人的失误及其可靠性分析

王武宏
曹琦 著

西南交通大学出版社

国家自然科学基金资助项目

人的失误及其可靠性分析

Human Error Identification in
Human Reliability Analysis（HRA）

王武宏　曹琦　著

西南交通大学出版社
·成　都·

内 容 简 介

人的失误及其可靠性分析的研究是当今一项颇具挑战性的前沿课题，引起了各国学者的高度重视和浓厚兴趣。本书结合作者对这一课题的研究积累，建构起人的失误及其可靠性分析的新框架和理论体系，其意义在于从不同角度来拓展人的失误及其可靠性分析的研究方法和运用范围。全书共分九章，即人的失误及其可靠性分析的发展、现状与前景，人的行为模式，人的失误致因分析的数据库，人的可靠性定量分析方法，人机系统中人的可靠性评价模型，人的失误机理辨识，两人监控作业能力分析，存在多状态人为失误时人机系统可靠性评价模型，人机环境系统动态结构分析的事变树模型等。

本书适用于核科学技术、航空、交通运输、机械仪表、电子电气、自动化、管理科学、心理学及安全科学等跨学科的研究人员、教师、研究生，可使读者从中获得该领域的系统性新知识。

人的失误及其可靠性分析
王武宏 曹 琦 著
出版人 张 雪
责任编辑 李彤梅
封面设计 郑 宏
*
西南交通大学出版社出版发行
（成都二环路北一段 111 号 邮政编码：610031）
郫县报华印装厂印刷
*
开本：850mm×1168mm 1/32 印张：8.25
字数：196 千字 印数：1～500 册
1999 年 3 月第 1 版 1999 年 3 月第 1 次印刷
ISBN 7-81057-046-3/Z·073
定价：18.00 元

前　言

人的失误及其可靠性分析的研究是当今一项颇具挑战性的前沿课题，引起了各国学者的高度重视和浓厚兴趣，相继出现了许多量度人失误率的可靠性分析方法，并且在核科学技术、航空、交通运输、机械仪表、电子电气、自动化、管理科学、心理学及安全科学等领域中得到了广泛应用，蕴存着极其丰富的内涵。

本书结合我们对这一课题的研究积累，建构起人的失误及其可靠性分析的新框架和理论体系，其意义在于从不同角度来拓展人的失误及其可靠性分析的研究方法和运用范围，以期人的失误及其可靠性分析的研究更趋完善。全书共分九章，其中第一、二、三、四章主要评述性地介绍了本领域的国内外学者对人的行为模式、失误致因的识别、人可靠性分析的数据和人可靠性定量分析方法等方面的一些较为成熟的研究成果，同时也阐述了我们对人的差错元、人的行为特征、人的行为形成主因子的定量化辨识及人行为的实际模式等内容的新认识；第五、六、七、九章则结合交通运输系统的特性，着重从国家自然科学基金资助项目（59408010）的部分成果中，较为细致地论证了人的失误机理、可靠性量化方法、两人监控作业能力、事变树模型及其应用价值；而第八章则介绍了存在多状态人为失误时人机系统可靠性评价的几种模型，旨在为感兴趣的同行提供人的失误及其可靠性分析的研究思维。

尽管我们力求本书的全面和详尽，并且注重该领域的最新成果，无奈自身学识所限，加之，我们的一些探索性研究成果（包括那些粗浅和不成熟的成果）尚需不断完善和深入，因此，书中

肯定存在不少缺点、遗漏乃至错误，藉此之际，我们殷切地希望大家的不吝指正！

刘登弟、苏文胜、魏永春、张继超、王晓红等在本书的文稿整理中付出了辛勤的劳动，而意大利欧洲系统工程与信息研究所的 P. C. Cacciabue 博士、美国德克萨斯技术大学的 M. R. Endsley 博士以及 A. D. Swain 博士为我们提供了有价值的资料并给予友好建议，没有他们的帮助，本书是难以面世的。在此，谨向他们致以我们最诚挚的感谢之情！

本书的顺利出版，承蒙国家自然科学基金和西南交通大学重点出版基金的资助，特此鸣谢！

最后，谨将本书奉献给那些关心、鼓励、支持和帮助我们的人们！

作　者

目　录

第一章 总 论

1.1 人的失误及其可靠性分析概述

在大多数情况下，人机系统主要是通过人的操纵、调节和检查等方式来实施控制的。即使高度自动化的人机系统，亦或新近发展的人机一体化系统，也不能完全离开人的监视以及对异常情况的处理。因此，对人机系统可靠性的评定，如果不考虑人失误的可能性及其概率，评定结果不可能代表系统真实的可靠性水平，同时也将导致对系统安全性评价或概率风险性评估的不完全甚至难以获得定量性结果。

许多研究业已表明：人机系统的可靠性与安全性在很大程度上取决于人的可靠性。据统计[27]，20%～90%的系统失效与人的失误有关，其中直接或间接地肇发事故的比率为 70%～90%，在将来，这种比率有可能变得更高。一方面，新的技术进步为完成相当复杂的作业提供了越来越可靠的机器；另一方面，人就显然成为人机系统中更为不可靠的因素。

通过大量的研究发现，人为失误在事故致因中占居着主要地位[5,40,57,66,78]。1980～1984 年间，美国海军设施的控制系统失效事故中由人的失误肇发的占 63.6%；美国警察当局对 13568 起交通事故的致因研究表明交通参与者的失误为 80%；最具权威的美国 NASA 航空安全报告揭示出 22226 件飞行事故中人为失误的比率高达 80%；西德"汉莎"航空公司从 1959～1989 年的事故分析也总结到人为失误造成飞机失事的原因占到 70%；而

Heinrich 在对具有 2000--2200 员工的大型公司所发生的 551 件事故的致因分析披露出 80%的事故与人的失误有关。相近的数据也可以在电子电器事故（50%～70%）、石油化工事故（60%）及核电站事故（90%）中发现；而进入 90 年代后，人为失误肇发的各类事故其比率已上升到 90%。由此可见：当一个系统变得更加复杂并且人的失误严重地影响到系统的安全性、可靠性及经济性时，人的可靠性就显得愈发重要，这点从人为失误肇发的福特宾达汽油罐的破裂、三哩岛核电站放射性物质泄漏事故、苏联切尔诺贝利核电站事故和爱西瓦特石油爆炸等灾害性事故的危害程度以及对社会、环境、生态所造成的恶劣影响中可以更加清楚的认识到。

1.1.1 人的失误及其可靠性分析的目的

通过对人失误的因素，诸如教育不够、训练不当、设计不合理及作业程序混乱等的辨识，人们越来越意识到管理决策中人为失误所造成的恶劣后果增大了系统的危险性，从而希望揭示出从事这种职业的风险性大小。如果这些系统的运行并不直接涉及人的操纵或控制，那么风险就在人们所能接受的范围内，一旦包括人员，就需要对这种风险性进行更为客观的估计。贯穿于整个系统的设计、制造、运用、维修、管理甚至报废阶段的人可靠性分析的主要目的就在于对人失误概率的合理量度，这种量度将有助于揭露人为失误的潜在隐患，并且实现意外事故的预先控制。

对一个人机系统进行人可靠性分析得越早，获取的效益将越高。这就意味着对人失误的客观评价不仅能提高系统的可靠性和安全性，而且更重要的是能减少对社会的不良影响。因此，人可靠性分析正代表了这种行之有效而又迫切的需求趋势，其目的可归结为：

实用目的：采用特定的系统来控制人失误的危险后果及其影响程度；

工程目的：准确地评估给定作业状态下人的可靠性，以期作为对系统设计的依据；

科学目的：丰富人的可靠性理论，实现对人机系统的客观认识。

1.1.2 人的失误及其可靠性分析的含义

（1）人的可靠性（Human reliability）

人的可靠性研究贯穿于整个人机系统的设计、制造、使用、维修和管理的各个阶段，应充分辨识出人失误的本质并量化其可能性，通过对作业状态中人行为结构的分析，借助相应的安全保障体系，当人发生失误时，在确保人身安全的前提下，不致严重地影响到系统的正常功能。这样，人的可靠性就可以定义为：在规定的条件下，在最短的时间内，由人成功地完成作业任务且能实现人机系统合理有效运行功能的能力。而人的可靠度则指对其可靠性的概率量度。一般来说[6]，人对简单且离散的信号反应的可靠度在0.99995～0.99999之间，对复杂输入的复杂反应其可靠度（包括与另外操作者共同反应）为0.970～0.990之间。

由于人的行为在人机系统中主要表现为系列操作和综合认知两类，人的可靠性就应包括人的操作可靠性和认知可靠性两方面的含义。需要特别强调的是，人的可靠性是指人员经过训练之后，进入“稳态工作期”的可靠性，不包括学习阶段“初始失调期”的情况。表1.1为人与机器可靠性的特征比较[2]。

（2）人的失误（Human error）

人的功能自由度导致人在完成同一作业时，其行为具有很强的不确定性，从而引起人机系统的故障或影响到系统的正常功能。这样，人的失误就可定义为：在规定的条件下、在特定的作业程度中，在最短的时间内，人完不成系统分配给他的功能且导致作业计划混乱或系统不正常和财产损失的一种状态。而人的失误概率（简称失误率）则是对人失误的概率量度。

表 1-1 人与机器可靠性的特征区别

比较特征	机器可靠性	人的可靠性	
		间歇性作业	连续性作业
系统定义	由一系列执行相应功能的元件组成	由若干的人行为单元组成	连续性的控制作业
系统组成	元件间具有功能关系	为完成特定的作业，行为之间具有功能联系	不必要确定作业单元间的功能联系
系统效分析失	故障树分析	在特定的作业中，由一组相互影响的失误集合确定	对连续性的系统行为，由两态失误逻辑分析
失效特性	• 两态失效逻辑 • 多维失效 • 共因失效	• 有时较难运用两态失误逻辑 • 多维失误 • 共因失误 • 差错纠正能力	对连续性的系统行为，由两态失误逻辑分析
失效原因	大多数机器失效可以通过物理与化学原理进行解释	没有较好的方法对人的失误进行解释	对连续性的系统行为，由两态失误逻辑分析
系统可靠性评价	• 通过失误逻辑的概率处理和统计独立假设就可进行系统可靠性评价 • 如果不符合统计独立假设，较难用网络可靠性和阶段分配可靠性来评价	由于描述人行为单元功能关系的困难，较难对人可靠性进行评价	通过两态失误逻辑的概率处理，根据随机模型就可以进行可靠性评价
数据	对大多数机器来说，要求具有相当大的数据库	• 建立了人失误的部分数据库 • 大多数通过专家评估	通过两态失误逻辑的概率处理，根据随机模型就可以进行可靠性评价

(3) 人可靠性分析（Human reliability analysis，即 HRA）

人可靠性分析可定义为用于定性或定量评估人的行为对系统可靠性或安全性影响程度的方法。尽管人可靠性分析已作为一门独立的学科，但它与概率风险性评价（Probabilistic risk assessment，即 PRA）仍具有一定的联系，概率风险性评价的目的

在于辨识有人参与作业的风险性，而人可靠性分析则在于评估人完成这些作业的能力，包括如下内容：

①人的可靠性如何由概率来量度；

②人的行为对人机系统的影响是怎样通过人失误的可能性评估的；

③人可靠性分析与概率风险性评价相对独立，但又彼此相关，即两者之间具有内在的联系。

由此可知，人可靠性分析作为一种旨在将人为主要失误降低到现阶段所能接受的最低水平的一种设计或重新设计的工具，其意义不仅在于通过严格的系统辨识来揭示人机系统不能正常运转所造成的损失并识别不希望发生事故的危险后果的原因，而且更重要的是实现对这种损失和后果能够予以客观定量化的评价，包括定性与定量分析两个方面。

1）人可靠性的定性分析

人可靠性的定性分析在于辨识人失误的本质和失误的可能状况，它是通过观察、访问、查询和失误记录等手段来进行人机系统中人的失误分析。在系统进行过程中，人的失误包括四个方面，即没有执行分配给他的功能、错误地执行了分配给他的功能、按错误的程序或错误的时间执行了分配给他的功能、执行了没有分配给他的功能。造成这些失误的原因可以通过人的行为形成因子（Performance shaping factors，即 PSF），即影响人正常行为的一些因素来进行归纳，一般是从人机界面的缺陷、人自身的内部特征、作业特性、组织管理和环境因素等五个方面来构造。这些行为形成因子将导致人的感知、解释、诊断、决策和操纵失误，其中一些将直接或间接地诱发系统故障乃至肇发事故。因此，人可靠性的定性分析的目的不仅在于减少人的失误而进行系统设计或重新设计时提供依据，更重要的是为人可靠性的定量分析打下基础。

2）人可靠性的定量分析

人可靠性的定量分析是从动态和静态两个方面来估计人的失

误对系统正常功能所具有的影响及其程度。这种估计是通过人的操作数据、行为模式和适当的数学模型来进行的。对于复杂和重要的人机系统，还可以根据人机工程专家、工程技术人员和管理人员，尤其是实际作业人员的经验建立专家知识库，采取定性与定量相结合的分析方法。

1.1.3 人的失误及其可靠性分析的目标和方法

根据人机系统中人的作用和人对系统的影响程度，结合相关的理论、方法及人机环境系统特性，人的失误及其可靠性分析的研究目标和方法主要分为如下八个方面：

(1) 人作业可靠性评估

·目标

评估人的失误概率，定量辨识人的行为对人机系统可靠性的影响及其程度。

·研究方法

① 人操作行为数据的统计处理；

② 随机模型；

③ 计算机模拟；

④ 人的行为分析。

(2) 人的维修作业可靠性

·目标

调查维修人员在实际故障诊断和修理过程中所产生的失误，并且定量评价这些失误对系统有效性的影响程度。

·研究方法

① 随机模型；

② 人的行为分析。

(3) 人作业可靠性评估中的数据采集

·目标

为量度人的作业可靠性，建立人作业行为的数据库。

·研究方法

① 实验室测试；

② 实际作业状态的辨识；

③ 专家评判。

(4) 人机系统的有效性

·目标

结合人与机器的不同特性，获取评价人机系统有效性的方法。

·研究方法

① 人机系统状态的计算机模拟；

② 随机模型。

(5) 人机系统可靠性分配

·目标

在现有的技术经济条件下，优化人机系统可靠性设计。

·研究方法

① 经典的优化技术；

② 计算机模拟。

(6) 闭环控制系统中人的行为模型

·目标

建立追踪、补偿人机系统中人行为的数学模型。

·研究方法

① 优化控制理论；

② 参数辨识。

(7) 人认知行为的计算机模拟

·目标

辨识影响人认知行为的因素，建立人的认知可靠性模型。

·研究方法

① 认知心理学和认知工程学的理论；

② 人工智能；

③ 计算机模拟。

(8) 人机环境系统模型

·目标

建立人机环境系统静、动态结构模型，用于辨别人在系统中的地位，以便充分把人特有的心理活动过程及生理反应特性体现在系统设计中。

·研究方法

① 随机、模糊和突变模型；

② 计算机仿真；

③ 现场和实验测试。

1.2 人的失误及其可靠性分析的发展过程

早在50年代，一些行为科学家和工程师们注意到仅仅辨识出人失误的原因尚显不够，还必须量化人失误的可能性大小，以便作为一种有用的工具，用于对复杂系统的风险评价。

第一次量化人失误概率的工作是由Sandia国家实验室的数学家H. L. Williams和电子工程师Purdy Mergs于1952年进行的，他们在研究中发现[45]：地面上人的简单操作失误率为0.01，而空中完成相同的操作时，人的失误率将达到0.02。可以说，Sandia国家实验室的研究揭开了人可靠性分析这一新领域的序幕。

1964年8月17～19日，第一届人可靠性分析的学术会议在新墨西哥大学举行，全部论文于1964年12月发表在美国人的因素学会主办的《人的因素》杂志的第六卷上。从那时起，相继建立了三个人的可靠性数据库，即AIR数据库、Aeiject总数据库和BanKer－Ramo数据库；与此同时，也出现了不少人的可靠性分析方法，其中人因失误率预测法(THERP)是1961年Alan D. Swain等进行核武器的安全性评价时提出的，随后在不断改进和完善的基础上，成为目前的一种较为成熟和普及的人可靠性分析方法。美国Knoxiville的加工安全研究所，每年举行两次为期6天的介绍

该方法的研讨班，由 Alan D. Swain 及其合作者主讲。* 这对人的失误及其可靠性分析的研究及应用具有一定的促进作用。

人可靠性分析最初应用于军事武器装备中人的失误率评价，而大规模地应用于其他系统，诸如核电站则是由丹麦的欧洲 RISφ 国家实验室、英国原子能局和法国原子能委员会开始的，其中部分成果于 1968 年 10 月 8 日～9 日在 RISφ 国家实验室举行的未公开的欧洲原子能学会的学术会议上进行了报道。美国于商业中的应用是从 1972 年开始的，即以著名的 WASH—1400 核安全评价为其标志，这次研究使用了 THERP 方法对两个核电站的人为失误进行了评估。

1973 年，国际电气与电子工程师学会主办的《IEEE 可靠性汇刊》出版了人可靠性研究的专集，被认为是人的失误及其可靠性研究的重要里程碑，从而把人可靠性研究推向一个新阶段；随后又举行了两次 IEEE 人的因素的学术会议，到 1985 年的第三届 IEEE 人的因素学术会议上，众多的学者发表了许多见解颇为新颖的观点，对人可靠性的深入研究起到了积极作用；接着于 1988 年，欧洲安全与可靠性学会主办的《可靠性工程与系统安全》以增刊的形式发表了一系列人可靠性分析的研究论文，并于 1990 年，又出版专刊对人可靠性分析的研究方向和现状进行了争论，在充分肯定了人可靠性研究的重要意义后指出了相应的发展策略，至此，人可靠性分析的研究迈入了第二阶段。

进入 90 年代，人可靠性分析方法的研究更趋活跃，被认为是多学科交叉渗透的面向 20 世纪的重点研究领域[11]。这样，许多学者将人工智能、随机模拟、心理学、认知工程学、神经网络、信息论、突变论、模糊集合等学科的思想应用到人可靠性分析中，出现了以 J. Reason（1990）为代表的人可靠性心理模型，Erik Hollnagel（1992）的人可靠性分析综合认知模型，Alenka Hudoklin

---

* Alan D. Swain 博士与王武宏的私人信件，1995 年 2 月 14 日，Tucson。