训,并结合自身任务软件特点发布了一系列软件研制和管理规范,并在实践中不断完善,积极推动了软件工程化程度,保证了任务软件研制质量,对任务的成功起到了巨大的支持和保证作用。但是,与军用型号任务不断发展的需求以及与国外的先进技术水平相比,我们的软件工程化水平还存在不小的差距。随着武器装备信息化水平的提升,软件研制的工作量越来越大,质量要求越来越高,而目前各军用软件承制单位的技术水平和管理能力参差不齐,并且由于人员的新老交替,有大量的新手加入到军用软件研制的队伍中来,缺乏工程经验。在这种形势下,我们必须努力学习国内外的先进技术,不断总结已有的成功经验,并做好培训工作,进一步宣贯软件工程思想,提高软件工程研制和管理水平以及实施能力。

本人从事国家载人航天工程、卫星研制、武器装备研制和管理工作 20 余年,曾担任中国空间技术研究院软件专家组副组长,目前为中国科学院先导卫星工程专项软件专家组责任专家、总装备部军用软件研制能力评价员,具有扎实的理论基础、军用软件研制和管理能力和丰富的实践经验,在中国空间技术研究院作为 GJB 5000A 的倡导者和实践者,推进实施全院军用软件研制能力改进工作。目前,全部软件研制单位均通过了总装备部军用软件研制能力相应等级的评价,并形成了软件研制和管理体系,在各型号任务中得到广泛推广和应用,在军用软件研制与管理领域获得国防科技进步三等奖,为承担军用软件研制的航空、航

天、中电等所属集团、院、所、高校的研制和管理人员授课 50 余次,曾参加 20 余家单位军用软件研制能力的评价工作,在航空、航天等军用软件研制和管理领域有较高的声誉。本人和郑琪、王首一同志结合多年工作经验和军用软件研制和管理特点编写了本书。

本书结构合理,内容丰富,既体现了技术的先进性,又结合了军用软件研制和管理的实际情况,对规范军用软件研制的技术管理、质量控制和监督具有较强的指导作用,对提高军用软件研制质量和承制单位军用软件研制能力具有重要的促进作用,也可以作为军事监督代表和上级主管部门监督检查承制单位和型号软件研制能力和产品质量的借鉴,相信本书能为提高军用软件工程化水平起到重要作用。

本书适用于军用软件研制人员、管理人员、质量管理人员、型号三师系统人员、军事监督代表、上级主管部门,可以作为软件研制和监督检查的参考,希望能为提高军用软件研制质量、保障型号任务成功贡献力量!

本书在编写过程中,参阅了大量的国内外图书、标准、规范、报告、论文,吸纳并借鉴了许多专家和学者的研究成果和实践经验,在此表示衷心感谢!由于本人水平有限,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。

吴清才

2013 年 4 月

目 录

第 1 章 软件与软件工程概述	1
1.1 软件概述	1
1.1.1 软件定义	1
1.1.2 软件特点	2
1.2 软件工程概述	5
1.2.1 软件工程定义	5
1.2.2 软件工程的基本原则	7
1.2.3 软件工程的工作内容	7
1.2.4 软件能力成熟度模型	12
1.2.5 软件过程改进体系建设	18
1.3 软件工程化阶段	19
1.3.1 软件研制阶段划分	19
1.3.2 软件研制各阶段的技术工作	20
1.4 软件研制的组织与管理	26
1.4.1 软件研制的组织与职责	26
1.4.2 软件研制的策划	26
1.4.3 软件研制各阶段的管理任务	27
第 2 章 软件系统分析与设计	31
2.1 概述	31
2.1.1 系统分析与设计的目的	31
2.1.2 系统分析与设计的任务	31
2.2 软件系统分析与设计要求	32
2.3 软件关键等级的确定	32
2.4 软件任务书的一般要求	35
2.4.1 系统需求分析与设计阶段与软件任务书有关的任务	35
2.4.2 软件任务书的基本要求	36
2.5 软件系统分析与设计阶段的工作产品	39

2.6	软件系统分析与设计的验证与确认	39
2.6.1	活动概述	39
2.6.2	任务描述	40
2.6.3	通过准则	41
第3章	软件需求分析	42
3.1	概述	42
3.1.1	需求分析的目的	42
3.1.2	需求分析阶段的主要任务	42
3.1.3	软件需求分析的重要性	43
3.1.4	软件需求分析工作的特点	44
3.2	软件需求分析的工作过程	44
3.2.1	需求信息的获取和记录	46
3.2.2	需求分析	46
3.2.3	需求评审	47
3.2.4	需求管理	48
3.3	软件需求规格说明编写要求	48
3.3.1	需求规格说明的主要内容	48
3.3.2	“软件需求规格说明”的格式	55
3.3.3	需求规格说明的质量要求	58
3.4	软件需求文档中经常出现的问题	59
3.4.1	一般问题	59
3.4.2	软件功能方面的问题	59
3.4.3	需求中实体方面的问题	59
3.4.4	性能需求方面的问题	60
3.4.5	安全性可靠性方面的问题	60
3.4.6	需求规格说明的内容范围问题	60
3.5	“软件需求规格说明”的检查和验证方法	61
3.5.1	人工检查	61
3.5.2	采用结构化方法检查	63
3.5.3	采用仿真模型检查	65
3.5.4	采用形式化方法检查	65
3.6	软件需求分析的验证与确认	66
3.6.1	活动概述	66
3.6.2	任务描述	67
3.6.3	通过准则	69

第 4 章 软件概要设计	70
4.1 概述	70
4.2 结构化设计的概念和原则	71
4.2.1 抽象与细化求精	71
4.2.2 模块化与信息隐蔽	71
4.2.3 有效的模块设计——模块独立性	72
4.2.4 软件的体系结构	74
4.2.5 程序结构	75
4.3 概要设计阶段的工作过程	75
4.3.1 复核并理解软件需求文档	76
4.3.2 建立物理模型	76
4.3.3 编写概要设计说明	78
4.3.4 编写组装测试初步计划	78
4.3.5 概要设计阶段评审	78
4.4 软件的结构化设计的图形工具	78
4.4.1 HIPO 图	78
4.4.2 结构图	79
4.4.3 状态转移表	81
4.5 面向数据流的设计方法	82
4.5.1 变换型结构映射	82
4.5.2 事务型结构映射	84
4.5.3 优化程序结构设计	86
4.6 实时嵌入系统软件的设计	88
4.6.1 实时系统概述	88
4.6.2 任务调度策略	90
4.6.3 实时系统的软件任务结构化设计	94
4.7 概要设计的质量要求	97
4.8 概要设计文档的基本内容	98
4.9 概要设计阶段的验证与确认	102
4.9.1 活动概述	102
4.9.2 任务描述	103
4.9.3 通过准则	105
第 5 章 软件详细设计	106
5.1 概述	106

5.1.1	详细设计的基本概念	106
5.1.2	详细设计的任务和内容	107
5.1.3	详细设计文档的用途	107
5.1.4	详细设计的质量要求	107
5.2	详细设计工作过程	108
5.2.1	理解概要设计	109
5.2.2	细化软件部件形成软件单元	109
5.2.3	规定软件单元间接口	110
5.2.4	设计算法和细节	110
5.2.5	进行过程描述	110
5.2.6	进行可靠性安全性设计	110
5.2.7	编写详细设计说明	110
5.2.8	编写初步单元测试计划	110
5.2.9	建立并填写单元开发卷宗	111
5.2.10	详细设计评审	111
5.3	详细设计方法和技术	111
5.3.1	结构化程序设计	111
5.3.2	软件安全性、可靠性设计	112
5.3.3	详细设计工具	113
5.4	详细设计文档内容	118
5.5	详细设计阶段的验证与确认	119
5.5.1	活动概述	119
5.5.2	任务描述	120
5.5.3	通过准则	122
第 6 章	软件实现	123
6.1	理解“详细设计”	124
6.2	编程和编译/汇编	124
6.3	代码调试	124
6.4	静态分析	124
6.5	代码走查	127
6.5.1	代码走查的特点	127
6.5.2	代码走查的目的	128
6.5.3	代码走查的目标	128
6.5.4	软件工程中的几种走查方式	128
6.5.5	走查的分类	128

6.5.6	走查方法和步骤	128
6.5.7	走查发现的常见问题	128
6.5.8	走查中的重点和难点	129
6.6	单元测试	131
6.7	安全性关键单元检查和评审	132
6.8	软件实现的技术和方法	132
6.8.1	结构化编程方法	132
6.8.2	一般软件的编程规则	133
6.8.3	安全性关键软件的编程规则	138
6.9	编程的质量要求	139
6.10	典型工作产品	139
6.11	软件实现阶段验证与确认	139
6.11.1	活动概述	139
6.11.2	任务描述	140
6.11.3	通过准则	143
第7章	软件测试	144
7.1	概述	144
7.1.1	软件测试的基本概念	144
7.1.2	软件测试的基本原则	145
7.1.3	软件测试的重要性和局限性	146
7.2	软件测试过程	147
7.3	各软件研制阶段的测试活动及要求	151
7.3.1	单元测试	151
7.3.2	组装测试	153
7.3.3	确认测试	155
7.3.4	第三方独立确认测试	156
7.3.5	系统测试	161
7.3.6	回归测试	163
7.3.7	其他阶段的测试	164
7.4	主要测试内容	165
7.4.1	功能测试	166
7.4.2	性能测试	168
7.4.3	边界测试和余量测试	169
7.4.4	强度测试	169
7.4.5	可靠性测试和安全性测试	170

7.4.6	其他常见测试内容	170
7.4.7	各测试类型应开展的测试内容	170
7.5	软件测试技术及工具	171
7.5.1	静态测试技术	172
7.5.2	测试用例设计技术	173
7.5.3	测试覆盖率分析技术	176
7.5.4	嵌入式测试环境搭建技术	178
7.5.5	软件测试工具与环境	179
7.6	测试质量的控制	181
7.6.1	测试过程的控制要素	181
7.6.2	测试机构的组织管理	182
7.6.3	测试组织的测试能力成熟度模型	183
7.7	软件测试阶段验证与确认	185
7.7.1	软件部件测试阶段验证与确认	185
7.7.2	软件配置项测试阶段验证与确认	188
7.7.3	通过准则	193
7.8	分系统测试阶段验证与确认	194
7.8.1	入口准则	194
7.8.2	活动概述	194
7.8.3	任务描述	195
7.8.4	通过准则	198
7.9	系统试验验证阶段验证与确认	198
7.9.1	入口准则	198
7.9.2	活动概述	198
7.9.3	任务描述	200
7.9.4	通过准则	202
第8章	软件验收、交付与维护	203
8.1	概述	203
8.2	软件产品的验收和交付	203
8.2.1	验收的级别和条件	203
8.2.2	验收和交付过程	204
8.2.3	软件研制报告	208
8.3	软件维护	209

8.3.1	软件维护的相关知识	209
8.3.2	军用软件维护的一般要求	212
8.3.3	软件的可维护性	213
8.3.4	提高软件可维护性的方法	215
8.3.5	软件维护的过程	218
8.4	软件维护的其他问题	220
8.4.1	维护工具	220
8.4.2	软件维护与软件重新设计	220
第9章	软件可靠性与安全性	221
9.1	概述	221
9.1.1	软件可靠性	221
9.1.2	软件安全性	222
9.1.3	软件可靠性与软件安全性	223
9.1.4	软件的可靠性和安全性与其他产品的可靠性和安全性	224
9.2	软件失效机理与软件可靠性和安全性措施	224
9.2.1	软件失效机理	224
9.2.2	软件可靠性和安全性措施	227
9.3	软件研制各阶段的软件可靠性和安全性要求	229
9.3.1	系统需求分析和设计	229
9.3.2	软件需求分析	230
9.3.3	软件概要设计	232
9.3.4	软件详细设计	232
9.3.5	嵌入式软件可靠性设计	233
9.3.6	软件实现	244
9.3.7	软件集成和验收测试	245
9.3.8	软件运行和维护	246
9.4	软件可靠性和安全性方法	247
9.4.1	软件故障树分析方法	247
9.4.2	软件故障模式及影响分析	250
9.4.3	恢复块	254
9.4.4	数据冗余	256
9.4.5	软件可靠性和安全性设计检查单	257
9.4.6	软件可靠性度量	260

9.4.7	软件可靠性评价	268
第 10 章	软件项目过程管理	271
10.1	概述	271
10.2	需求管理	273
10.2.1	目的	273
10.2.2	主要内容	273
10.2.3	工作程序	274
10.2.4	主要模板和检查单	280
10.3	项目策划	284
10.3.1	目的	284
10.3.2	主要工作内容	285
10.3.3	工作程序	286
10.3.4	软件生存周期模型及选择指南	292
10.3.5	软件项目估计方法指南	299
10.3.6	主要模板和检查单	309
10.4	软件配置管理	314
10.4.1	目的	314
10.4.2	术语定义	315
10.4.3	配置管理库	316
10.4.4	配置管理的组织结构和职责	317
10.4.5	配置管理工具	318
10.4.6	配置管理主要工作内容	318
10.4.7	工作程序	319
10.4.8	主要模板和检查单	332
10.5	项目监督与控制	345
10.5.1	目的	345
10.5.2	工作内容	345
10.5.3	工作程序	346
10.5.4	计划变更判断准则	348
10.5.5	主要模板和检查单	349
10.6	过程和产品质量保证	353
10.6.1	目的	353
10.6.2	工作内容	353

10.6.3	主要活动	353
10.6.4	验证	360
10.6.5	主要模板和检查单示例	361
10.7	验证与确认	383
10.7.1	概述	383
10.7.2	验证	383
10.7.3	确认	386
10.7.4	验证与确认方法	388
10.8	风险管理	405
10.8.1	目的	405
10.8.2	风险管理内容	406
10.8.3	风险管理过程	407
10.8.4	风险分析方法	417
10.9	外协单位的控制	417
第 11 章	军用软件定型与鉴定	418
11.1	组织实施	418
11.2	定型和鉴定范围	418
11.2.1	定型范围	418
11.2.2	鉴定范围	419
11.3	定型分级	419
11.4	组织职责	420
11.4.1	软件承制单位上级主管部门	420
11.4.2	软件承制单位	420
11.4.3	软件定型测评机构	421
11.5	定型程序	421
11.5.1	软件定型测评	421
11.5.2	部队试验试用	426
11.5.3	软件定型与鉴定申请和审批	428
11.5.4	软件定型与鉴定工作的监督	432
第 12 章	软件重用	433
12.1	重用软件的选择	433
12.2	重用软件的分类	433

12.3	重用软件的研制要求	434
12.3.1	Ⅳ类软件研制要求	434
12.3.2	Ⅲ类软件研制要求	435
12.3.3	Ⅱ类软件研制要求	436
12.3.4	Ⅰ类软件研制要求	437
12.3.5	商用成品软件研制要求	438
12.4	重用软件审批程序	439
12.4.1	软件重用可行性分析	439
12.4.2	软件重用申请	439
12.4.3	软件重用审查	440
12.4.4	软件重用批准	440
12.4.5	软件重用中止	440
12.4.6	重用软件验收、交付与维护	441
12.5	重用软件的数据包要求	441
参考文献		444
附录 缩略语列表		449