飞机设计技术丛书

WP

# AIRCRAFT SYSTEM SAFETY

## MILITARY AND CIVIL AERONAUTICAL APPLICATIONS

# 飞机系统安全性

## 军用及民用航空应用

（英）杜安·克里津格(Duane Kritzinger) 著

唐长红 等 译

航空工业出版社

# 飞机系统安全性

## 军用及民用航空应用

（英）杜安·克里津格 著
唐长红 等 译

航空工业出版社
北京

## 内 容 提 要

本书围绕“飞机系统安全性”这一主题，介绍了与之相关的法规、方法等，并融入了许多案例，以帮助读者理解安全性所涉及的设计、制造、使用、维护等各个环节。

本书可以作为高等院校适航专业教材，也可以作为相关专业本科生、研究生与教师的参考书，同时还可供航空器设计、制造、运营和适航管理人员及所有对适航感兴趣的读者阅读和参考。

**图书在版编目（CIP）数据**

飞机系统安全性 /（英）克里津格（Kritzinger，D.）著；唐长红等译. --北京：航空工业出版社，2013.5
（飞机设计技术丛书）
书名原文：Aircraft system safety
ISBN 978-7-5165-0155-9

Ⅰ.①飞… Ⅱ.①克…②唐… Ⅲ.①飞机－飞行安全 Ⅳ.①V328

中国版本图书馆 CIP 数据核字(2013)第 091993 号

**北京市版权局著作权合同登记**
**图字：01-2012-4646**

飞机系统安全性
Feiji Xitong Anquanxing

航空工业出版社出版发行
（北京市安定门外小关东里 14 号 100029）
发行部电话：010-64815615 010-64978486
北京地质印刷厂印刷 全国各地新华书店经售
2013 年 5 月第 1 版 2013 年 5 月第 1 次印刷
开本：787×1092 1/16 印张：19.5 字数：445 千字
印数：1—3000 定价：68.00 元

# 译 者 序

忧者自忧，扰者自扰，任何事情都没有表面看起来那么简单，会出错的事情总会出错；祸福因果，万物有端，你最担心的事件就是更有可能发生的事件。

持续追求安全，是世界航空永恒的目标和不懈发展的课题，也是随着时代技术进步，人类航空安全理念抽象和解析、演化和提升的过程。

就飞机设计而言，安全性是飞机研制中的一项重要指标，是依赖技术能力和认知水平所赋予飞机的固有品质。安全性设计是权衡技术可行性与经济可承受性的核心。

飞机系统安全性分析与评估是飞机系统设计的基础。通过对系统设计功能中潜在危险的识别，进而进行分析和评估，提出系统设计的安全性要求，指导系统架构设计，并通过对系统开展全面的安全性设计活动，将系统安全性分析与评估技术和飞机设计制造过程有机结合起来，以表征和证明飞机的安全品质满足一定的规范和要求。系统安全性设计是工程实践过程中逐步发展起来的一套系统分析与评估的技术和方法。

前车之鉴，后事之师，用经验和教训指导工程研制实践，是规避风险、避免失误的捷径。欧美在民用飞机研制实践中总结发展起来的飞机系统安全性分析与评估的技术和方法，有效指导着当代先进飞机的设计，对降低飞机灾难性事故的发生概率和人们对飞机系统的安全认知起着重要作用。在大型飞机研制过程中，广泛借鉴世界航空先进的安全理论和实践经验，对于跟进航空技术进步具有事半功倍的效果。

本书从安全性的概念和相关法规标准出发，基于风险分析与评估方法以及目标综合理论，探索军用、民用飞机系统安全性分析与评估的基本方法，详细论述了“危险”应用的相关问题和对危害致因的识别，阐述了系统安全性分析与评估的目标、目的和要求等基础知识，并附有大量安全案例。内容由浅入深，从简到繁，从理论到方法，从现状到未来，是一本关于系统安全性分析与评估不可多得的优秀书籍，对从事工程系统设计的工程师、安全性专业技术人员和管理者，以及安全性分析与评估的专业教学都具有重要的参考价值。

本书在翻译过程中，力求直译，以尊重作者的原意，以免疏漏弦外之音，因时间仓促，难免斟酌不足，诚望读者批评指正。翻译过程中得到了中航工业第一飞机设计研究院的大力支持，在此代表译者表示衷心感谢。

唐长红

2013 年 1 月 26 日

# 致　　谢

本书能够问世完全有赖于作者受雇于南非空军和剑桥马西尔航宇公司的经历。因此，不免对这份丰富的经历永存敬意，它们涉及各个方面，分别来自接触到的各种飞机（即固定翼与旋翼飞机、军用与民用飞机、运输与高速喷气飞机、有人驾驶与无人驾驶飞机）、交往的各国审定当局（军队与民航）、从事的各种不同项目（即结构与航空电子的项目）以及作者成长道路上遇到的兴趣广泛、知识渊博的人们。

首先要感谢那些协助本书筹备的人员。特别感谢作者的朋友、同事，自愿对作者要表达的各种理论进行审查，提出新颖有价值的见解，他们是：Bernie Guignard（第 1 章），Doug Henderson（第 10 章），Grayhame Fish（第 1 章），Ian Roberts（图 8 - 8），Iya Solodilova（图 8 - 8 及附录 A），Jim Watts（第 8 和第 9 章），Stephen Goldsmith（第 1 ~ 第 12 章），Richard Ehlers（第 3 和第 6 章）以及 Vic Owen（第 2、第 4 和第 6 章）。此外，还要感谢提供插图的人员，他们是：Adam Cundick（封面图片），Dave Ash（图 8 - 8）和 Simon Parker（图 5 - 2）。

作者的许多知识还源于各种研讨会、会议、杂志、论文以及其他书籍。本书中对所有这些相关著作有引用的，都在书后参考资料与扩展阅读中列出了。特别感谢 Ted Lloyd 和 Walter Tye 具有开拓性的著作《系统安全性》（1982 年首次出版），书中观点至今仍是所有从事飞机系统安全性评估人士的无价之宝。非常感谢伍德海地出版有限公司独立审查人员提出的建设性评语以及语言表述方面的建议，还要感谢作者适航顾问朋友 Brian Perry（民用）和 Jan Schutte（军用）提出的各种非常珍贵的评论、修正意见、提案与改进意见。对意见的落实，真诚希望他们都能认同。

衷心感谢有幸获得承诺允许复制以下版权的素材：图 13 - 1（波音公司）、图 13 - 2（Doug Arbuckle，来自美国国家航空航天局）、图 6 - 1（洛克希德·马丁公司）、图 8 - 1（Barry de Beer，来自南非国防部），同时，还向 Robert Eijkelkamp 上尉（来自荷兰皇家空军，提供了封面照片，该照片由 Fotovlucht Soesterberg 拍摄）致谢。

还要感谢伍德海地出版公司的以下人员：Sheril Leich（责任编辑）、

Emma Pearce（项目编辑）和 Stuart Macfarlane（制作服务），感谢他们在将手稿付诸出版过程中提供的支持、建议、意见反馈和帮助等。

尤其要感谢的是我的挚友、最严厉的批评家、头号粉丝和深爱着的妻子——Nicole，是她鼓励我一路坚持下去，是她认真阅读我的手稿并且促成了这本书最终定稿。

# 前　言

作为一名充满青春活力的机械工程师，进入南非空军（SAAF），很快就能从事军方对飞机改进的安全性评估工作，作者深感荣幸。起初，对这些评估工作的技术方法（尤其是故障模式影响及危害性分析，即 FMEA）比较陌生，业务上难有兴致而疲于应付。

几年后，评估工作转向由第三方（如承包商）提出的飞机改进，此时，很容易对他们的安全性评估提出更多的批评和要求。但由于评估工作与系统配置脱节，作者再次发现，其有效作用并非如人所愿，最终结果也只不过是废纸一堆，不免渐渐就又落后于系统的发展。

在闯荡空军 13 年之后，最后加盟到私营企业。至此，职业生涯算是度过了一个轮回，接下来再次面对的是另一种局面。当时，作者所承担的安全性评估工作都要受到严格审查，审查方除了民航当局（如英国民用航空局（CAA）、美国联邦航空局（FAA）等），还有军方当局（即作者的旧部）。

为此，不可再懈怠，该是寻求一种更稳妥、更连贯的、不单是评估安全性还有呈报这种评估方法的时候了。鉴于作者的个人经验，其中基本要点如下：

- 当事者的期望（例如，想从安全性案卷或者 FMEA 中得到什么），尤其是在军民方法融为一体时（例如，民用机构改进军用飞机，反之亦然）。
- 术语和定义（例如，区分危险与失效之间的差异）。
- 安全性准则（即责任方为完成或监管某项任务而设定的目标）。
- 审计事宜（即把安全问题、证据和决定记录备案）。
- 实用性（即安全性评估或案卷的作用不仅在于风险评估，而且还贯穿于产品全生命周期——从设计方案评估到运行期间的故障诊断）。
- 系统集成（即把子系统安全性评估有效融入系统安全性评估或案卷中）。
- 说明（即如何借助之前各类文件让人们相信系统（及评估）是完整的）。

尽管理论上并不存在一种唯一正确的安全性评估方法，作者还是努力提出自己的《用户指南》，以便能协助作者完成协调、有效、高品质的安全性评估。

作为一名首席安全性审定工程师，作者还有幸帮助、培训及教授同仁们各种有关飞机改进的安全性评估。作者发现这本《用户指南》特别有用，随着把经验教训（源于大家的奋斗）再次融入[①]到该《用户指南》中，会使得下一次整个教学工作更有成效。在教学期间，曾有一位年轻工程师提出，“要是我们能在大学时就学到这方面的知识该多好”。当时，作者就萌生一种想法，要为此编撰一本教科书。

本书针对上述要点，而不是提供关于如何使用某种工具或技术的样板（或许在下一本书中提供）。安全性一直是航空界关注的永恒话题，并且一直由主导部门建立新的、逐步完善的、评估可接受的安全性等级方法。本书中这些方法毋庸置疑均适合于大型运输机系统[②]研发。而实际上，任何工业部门，从事制造复杂的、具有潜在危险系统的，所需要的方法也都与此相差无几。

本书中旁引有大量的思路、观点、工具与方法，虽然源于不同领域与行业，但作者初衷都在于使得本书中这些安全性理论更为简明。尽管该学科领域极富动态性并始终处于变革中，但是，某些基本因素是永恒的，它们是诠释该领域的基础。作者衷心希望，那些关注安全性评估的人们（包括学生、设计人员、安全性评估人员及其管理者、雇主们等）将从中获益，他们能充分了解书中提到的各种思路的前后关系、价值与各种不足。不仅如此，本书还将引导人们解决安全性问题。

① 这并非是过去式——只要从事安全性评估，作者就不会停止学习，也会一直这样做下去。

② 符合 JAR/FAR 第 25 部要求的商用运输机的安全性记录。常作为一种标准被用来判定其他运输机系统的安全性。

# 目　　录

# 引　言

世上所有人都希望，在任何情况下，都不受伤害。只可惜，因为每项活动总存在自身的危险因素，绝对安全是不可能的。各种事故不但可能，而且又真的会发生，总有一天，事故又会不期而至。事故类型虽然不同，但都具有以下共同点：

- 事故均捉摸不定，没有人能够预知是否会酿成灾难。
- 事故本来都可预防——即责任可追究。

未来管理者的法律责任可能要逐步加强。在英国，有一项新提案，提出引入新的罪行——团伙杀人罪。此提案的出台与之前多个案例有关，在这些案例中，对过失杀人的指控都落了空，因为不能把责任追究至某个具体的人，而且要“宣判”某公司有罪，又无先例可循。然而，根据 Hadden－Cave（1999）的要求，该新提案将会引入团伙杀人罪、草菅人命罪和无意识杀人罪。一旦引入，整个英联邦都得采纳。当然，英国法律也不例外。世界上其他国家也都正面临同样的问题，而且也准备好了在新的边沿领域推行管理者责任制。

落实这些道德法律责任，要求各种安全性风险都必须明确认定、量化以及得到相应的控制。关键性问题是负责安全的管理者（对于所有当事方）是否曾存在失职过错。至于刑事责任，所有公司都必须认真从其安全管理体系入手。

任何新的系统在使用之前，都必须提供书面证据，证明它是安全的、可以接受的，立法也一样。惯例做法是把大量的试验结论、安全性分析、成果以及其他数据提交给第三方（如某规章制定机构）。一般都希望这种重要（真实）证据能成为最权威的证据，能够证明该系统是完全可以接受的。而当下，随着系统构成越来越复杂，软件使用越来越密集，对这种信息的完整性、一致性的评估难度会越来越大。所以，急需非常严谨的安全性评估方法来提供一种有论证支持的逻辑决断，并且该评估方法应有明确的目标、策略、设定与论证。

目前，经常听到的都是安全性是至关重要的说法，即其优先权至高无上。因此，安全性在大家的心目中已占据了重要的位置，而且许多人都立志不惜一切代价消除所有安全风险，但又很难如愿。只有感情不行，真正需要的是切合实际的一致性方法，瞄准各种具有潜在危害的原因，并且找出解决问题最有效的途径。此外，大家必须调整心态，一方面不要忽视安全性，另一方面又不可让安全性妨碍事情的有效发展。

实际上，安全性属于内在而非外加的属性。所以，必须把重点放在危险的识别与分析上，而不是放在设计标准的可靠性上。由于安全性所涉及的过程都是计划好的、成熟的、系统化的和主动性强的，所以，又首先必须重点把安全性作为一种设计参数，从而把可接受的安全标准融入系统。这样做又必须有成熟的工具与方法，才能确保达