第一部分

引　言

第一部分是全书的基础。该部分解释了什么是安全关键软件，以及它为何在当今环境中至关重要。此外还给出了本书的概览，以及所使用方法的说明。

第1章　引言和概览

1.1　安全关键软件的定义

安全性（safety）的一个一般性定义是“避免那些可能引起人员死亡、伤害、疾病，或者设备、财产的破坏或损失，或者环境危害的条件”[1]。安全关键软件（safety-critical software）的定义则更带有主观性。美国电气和电子工程师协会（IEEE）定义安全关键软件为：“用于一个系统中，可能导致不可接受的风险的软件。安全关键软件包括那些其运行或者运行的失败能够导致一个危险状态的软件，以及那些用于缓解一个事故的严重性的软件”[2]。美国国家航空航天局（NASA）出版的《软件安全性标准》将那些至少满足以下准则之一的软件识别为安全关键的[3,4]。

1）它驻留于一个安全关键系统（通过一个危险分析而确定的）并至少满足以下条件之一：

- 引起或助长一个危险；
- 提供对危险的控制或缓解；
- 控制安全关键功能；
- 处理安全关键命令或数据；
- 如果系统达到一个指定的危险状态，检测和报告或者采取纠正动作；
- 当一个危险发生时，减少其破坏性；
- 与安全关键软件驻留于同一个系统（处理器）。

2）它进行直接导致安全性决策的数据处理或趋势分析。

3）它提供安全关键系统的全部或部分验证或确认，包括硬件或软件系统。

从这些定义可以得出结论：软件本身即不是安全的也不是不安全的，然而，当它是一个安全关键系统的一部分时，它可能引起或助长不安全的条件。这样的软件被认为是安全关键的，它即是本书的主题。

1.2　安全性问题的重要性

1993 年，Ruth Wiener 在其著作《数字化之痛：为什么我们不应依赖于软件》中写道：“软件产品——即使是中等规模的程序——是人类制造的最复杂制品之一，而软件开发项目是我们最复杂的事务之一。无论它们吞噬了多少时间或金钱，无论我们在其中投入了多少人力，其结果仅仅是大致可靠而已。即便在最彻底和严格的测试之后，仍会留有一些隐错（bug）。我们永远无法用所有可能的输入去测试系统中的所有执行路线”[5]。从那时到现在，社会已经变得越来越依赖于软件。我们已经不可能回到纯模拟系统。因此，我们必须竭尽全力来确保软件密集型系统是可靠的和安全的。航空工业有一个良好的历史记录，但是由于复杂性和关键性的增长，我们必须更加小心地对待安全问题。

类似这样的说法屡见不鲜：“软件并没有引起过严重的航空器事故，所以何必大惊小怪？”关于软件对航空器事故的作用存在争执，因为软件是一个更大的系统中的一部分，而多数调查都是聚焦于系统层的方面。然而，在其他领域（例如核能、医疗、空间），软件的错误确实导致了生命的丧失或任务的失败。著名的事例包括阿丽亚娜 5 号火箭爆炸、Therac-25 辐射过量，以及海湾战争中的爱国者导弹系统宕机，等等。民用航空中的安全关键软件有令人钦佩的历史记录，然而现在并不是坐下来赞叹过去的时候。以下原因使得未来更具风险性。

- **代码行数的增长。**安全关键系统中使用的代码的行数正在增长。例如，从波音 777 到最近审定的波音 787 中的代码行数已经增加了 8~10 倍，并且未来的航空器还将有更多软件。
- **复杂性的增长。**系统和软件的复杂性在增长。例如，综合模块化航空电子（IMA）带来了重量减轻、安装容易、维护高效，以及降低更改成本的好处。然而，IMA 也增加了系统复杂性，并使得原先隔离于物理上不同的硬件联合体的功能被组合到单个硬件平台，一旦出现硬件故障，则相关的多个功能都会失效。这种复杂性的增长使得更加难以对安全性影响进行全面分析，且难以证明可以不产生非预期后果地实现预期的功能。
- **关键性的增长。**在软件规模和复杂性增长的同时，关键性也在增长。例如，飞行操纵面接口在 10 年前几乎全部是机械的。如今，许多航空器制造商在改用电传操纵软件控制飞行操纵面，因为电传操纵软件包含有提高航空器性能和稳定性的算法。
- **技术上的变化。**电子和软件技术在快速发展。要避免技术陈旧又保证其成熟性，是具有挑战性的。例如，安全性领域要求健壮的和经过证实的微处理器，然而，由于一个新航空器的开发需要花费大约 5 年的时间，经常在进行飞行测试之前，微处理器就已经接近过时了。另外，软件技术的变化使得要聘用到懂得汇编、C 或者 Ada（机载软件的最常用语言）的程序员很困难。这些实时语言在许多大学中是不讲授的。软件开发者也正在与实际生成的机器代码更加疏远。
- **以少搏多。**由于经济性的驱动和盈利的压力，许多（甚至是大多数）工程组织被要求以更少的投入做更多的事情。作者听到过这样的描述：“他们先是撤去了我们的秘书，然后撤去了我们的技术文档编写人员，接下来撤去了我们的队友。”大多数优秀的工程师一个人在做以往是由两个或者更多人做的事。他们被摊得很开，耗得很尽。人们在数月的超时加班之后会变得低效。作者的一位同事这样说：“超时加班是用于冲刺的，不是用于马拉松的。”然而，许多工程师在数月甚至成年地超时工作。
- **外包和离岸外包的增加。**由于市场的要求和工程师的短缺，越来越多的安全关键软件被外包和离岸外包。虽然不总是这样，但是外包和离岸团队经常不具备系统领域知识，以及有效发现与去除关键错误所需要的安全性背景。事实上，在没有适当监视的情况下，他们甚至可能注入错误。
- **有经验工程师的缺失。**许多为现在的安全记录做出贡献的工程师将要退休。没有一个严格的培训和辅导规划，年轻的工程师和经理不理解关键的决策和实践实施的原因，因此他们要么不加遵守，要么全然抛弃。一位同事最近在他的团队向作为系统专家的合格审

定机构的一位新任系统工程师，做了一个关于减速板的演示报告之后，表达了他的郁闷：在 2 个小时的报告之后，那位新工程师问道：“你们不是在说轮子，对吗[①]？”

- **可用培训的缺乏。**以安全性为焦点的学位教育基本上没有。此外，关于系统和软件确认与验证的正式教育也基本没有。

由于这些以及其他的风险驱动因素，比以往更加聚焦于安全性就尤为重要。

1.3 本书目的和重要提示

您对本书的阅读令作者深感荣幸。本书的目的是为实践中的工程师和经理提供开发航空用安全关键软件所需的信息。在过去的 20 年间，作者有幸从事了航空电子开发、航空器开发、合格审定机构、美国联邦航空局（FAA）委任工程代表（DER）、咨询师以及培训师的工作。作者已经评价过几十个系统上的安全关键软件，这些系统包括飞行控制、综合模块化航空电子、起落架、襟翼、防结冰、前轮转弯、飞行管理、电池管理、显示、导航、地形感知与告警、空中交通防撞、实时操作系统，以及其他许多。作者曾与多到 500 人，少到 3 人的团队一起工作。这些始终都是令人激动的经历。

丰富多样的职位和系统使得作者能够体验和观察到安全关键软件开发中的共同问题和有效解决方案。本书的写作就是为了利用这些经验来帮助实践中的航空器系统工程师、航空电子和电子系统工程师、软件经理、软件开发和验证工程师、合格审定机构及其委任者、质量保证工程师，以及有意愿实现和保证软件安全的其他人。

作为一个开发和验证安全关键软件的实践指南，本书提供基于现实项目的具体指导和建议。不过，这里还需要给出以下重要提示：

- 本书给出的信息代表的是个人观点。本书的编写是基于个人的经验和观察、个人研究，以及与世界上一些最聪明的人的交流。本书已尽全力给出在目前看来准确和完整的建议。在全书中，使用了诸如典型地、通常地、一般地、大多数时候、多次地、时常地等词汇。做出这些一般化概括所基于的是作者参与过许许多多的项目，然而，还有许多项目以及无数行的代码作者并未看到。您的经验也许有所不同，作者十分欢迎您的不同见解。如果您想要对某个话题进行澄清或者辩论、询问某个问题，或者分享您的想法，尽可发电子邮件到如下地址：LRierson1@aol.com 和 Digital_Safety@sbcglobal.net。
- 本书的叙述使用的是个人的和稍微非正式的口吻。在给数百名学生讲授 DO-178B（以及现在的 DO-178C）之后，本书希望成为作者（培训师）与您（工程师）之间的一个交互。由于作者不知道您的背景，因此努力以一种方式让写出的内容对于任何背景的您都能有所帮助。作者就像在课堂中那样加入了一些故事经历和间或的幽默。与此同时，专业性当然也是本书的一个恒定目标。
- 由于本书聚焦于安全关键软件，书中的内容是围绕较高关键等级软件（例如 DO-178C 的 A 级和 B 级软件）的。对于较低关键等级的情况，一些活动可能不需要。
- 虽然本书的焦点是航空软件、DO-178C 符合性，以及航空器合格审定，但是许多概念和最佳实践适用于其他安全关键或任务关键领域，例如医疗、核能、军事、汽车以及

① 向不了解的读者解释一下，减速板是在机翼上。

航天。

- 由于作者作为合格审定机构和委任工程代表的背景，阅读本书可能时常好似钻进了合格审定机构的大脑。本书讨论了 FAA 和欧洲航空安全局（EASA）的原则和指南材料，不过主要使用的是 FAA 的指南，除非二者存在显著的不同。虽然本书内容的意图是进行解释，并与写作当时的合格审定机构的原则和指南保持一致，但是本书并不构成合格审定机构的原则和指南。请向您的本地机构咨询适用于您的特定项目的原则和指南。
- 经过全球旅行和与六大洲的工程师的交流，作者已尽力呈现一个关于安全关键软件和合格审定的国际化视野。不过由于作者的大部分工作是在美国和 FAA 审定的项目上，主要的视角也是在这些方面。
- 本书通篇援引了包括 DO-178C 在内的许多美国航空无线电技术委员会（RTCA）文件。作者在 3 个 RTCA 委员会中担任领导角色，并在引用到的文件的编写中发挥关键作用，这是令人激动的工作。如在前言中指出的，RTCA 非常友善地允许作者引用和引述其文件。然而，本书并不是对这些文件的替代。作者努力覆盖其中的要点，引领您贯通 DO-178C 与相关文件的细微之处。但是如果您正在开发一个必须符合 RTCA 文件的软件，则应确保阅读其整个文件。您可以更多地了解 RTCA，或者通过以下地址联络他们购买文件：

  RTCA, Inc.
  1150 18th Street NW
  Suite 910
  Washington, DC 20036
  Phone: (202) 833-9339
  Fax: (202) 833-9434
  Web: www.rtca.org

- 本书的编排使您既可以从头到尾通读，也可以根据需要选读其中的章节。您会发现不同章节之间的偶尔重复。这是有意识的，因为有些读者会把本书作为一本参考手册，而不是通篇阅读。全书中都有对相关章节的引用，为那些不从头到尾阅读的作者提供便利。

1.4　本书概览

本书分为 5 个部分。第一部分（本部分）提供介绍和基础。第二部分对于软件在整个系统中的角色进行说明，并给出用于航空的系统和软件安全性评估过程的概括。第三部分首先概览 RTCA 的 DO-178C，名为《机载系统和设备合格审定中的软件考虑》，以及与 DO-178C 一起发布的其他 6 份文件；然后介绍 DO-178C 过程——提供关于如何有效实施的深入指导和建议。第四部分介绍与 DO-178C 一起发布的 4 份 RTCA 指南文件，主题包括软件工具鉴定（DO-330）、基于模型的开发与验证（DO-331）、面向对象和相关技术（DO-332），以及形式化方法（DO-333）。第五部分覆盖了与 DO-178C 和安全关键软件开发相关的专题。这些专题聚焦于航空，但是也可以适用于其他领域。它们包括未覆盖代码（无关代码、无效代码、非激活代码）、现场可加载软件、用户可修改软件、实时操作系统、分区、配置数据、航空数据库、软件复用、先前

开发的软件、逆向工程，以及外包和离岸外包。

还有许多未覆盖的专题，包括航空器电子硬件、电子飞行包，以及软件保密安全。这些专题与软件相关，在书中偶有提及。不过由于篇幅和时间所限，未能将其涵盖。