中航工业首席专家
技术丛书

“十二五”国家重点图书出版规划项目
中航工业科技与信息化部组织编写

韩 炜 编著

可信嵌入式软件开发方法与实践

METHOD AND PRACTICE OF DEPENDABLE EMBEDDED SOFTWARE DEVELOPMENT

航空工业出版社

中航工业首席专家技术丛书

“十二五”国家重点图书出版规划项目

可信嵌入式软件开发方法与实践

韩　炜　编著

航空工业出版社

北　京

内 容 提 要

本书从广泛的角度介绍了可信嵌入式软件工程相关的概念、技术、方法和实践。全书共分为4个部分共23章。第1部分为概论，介绍了嵌入式系统和嵌入式软件的分类、特征和发展情况，并对可信性软件的相关基本概念、属性和需要关注的研究内容进行了描述；重点阐述了软件自身的特点、导致软件不可信的因素和软件开发遇到的困扰；描述了软件工程基础知识，包括软件工程基本概念、基本原则和研究内容。第2部分为通用的软件工程的阐述，分别对软件全生命周期模型、开发计划与策划、需求开发及管理、软件架构设计技术、机载软件的设计、软件验证技术、软件质量保证、软件可信性评估、软件可靠性评估和软件安全性评估等软件工程各个方面进行了详细论述。第3部分为机载软件及其工程化方法，重点介绍了机载共性软件适航标准DO－178、《军用软件研制能力成熟度模型》，以及机载软件知识库。第4部分为天脉操作系统的开发实践，对自行研制的天脉操作系统的开发实践进行了详细的描述，其中包括天脉操作系统的研制策划、项目立项论证和研制总要求论证、软件计划过程和软件开发过程实践等。

软件研制有很多工程化规定和指南，但是缺乏工程化的方法学指导，以及对软件工程全面的融会贯通的理解，本书能够为航空工业和其他领域从事高安全性系统设计的软件工作人员提供有用的参考资料。

图书在版编目（CIP）数据

可信嵌入式软件开发方法与实践／韩炜编著. --北京：航空工业出版社，2017.9

（中航工业首席专家技术丛书）

ISBN 978－7－5165－1323－1

Ⅰ.①可… Ⅱ.①韩… Ⅲ.①软件开发－研究 Ⅳ.①TP311.52

中国版本图书馆CIP数据核字（2017）第231971号

可信嵌入式软件开发方法与实践

Kexin Qianrushi Ruanjian Kaifa Fangfa yu Shijian

航空工业出版社出版发行

（北京市朝阳区北苑2号院 100012）

发行部电话：010－84936597 010－84936343

北京隆元普瑞彩色印刷有限公司印刷 全国各地新华书店经售

2017年9月第1版 2017年9月第1次印刷

开本：787×1092 1/16 印张：34.25 字数：875千字

印数：1—2000 定价：170.00元

总　序

航空工业被誉为“现代工业之花”，是国家战略性高技术产业，同时也是技术密集、知识密集、人才密集的行业。中国是世界航空产业格局中的后来者，而中航工业作为支撑中国航空工业发展的核心力量，履行国家使命，必须大力推进自主创新，必须在科技创新和知识创新上有所作为。

从2009年开始，中航工业按照航空技术体系，在科研一线技术人才中陆续遴选出近百位集团公司级“首席技术专家”。此举既是集团公司对这些技术人才技术水平和能力的肯定，也意味着集团公司赋予了他们更大的责任和使命。我们希望这些技术专家在今后的工作中，要继续发挥科研技术带头人的作用，更加注重学习和创新，不断攀登航空科技新的高峰；要坚持潜心科研，踏实工作，不断推动航空科技进步；要带队伍、育人才，打造高水平的科研队伍，努力培养更多的高层次专业技术人才，为中航工业的发展做出更大的贡献。

21世纪企业的成功，越来越依赖于企业所拥有知识的质量，利用企业所拥有的知识为企业创造竞争优势和持续竞争优势，这对企业来说始终是一个挑战。正因如此，“知识管理”在航空工业等高科技产业领域得以快速推广和应用。依照这个思路，将首席技术专家们所积淀和升华出来的显性或隐性知识纳入知识管理体系，是进一步发挥其人才效益的重要方式，也是快速提升中航工业自主创新能力的重要途径。

知识管理理论的核心要义，就是把知识作为一种重要资产来进行管理，正如知识管理的创始人斯威比所说：“知识资本是企业的一种以相对无限的知识为基础的无形资产，是企业核心竞争能力的源泉。”如果专家们把其掌握的各类显性或隐性知识，用书面文字的形式呈现出来，就相当于构建了一个公共资料库，提供了一个交流平台，可以让更多的人从中受益——这就是出版这套“中航工业首席专家技术丛书”的初衷。

集团公司的这近百位“首席技术专家”，基本覆盖了航空工业的所有专业。每位专家撰写一部专著，集合起来，就相当于一个航空工业的“四库全书”，很有意义。在此，我要特别感谢这些专家们，他们在繁重的科研生产任务中，不辞辛劳地撰写出了自己的专著，无私地将自己的宝贵经验呈现给大家，担当起了传承技术、传承历史的责任。

相信这套丛书的出版，会使更多的航空科技工作者从中获益，也希望在一定程度上能助力中航工业的自主创新，对我国航空工业的科技进步产生积极影响。

中国航空工业集团公司董事长

前　言

当今时代的各种电子设备都依赖于嵌入式系统或嵌入式计算机，而研究嵌入式系统的重要内容是嵌入式软件。汽车、医疗设备、飞机内部使用的嵌入式系统对可靠性、安全性有着很高的要求，如飞机的机载电子系统涉及到飞行、功能等与飞机安全相关的控制，或涉及到实现使命的任务控制，如果出现未期望的事件，将可能导致飞机事故或任务失效。所以在航空电子等安全关键领域，可信的嵌入式软件研究是目前研究的一个热点。

可信计算有很多种不同的解释，英语描述“可信”有相信（trust）和依赖（dependence）两个词，实际上研究者也经常混用这两个词语。本书采用“dependence”一词，因为它更针对为人服务的嵌入式设备，更适于表示人对客观的物理世界的一种被动的信赖心理。而可信性（dependability）的定义也是多种多样的，其主要原因是人们会将软件的所有属性都归结为可信性，即是否可放心地相信和使用这个嵌入式系统或其中软件的输出结果，由此对嵌入式软件的各种属性进行分析、归纳，得到“可信性软件”的属性定义，从而全面地描述软件呈现给人的结果的可信程度，这是本书首先要研究的内容。根据综合分析，本书采用了“可用性”“可靠性”“安全性”“信息安全性”“维修性”5个属性表述一个嵌入式软件的可信属性。笔者认为，这5个属性相互之间呈现正交关系，而5个属性之和，则完整地表示一个软件的可信性。

“可用性”表示了人们在对软件运行时输出的信任；

“可靠性”表示了随着时间历程，对软件运行输出的信任；

“安全性”表示了软件所有的运行不会导致重大的伤亡或经济损失；

“信息安全性”表示了软件在经受恶意攻击时，软件运行不会导致重大伤亡或经济损失；

“维修性”表示了软件在以后的升级、完善等方面会给人们一个满意的表现。

为了实现一个可信的软件，笔者根据自己多年的实践经验和探索，首先定义什么情况会导致软件不可信，导致软件不可信的因素是什么，软件及其软件开发过程的哪些特点会导致这些情况，软件开发过程会遇到哪些困惑，为了解开这些困惑，需要借助于哪些可信软件的软件工程的基本原理、方法和过程。

开发软件的第一步是策划、选取适宜的全生命周期模型。嵌入式软件开发人员需要全面了解目前主流的瀑布、增量、快速原型、螺旋、敏捷开发等软件全生命周期模型，针对性地在软件开发过程中采取适宜的模型。同时需要根据所选取的模型，编制计划、标准，用来指导嵌入式软件开发过程。

笔者针对软件具体的开发方法，结合长期从事嵌入式软件的实践工作，在软件需求、架构、设计等方面进行了系统的论述。软件开发的出发点是基于需求的，所以开发人员必须掌握需求开发、需求管理的基本原理和方法。特别是长期采用的基于文档的装备软件开发已经暴露了很多的不适宜，而基于用例、面向对象、基于模型等方法成为目前嵌入式软

件开发的首选方式。

软件架构设计的质量直接决定了软件可信性的各个方面。对于一个专业化组织，开发专业所需的有生命力的、有效的、稳定的架构非常重要。软件的具体设计过程有很多成熟的方法，而软件开发过程的质量控制和软件的验证对于软件可信性的保证至关重要。

软件质量的定量评估是理论研究的热点之一，也是工程应用的薄弱环节。基于过程、基于产品、基于应用等是常见的几个维度，这些评估可以应用于软件的可靠性、安全性以及软件成熟度等方面。尽管这些方法不尽成熟，定量评估结果也没有取得广泛的共识，但这些探索可以为嵌入式软件在可靠性、安全性等方面的增长和评估建立很好的基线。

笔者及其团队对 DO－178B 民用软件适航的理念进行了深入的探索和实践，对 GJB 5000A—2008 所倡导的能力成熟度模型进行了广泛的实践，这些先进的软件工程方法及其过程在天脉嵌入式实时操作系统的研制过程中进行了非常鲜活的实践。本书最后使用了大量篇幅对天脉操作系统的研制过程进行了总结。这些总结从不同的侧面，描述了 12 年的天脉操作系统研制之路。首先，笔者论证了商用操作系统的可信性属性，以及自主研制可控基础软件的必要性，再从天脉操作系统的研发历史开始，深入描述了引入民用飞机 DO－178B 软件适航的目标、方法、思想的来龙去脉，按照有效捕获需求、DO－178B 要求实现计划阶段、开发阶段以及验证、质量保证、项目管理等方面，描述天脉操作系统在实现高安全、高可靠嵌入式操作系统的目标的基本考虑。除此之外，针对天脉嵌入式操作系统，团队引入了适用的 Schneidewind 模型和 FMECA 方法，对其可靠性、安全性进行了评估。

本书是在笔者及其团队长期实践机载高可靠嵌入式软件、消化大量国内外资料的基础上形成的，由多位长期从事嵌入式软件开发、验证及其软件项目管理的同志编写。其中，胡林平编写了“开发计划与策划”，李运喜编写了“机载软件的设计”，牟明编写了“软件验证技术”“软件安全性评估”“GJB5000 概要”，胡宁编写了“软件可靠性评估”，叶宏编写了“机载嵌入式软件”，陈峥编写了“软件知识库建立”，韩炜、叶宏和李运喜编写了“一个可信软件的实践”，谢克嘉、吕烨、刘小开、韩岱菲等同志对全文进行了编校，全书由韩炜统稿和审定。在此对这些同志的辛勤工作和巨大的贡献表示感谢。也谨以此书献给我的爱人和女儿，在本书编写过程中，她们对全书通篇进行了文字上的仔细认真的校对；而且多年来她们对我的工作一如既往的支持，使我可以专注于航空事业，专注于自主可控事业，工作上的些许成绩，也凝聚着她们的关心、支持和鼓励。

笔者相信本书论述所涉及到的方法、实践，会对嵌入式软件开发者有一定启发。尽管如此，由于编者水平有限，难免有不足之处，敬请广大读者批评指正。

韩　炜

2017 年 4 月

目　录

第1部分　概　论

第2部分 软件工程概念

第3部分 机载软件及软件工程

第4部分　一个可信性软件（天脉操作系统）的实践

第1部分

概　　论