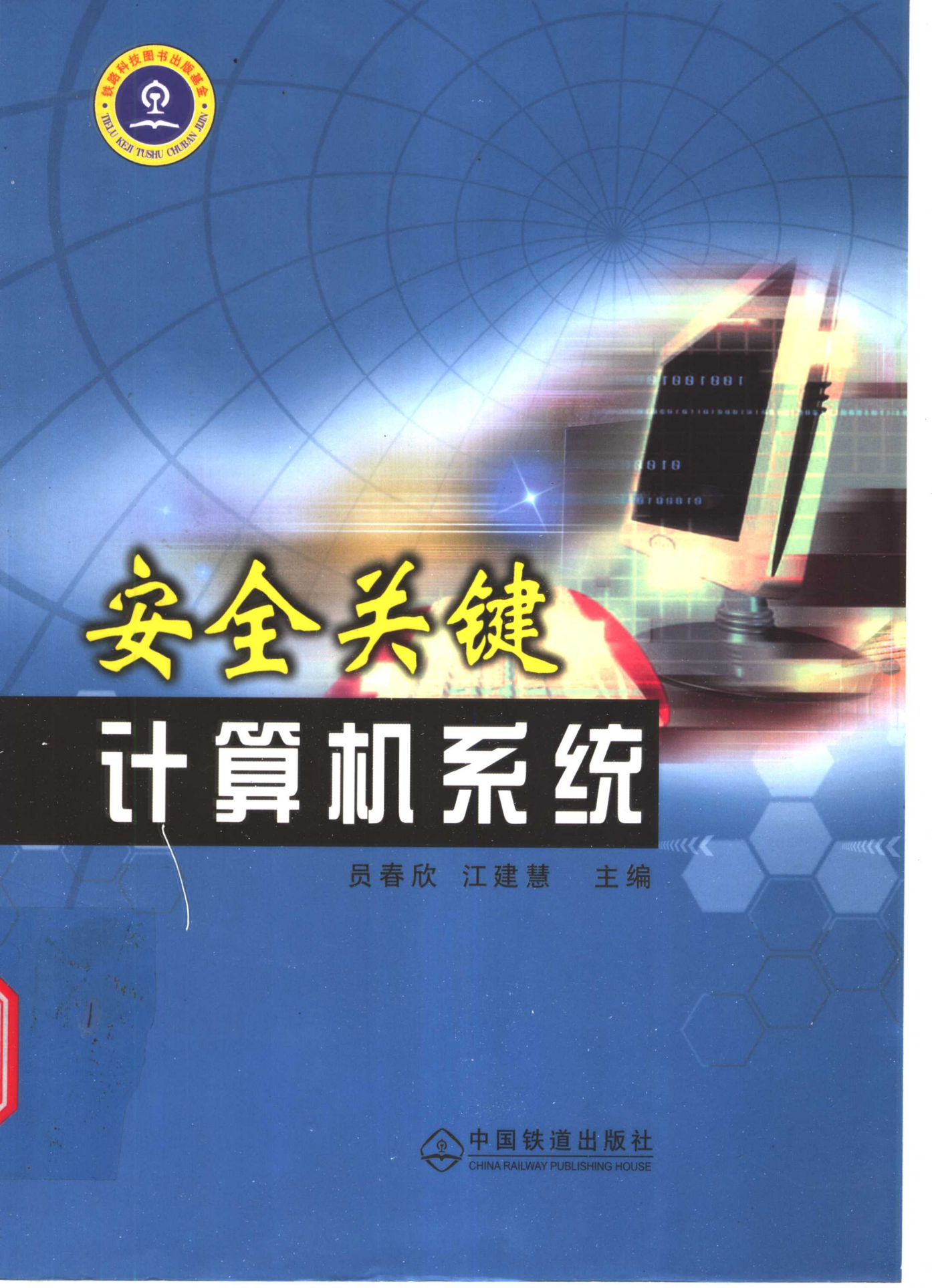
铁路科技图书出版基金
TIELU KEJI TUSHU CHUBAN JIJIN



安全关键计算机系统

员春欣　江建慧　主编

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

铁路科技图书出版基金资助出版

安全关键计算机系统

员春欣　江建慧　主编

中　国　铁　道　出　版　社
2003 年 · 北京

(京)新登字 063 号

内 容 简 介

本书主要介绍了安全关键系统概论、安全技术的国际标准、安全关键系统的安全原理、危险和风险分析方法、形式方法及其在安全关键系统中的应用。安全关键系统的需求工程、安全关键计算机系统的组成原理、安全关键计算机系统的软件，以及计算机系统的验证技术等。本书主要围绕交通安全计算机控制系统的需要进行选材，并力求反映本学科在国际上的新成就。

本书为高等学校交通信息工程本科专业的教材，也可作为自动控制专业、安全技术专业的教材或参考书。

图书在版编目(CIP)数据

安全关键计算机系统/员春欣，江建慧编著. —北京：中国铁道出版社，2003.7

ISBN 7-113-05221-5

Ⅰ.安… Ⅱ.①员…②江… Ⅲ.电子计算机-安全技术 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2003)第 036533 号

书　　名：安全关键计算机系统

作　　者：员春欣　江建慧　主　编

出版发行：中国铁道出版社(100054，北京市宣武区右安门西街 8 号)

策划编辑：殷小燕

责任编辑：殷小燕

封面设计：石碧容

印　　刷：北京市兴顺印刷厂

开　　本：787×1092　1/16　印张：17.25　字数：423 千

版　　本：2003 年 10 月第 1 版　2003 年 10 月第 1 次印刷

印　　数：1～3 000 册

书　　号：ISBN 7-113-05221-5/TP·928

定　　价：29.00 元

版权所有　侵权必究

凡购买铁道版的图书，如有缺页、倒页、脱页者，请与本社发行部调换

编辑部电话：路电(021)73147，市电(010)51873147　发行部电话：市电(010)51873172　路电(021)73172

序

生、老、病、死是万物的规律，是古今中外人类社会永恒的主题。非正常的生老病死的问题成为安全问题的主要威胁，而得到人们最广泛的关注。科学技术的进步和发展神话般地改善着人们的生活。但是，也加重了安全问题的威胁。在古代，人们靠步行，发生伤亡事故的可能性很小。自从有了火车、汽车、飞机，甚至航天飞机，可以毫不夸张地说，全国、全世界每天都发生伤亡事故。就在刚刚过去的中国大年初一，2003 年 2 月 1 日，美国“哥伦比亚”号航天飞机在着陆前 16 min 出现技术问题，并最终爆炸解体。航天飞机上 7 名宇航员同时遇难。当然，科学技术的进步也提供了保证安全的各种现代化措施，这就是安全关键计算机系统。由此可见，本书涉及的内容是多么重要。

今天，计算机系统达不到人们希望的可信性要求。但是，成功的事例也不少。日本新干线火车是可靠性和安全性的一个非凡的例证。日本新干线自 1964 年运营以来，每年几百万人次的旅客运量，没有因冲突、出轨或其他铁路事故而死一个旅客。不过，就在 20 世纪 60 年代初，新干线开通之前，东京附近发生了两次事故，都死亡 100 人以上。此后，日本人吸取教训，使得安全和可信成为一种文化。员春欣和江建慧以本书向我国读者介绍这些生命攸关的计算机系统的理论和技术是一件很有意义的工作。

安全关键计算机系统牵涉的内容很多。它是一个系统的问题，要靠硬件、软件及其外围设备才能实现，又要长期运营，保证系统的安全可靠。本人粗读本书，发现本书有两个特点：一个是内容全面丰富。从概念到具体技术、从管理到设计、研究，从工程设计到验证评估都有涉猎。广泛引用了国际的标准、动态、论文，以及国内的相关材料。这些材料一定是经过作者长年积累才能整理出来的。同时，还包括了作者们自己的一些研究工作。另一个是文笔流畅，易懂易读。作者们从事铁路信号的研究与教学几十年，有丰富的教学经验，为本书的写作提供了良好的基础。

本人感谢作者们的辛勤劳动和贡献，相信本书的出版，对从事安全关键计算机系统的管理、维修、教学、设计、科研各方面的读者都会有很大裨益。也会引起社会对安全问题的重视与人文关怀。同时，本书也可以作为大专院校学生的教材或教学参考书。

闵应骅

2003 年 2 月

于中国科学院计算技术研究所

前　言

安全关键系统是指空间技术、石油、化工、核电站、机器人、民用航空、铁路运输、公路交通、武器装备、医疗仪器等高风险系统，它具有很高的酿灾潜势，这种潜势一旦失控而释放，就会造成巨大灾难。在人类长期与高风险的斗争中不仅推动了“软”安全科学理论和技术的发展，也促进了“硬”安全科学理论和技术的形成与进步。随着计算机技术的诞生与发展，在安全关键系统中广泛采用计算机技术，作为人类与高风险斗争的有力武器，并在实践中积累了丰富的经验，经过不断总结提高，形成了安全关键计算机系统的理论体系，Nancy G. leveson 撰写的《安全件：系统安全与计算机》(Safeware: System Safety and Computer)和 Neil Strorey 所写的《安全关键计算机系统》(Safety Critical Computer System)等著作于 1995 年和 1998 年先后出版发行就是一个明证。而且，这个理论体系的实现又得到了与此相关的许多国际标准的支持。相比之下，作者深感国内在这方面还存在着较大的差距。为了在我国的安全关键计算机系统理论和技术的发展中尽微薄之力，促使我们编写此书介绍国际上在这方面的研究、发展情况，期盼着我国在这个领域也能早日与发达国家并驾齐驱，以上，就是我们编写此书的初衷。

考虑到本书还将作为大学交通信息工程本科专业的教材，并结合写此书的初衷，在选材上，一方面要照顾到基本知识、基本理论和基本技术等内容，以满足教学的需要；另一方面主要选取 20 世纪 90 年代以来发达国家的新成果，使本书内容有先进性。根据我们能查到的国外文献，有关安全关键计算机系统的文献实在太丰富了，但限于篇幅，只能忍痛割爱，择其要点写入本书。尤其要结合交通安全控制系统的需要进行选材。

全书共由 10 章组成，它又可以分成 5 个板块。

属于第 1 板块的是第 1 章安全关键系统概论。其目的在于使读者对安全关键系统有一概括的了解，其中包括什么是安全关键系统及其分类，安全关键计算机系统的结构及其与其它学科的联系，以及安全关键计算机系统理论框架等。

属于第 2 板块的是第 2 章安全技术的国际标准和第 3 章安全关键系统的安全原理。主要介绍近代安全关键(计算机)系统理论的两个特点：

第一，它是以危险和风险分析为基础，导出系统应该具有的安全功能及其完整性指标，以实现系统的功能安全，达到将系统风险降低到当时社会可以接受的程度。

第二，安全功能的选取和实现必须做到：从人－机－环境的大系统入手，贯穿系统的安全生存周期的全过程，采取本质安全－安全防护－使用信息等多层次的安全措施。

属于第 3 个板块的有第 4 章危险和风险分析方法、第 5 章形式方法和第 6 章安全关键系统的需求工程。主要讨论危险和风险分析方法，进而导出安全需求的方法。

属于第 4 个板块的有第 7 章安全关键计算机系统的组成原理，第 8 章安全传输系统理论以及第 9 章安全关键计算机系统的软件。主要讨论构成安全关键计算机系统的硬件和软件的各种实现技术。

此为试读，需要完整PDF请访问：www.ertongbook.com

属于第5板块的是第10章系统验证。主要讨论所实现的安全关键计算机系统进行正确性验证的各种方法。

全书的编写大纲由同济大学的员春欣首先拟出初稿，经与同济大学的江建慧多次认真研究修改后定稿。第1章和第9章由员春欣和江建慧共同执笔编写。第2至8章由员春欣执笔编写，经江建慧两次审阅，然后根据所提意见进行修改定稿。第10章由江建慧执笔编写。本书由董德存教授主审。

本书能够列入计划是和同济大学张树京教授和董德存教授的积极推荐分不开的，是和中国铁道出版社的各级领导、编辑的支持分不开的，并得到铁路科技图书出版基金的资助。原上海铁道大学的教务长缪润生副教授和董德存教授在财力上给予了大力支持。李佳玉同志提供了有关外文资料翻译稿。施莉娟、张秀荣参加了编写大纲的讨论。陆风兰同志和同济大学交通运输学院研究生张雷、曲文澜、张凯杰、杜杰友、罗丽云、江亚承担了录入工作。在此，作者向他们表示衷心的谢意。作者参阅了大量的文献，才能完成此书的编写工作，作者也向这些文献的作者表示衷心的感谢。

作者怀着遗憾和歉意写完本书的最后一个字。由于篇幅的限制，许多内容未能展开，甚至有些重要内容未能写入。由于作者的水平有限，书中错误和疏漏之处在所难免，恳请读者给予指正，不胜感激。

最后，中国科学院计算技术研究所研究员、博导闵应骅先生在百忙中抽暇为本书作序，作者向闵应骅先生表示深深地谢意。

作者 2003年5月于上海

目　录

此为试读,需要完整PDF请访问: www.ertongbook.com

第1章　安全关键系统概论

当你看到本书的时候，立即会产生许多问题：什么是安全关键系统？它的作用如何？又是怎样分类的？它经历了怎样的发展历程，现状如何？它研究哪些内容？所有这些问题，你可以从本章的论述中得到明确的回答。

1.1　什么是安全关键系统？

John Rushby 给关键系统(Critical System)作了如下定义：关键系统是指一旦发生故障可以导致不可接受后果的系统。不可接受的后果包括生命的死亡、财产的损失、环境的破坏或机密信息的泄露。依次称作生命关键(life critical)、财产关键(money critical)、环境关键(enviroment critical)和信息关键(information critical)等系统。

安全关键系统(Safety Critical System)采用了 ENV 50129—1999 的定义：凭借它自身可以达到为了实现所要求的安全功能必须的安全完整性等级的系统，或者说对安全承担直接责任的系统。

安全关键计算机系统(Safety Critical Computer System)——若以计算机为核心子系统构成安全关键系统的监控系统时，则把这种监控系统称为安全关键计算机系统，这是本书讨论的对象，为简单起见称为安全关键系统。

安全关键系统具体地是指空间技术、航空、铁路、公路、水路运输、核电站、石油和化工、国防和武器装备、机器人以及医疗仪器等高风险系统。为了更深入地理解安全关键系统，对它们做进一步的讨论。

空间技术或称太空技术。这里主要指的是宇宙飞船和气象、海洋、通信等卫星。它为人类探索和利用宇宙空间，为人类生产力发展和生活质量提高作出了巨大贡献，但是人类为此也付出了高昂的代价。1986 年 1 月 28 日美国“挑战者”号航天飞机升空不久发生爆炸，7 名宇航员丧生，经济损失惨重。飞机失事原因是由于固体火箭推进器的橡胶密封圈因温度太低而失效，导致火箭裂缝，火焰直向外燃箱喷射，点燃箱中 200 多万 m^3 的氢和氧而发生爆炸。另外，发射中心违规，按规定气温低于 10.5℃不能发射，但该中心却在气温 −3.3℃时发射，这是导致悲剧发生的根本原因。10 年后，1996 年 6 月 4 日早晨，欧洲第一枚阿丽亚娜 5 型火箭升空后 40 s 到达 3 700 m 上空发射装置开始偏离飞行轨道、随后爆炸。火箭价值 5 亿英镑。事故的主要原因，一是在设计上，没有根据阿丽亚娜 5 型火箭的特点进行“定位软件”的重用，而是照搬阿丽亚娜 4 型火箭的“定位软件”，并用相同版本的软件装入双倍冗余的计算机中；二是在测试和合格认证中，先入为主地断定惯性制导系统没问题，而未进行惯性制导系统的闭合仿真认证。结果，恰恰就是由于照搬“定位软件”引起惯性制导系统出现问题，而酿成大祸。

化学工业。这个领域使用安全关键计算机系统的目的就是在实现化学反应过程的自动控

制中，防止火灾、爆炸、有毒物质的泄漏等对人的伤害和对环境的污染。不幸的是，灾难仍时有发生。1984 年 12 月 3 日凌晨，美国碳化物联合公司设在印度博帕尔市的一家农药厂，因管理紊乱，缺少保证安全的冷却装置，加上违规操作，误将水注入储罐，与异氰酸甲脂形成放热的反应，使温度急剧升高，压力超过正常压力的 20 倍，致使防爆膜破裂，罐内的 45t 液态的异氰酸甲脂氧化后外溢，致使熟睡中的人们受到侵害，中毒或窒息；导致 4 000 人死亡，20 万人中毒，5 万人的眼睛受到严重伤害，19 000 人形成终身残废；无数的牲畜和农作物被毁；事故后的 5 年中，中毒者每天相继死亡 1 人；幸存者免疫力下降，不断受到各种疾病感染；受害的妇女，自然流产率比普通妇女高 4 倍。

核电站。这个领域的根本安全问题是防止放射性泄露。但是，灾难还是降临了人间。1986 年 4 月 27 日切尔诺贝利核电站发生爆炸。至少 92 000 人从周围地区撤离，25 万儿童很快转送到夏令营。在苏联、意大利、法国、德国、斯堪的那维亚等国家中，在人、动物、食品、产品、乳制品上等等检测到高等级的辐射。由此可见，灾难影响地域之广泛。切尔诺贝利城实际上已被摧毁，成了一片废墟。当时记下了 31 人死亡，然而死亡人数在不断地增加。据估算，清除污染的工作人员中近 1 万人死亡。至少 50 万人受到放射性污染，仅在 22.9 万名清除污染的工作人员中，大约有 8 500 人在 1991 年前死亡。

机器人。机器人在现代自动化生产系统中的广泛使用，极其显著地提高了生产效率和产品质量，有力地改善了有毒、有害工种工人的安全卫生条件。机器人的安全问题实际上就是要实现科幻小说家 I. Asimov 提出的“机器人三定律”：

第一定律：机器人不得伤害人类。

第二定律：机器人必须服从人类的命令，除非这命令违反了上述第一定律。

第三定律：机器人必须保护自己的生存，除非这种保护违反了上述第一、第二定律。

实际上，国外曾多次发生工业机器人打死工人的悲剧。1981 年 7 月 4 日，日本的川崎重工业明石工厂，一工人被机器人挟住胸部而压死。由于工厂是无人化的，被挟住的工人没人发现，当偶然过路的其他工人发现时已经倒地死亡。1984 年 11 月，在日本发生了机器人从上方袭击作业者的事故，击破安全帽的塑料薄膜，继而穿透被害人的头骸骨而致死，灾害现场惨不忍睹。据统计，1987 年至 1990 年末日本已有 11 人被机器人打死。由此可见，机器人的安全性是至关重要的。

民用航空。这个领域广泛实现了航空器驾驶舱自动化和空中交通管理的自动化。高新技术的应用在给民航带来经济效益的同时也带来了安全效益，有效地避免了飞机失控、相撞等传统飞机经常发生的事故。至今，已成了最安全的交通工具。但是，即使驾驶自动化水平很高的第三代喷气客机有时也难逃机毁人亡的噩运。由于自动驾驶仪成功地取代了许多原先由人来完成的工作，在某些方面甚至比人做的更好，因此某些驾驶员产生了过分依赖自动驾驶的思想，驾驶员忽略了对飞机的监控。例如，1992 年某航空公司的一架 B737-300 飞机，在临近机场下降改平飞时，自动油门发生故障，右发一直保持慢车位，造成飞机长时间推力不对称，结果，自动驾驶仪横侧操纵能力饱和，致使飞机坡度不断增加。当飞行员发现情况异常时，为时已晚。实际上，这起事故可以由驾驶员及时断开自动油门改为手动操纵油门就能避免。另外，空中交通管理的失误是造成机毁人亡的另一个重要原因。2002 年 7 月 1 日德国时间晚 11 时 43 分，一架俄罗斯图-154 客机与敦豪国际快运公司的一架波音-757 货机，在德国南部靠近瑞士的博登湖附近 12km 的高空相撞坠毁，机上 71 人全部罹难。当时负责对两架飞机进行飞行

监控的是瑞士空中导航公司，事发时，所属瑞士苏黎世空管中心的飞机防撞自动报警系统正因保养检修而关闭，而值班的两名空管人员又有一人离岗休息。事后，对图-154客机黑匣子数据的解读表明，这架飞机的驾驶员收到改变飞行高度的时间，距撞机前只有短短44 s，实际上至少应在1.5 min前就开始降低飞行高度。7月13日瑞士空中导航公司值班导航员表示，他愿意承担对7月1日两架飞机高空相撞事故的责任。很显然，这完全是由地面导航员指挥失灵造成的重大事故。

20世纪70年代令航空界震惊的是，事故原因因素分类统计表明，“人为因素”已经上升为现代航空事故的主要原因因素，占到80%～90%，这中间又以人犯错误最为常见(包括过分依赖驾驶自动化)。

铁路运输。铁路运输是一个庞大而复杂的交通系统，它的高风险表现在列车碰撞和脱轨事故直接造成人员伤亡和财产损失的严重性上。此外，与其它交通系统相比，超越或交错的自由度极低，在短时间设定迂回通路又不容易，这就会使局部事故造成大范围的运输障碍，进一步加剧了经济损失。为此，铁路运输部门围绕防止列车碰撞和脱轨，在整个铁路运输系统的各个环节上采取了一系列安全措施，取得了很好的效益。

尽管如此，列车碰撞和脱轨事故仍难以避免。美国联邦铁路管理局的事故报告表明，从1985年到1987年共发生了171起事故，其中碰撞和脱轨事故只占了14起，但死亡人数却在总死亡人数23人中占了20人，受伤人数在总受伤人数831人中占了446人。其中，1987年12月发生在马里兰州Chase的重大恶性事故，是由3台货物机车组成的列车未能观察信号而通过道岔从支线进入正线，与一列时速为169km的客运列车撞击，造成16人死亡，176人受伤。因此，高度重视避免列车的碰撞是非常必要的。

随着生产的发展和人们生活水平的提高，客运量在不断增长，高速铁路运输的重要性已经日益为人们所认识，它是解决大通道旅客快速输送问题的最有效途径，已经成为世界各国和我国铁路必然的发展趋势。但是，它在带来效益的同时也带来更大的风险，这就必然去探索一套全新的安全理论和措施，降低碰撞和脱轨的风险。

公路交通。随着汽车工业的发达并且进入千家万户，更由于高速公路的大量修建，在给人们的出行带来便利的同时也加大了风险。为此，每年将1/5左右的汽车生产费用投放到车载电子和计算机系统上，在地面上还配置了高速公路交通管理电子信息系统。

公路交通的主要危险是汽车的碰撞和汽车的失事。为了避免碰撞，在发现前方有障碍物时，通常采取停车或绕行的措施。然而，停车或绕行如发生在铁路平交道口、隧道或视野不好的拐弯处，往往却成了引发碰撞事故的原因。因此，对汽车的安全状态，被时时刻刻变化的环境条件所左右。根据德国1995年发表的统计结果，25%的公路交通事故是尾追碰撞。尤其在恶劣的气候条件下，甚至会发生多米诺骨牌式的尾部碰撞。为了解决这个问题，发达国家都在研究制造汽车的避撞自动控制系统，这是进一步降低高速公路风险的重要方向。

军事防御系统。在科罗拉多州夏延山下人工开凿的一个巨大山洞群里，由庞大复杂的指挥、控制、通信系统构成的北美防空联合司令部早期警报指挥中心，时时刻刻等待着原苏联人即将进攻的信号。由于一个价值仅45美分的极小的计算机集成电路芯片失效，曾在1979年11月9日和1980年6月3日两次发生虚假的原苏联人进攻的警报。第一次，1 000枚具有击中原苏联本土目标能力的民兵式洲际弹道导弹处于初级戒备状态；10架战术战斗机起飞。第二次，战略空军司令部值班军官命令全部待命的B-52机组人员登机并启动引擎。战争处于一

触即发状态。由此看来，军事防御系统的虚假信息造成多么大的危险。但是各子系统的彼此独立，其间配合又是松散的，很快就证明警报是假的，很快解除了警报，恢复了安宁。

武器装备。武器装备的最大特点就是从它诞生之日起就存在着巨大的危险（称固有危险），稍有疏漏，其后果不堪设想。俄罗斯"库尔斯克"号潜艇，2000 年 8 月 12 日在巴伦支海上参加军事演习出事沉没，艇上 118 名海军官兵全部遇难。它震惊了全世界！2002 年 7 月 26 日，俄罗斯总检察院总检查长乌斯季诺夫宣布，调查结果显示，2000 年 8 月 12 日，在巴伦支海参加军事演习的"库尔斯克"号核潜艇上人员在准备发射鱼雷时，由于易燃物质过氧化氢从鱼雷上一个微小的裂缝泄露，鱼雷装置发生爆炸。爆炸引起潜艇隔舱内温度急剧上升至 2 000℃到 3 000 ℃的高温，在第一次爆炸发生 2 s 后，潜艇内存放的其它鱼雷又发生了第二次大爆炸，它摧毁了 80％的船体。幸存的艇员全部逃到了第 9 舱，他们在那里为生存奋斗了 8 h。这个震惊世界的大悲剧，罪魁祸首却是鱼雷上的一个微小裂缝。因此，武器装备比其它安全关键系统，在安全性上有着更高的要求。

医疗系统。由于"人命关天"，医疗系统本来就是一个高风险部门。由于以计算机为核心的各种医疗仪器和设备研制成功并投入临床使用，使许多人力所不能及的医疗行为变得很容易实现。减轻了病人的痛苦，提高了医疗水平；对推动医疗系统的现代化发挥了巨大作用。但也必须清醒地认识到，这些医疗仪器的风险也在加大，哪怕一个很小的失误也会带来不可挽回的严重后果。

Therac-25 是基于计算机的电子加速器放射治疗系统，已经安装了 11 台，美国 5 台，加拿大 6 台。根据调查，由于操作人员的差错，对仪器的安全校验粗心大意以及取消了硬件安全联锁等原因，从 1985 年到 1987 年共发生了 6 次过剂量放射线照射，最大的达到正常值的 100 多倍，最后造成 4 人死亡的严重后果。

通过对各类安全关键系统的讨论，使我们认识到：

1. 安全关键系统就是指各种高风险系统，它具有很高的酿灾潜势。这种潜势一旦失控而释放，就会造成巨大灾难。

2. 安全关键系统是一个规模庞大、各子系统间配合紧密、相互作用极其复杂的系统，并总是与时俱进、采用当代高新技术，有的本身就是属于高新技术范畴。

3. 安全关键系统的绝大多数是在非常恶劣、危险的环境下运行，有些环境因素人类也难以驾驭。

4. 由于 1、2、3 原因，即使一个很小的设计失误、一个小零件的故障、或使用人员的一个小差错，都会导致安全关键系统发生意想不到的多重故障，最终酿成事故。

5. 安全关键系统一旦酿成事故，就会造成大量的人员伤亡、巨额财产损失以及大范围环境破坏的惨重灾难。人类必须严肃、认真、科学地对待安全关键系统。

6. 科学技术的进步在为人类造福的同时，也带给人类新的更大的威胁。正是人类与高风险的不断斗争中，不仅推动了"软"安全科学理论和技术的发展，诸如安全管理学、安全系统学、安全法学、安全经济学；而且也有力地促进了"硬"安全科学理论和技术的形成和发展，其中以计算机为核心的安全关键系统理论就是一例，也是本书关注的重点。

7. "硬"安全科学理论和技术的形成和发展，改变了人类对安全关键系统认识的被动局面，可以这个科学体系为指针，指导我们更好地分析每一种安全关键系统的特殊性，主动地全面地采用更为合适的安全技术，研制出更加安全可靠的安全关键系统；指导我们更主动更深入地探

索安全关键系统的规律，不断地充实它、发展它。

应该看到，用安全科学理论指导安全关键系统的实践，并将安全技术合理地用于安全关键系统中，已获得重大经济效益和社会效益。使许多安全关键系统能够正常运行，并在系统发生故障时发挥了保证安全的重大作用。1992 年我国用长征 2 号捆绑式运载火箭发射“澳星”就是令人信服的实例。3 月 22 日第一次发射，4 个助推器点火过程中，突然出现故障，当即采取控制措施，终止了发射，保全了“澳星”和火箭。一场重大的损失和灾祸避免了，但给人们留下了深思。在火箭发射出现故障的刹那间，发射系统实现了自动关机，这一成功的安全系统控制事例，说明中国科技工作者用安全系统理论与火箭发射安全工程相结合，结出了成功的硕果。终止发射后，科技人员能够在短时间内查明故障原因，又一次显示出他们已把握住系统中各安全因素及其相互作用的内在规律。

1.2　安全关键系统的结构

1.2.1　系统与环境

安全关键系统的结构如图 1.1 所示，它由控制器、输入接口、输出接口、人机接口、传感器和转换器（也称为执行机构）等部分组成。其中，控制器、输入接口、输出接口等组成了广义控制器，人机接口、传感器和转换器组成了环境接口，而各类系统使用人员、受控对象或物理过程等组成了环境。广义控制器按一定的方式通过环境接口与环境进行相互作用。

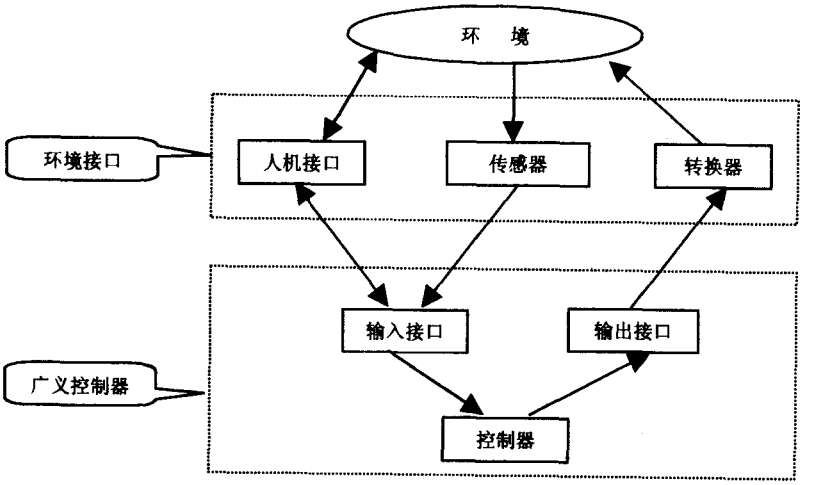


图 1.1　一个典型的实时系统结构

在图 1.1 中，操作员、维护员、管理员等各类系统使用人员通过人机接口与广义控制器进行交互，该接口至少提供显示和记录功能；受控对象或物理过程通过传感器将自身的状态信息以某种电信号方式输入给控制器；输入接口把人所发出的指令、输入电信号等转换为控制器能够接受的形式；控制器完成规划、计算和控制等任务；转换器接受控制器所发出的命令，改变受控设备的状态；输出接口把控制器的命令转换为转换器能够识别的信号。

安全关键系统的物理结构可以是集中式的，也可以是分布式的。控制器可以是一个由继电装置所构成的电气控制器、或者是一个由电子元器件所构成的电子控制器，或者是一个由计

此为试读，需要完整PDF请访问：www.ertongbook.com